Nations Unies TD/B/C.II/EM.5/3

Conférence des Nations Unies sur le commerce et le développement

Distr. générale
10 avril 2015
Français
Original: anglais

Conseil du commerce et du développement
Commission de l'investissement, des entreprises et du développement
Réunion d'experts sur la cyberlégislation et réglementation comme moyen de renforcer le commerce électronique, y compris les études de cas et les enseignements tirés de l'expérience
Genève, 25-27 mars 2015

Rapport de la Réunion d'experts sur la cyberlégislation et réglementation comme moyen de renforcer le commerce électronique, y compris les études de cas et les enseignements tirés de l'expérience

Tenue au Palais des Nations, à Genève, du 25 au 27 mars 2015

Table des matières

GE.15-07537 (F) 040515 060515
1507537

Introduction

1. La Réunion d'experts sur la cyberlégislation et réglementation comme moyen de renforcer le commerce électronique, y compris les études de cas et les enseignements tirés de l'expérience, s'est tenue au Palais des Nations, à Genève, du 25 au 27 mars 2015, comme l'avait décidé le Conseil du commerce et du développement à sa cinquante-neuvième réunion directive, le 24 juin 2014. Elle a rassemblé plus de 200 participants, représentant tous les groupes de parties prenantes.

I. Résumé du Président

2. La réunion a porté sur les grandes questions suivantes: la manière d'évaluer les besoins en matière de cyberlégislation, les pratiques les plus propres à faciliter les transactions électroniques internationales et à améliorer la sécurité en ligne, le rôle des parties prenantes, les mesures susceptibles d'être prises pour suivre les progrès des pays et des régions en développement dans l'élaboration de législations appropriées, et la contribution que les organisations internationales et d'autres partenaires de développement peuvent apporter à l'application de lois harmonisées sur le commerce électronique.

A. Déclarations liminaires

3. La Directrice de la Division de la technologie et de la logistique de la CNUCED a indiqué que le commerce électronique avait crû et évolué rapidement dans les pays développés et les pays en développement, transformant l'économie mondiale et influant sur les chaînes de valeur internationales, comme des tendances récentes l'avaient montré. Compte tenu des perspectives qu'il offrait et des problèmes qu'il posait, le commerce électronique appelait des mesures adaptées. En tout état de cause, plus d'efforts devaient être faits pour l'inscrire dans un environnement propice, qui soit ouvert à tous et favorise la croissance économique et un développement durable.

4. À compter de la parution de son premier rapport sur le commerce électronique, en 2000, qui avait fait date, jusqu'à celle de son *Rapport 2015 sur l'économie de l'information*[1], la CNUCED avait joué un rôle pionnier dans ces domaines. Elle avait aussi travaillé en étroite collaboration avec d'autres organisations internationales sur les questions du commerce électronique et des technologies de l'information et de la communication (TIC) au service du développement.

5. Le Chef de la Section de l'analyse des TIC de la Division de la technologie et de la logistique a brièvement présenté le programme de travail de la réunion, en mettant en évidence les grandes tendances du commerce électronique et les principaux points à prendre en compte pour créer un cadre légal et réglementaire qui le rende profitable à tous. Il a indiqué que, au vu de l'inventaire mondial entrepris par le secrétariat de la CNUCED, les pays en développement restaient à la traîne en matière de cyberlégislation.

[1] CNUCED, 2015, *Rapport 2015 sur l'économie de l'information: Libérer le potentiel du commerce électronique pour les pays en développement* (New York et Genève, numéro de vente E.15.II.D.1, publication des Nations Unies).

B. Tendances du commerce électronique et problèmes juridiques

6. Les intervenants ont insisté sur la croissance et l'expansion géographique rapides du commerce électronique, qui se poursuivraient probablement dans les années à venir. Avec l'amélioration généralisée des TIC, les services de commerce électronique et les services connexes de livraison avaient fait l'objet d'une demande accrue. Le commerce électronique avait permis à un plus grand nombre de petites et moyennes entreprises de s'engager dans des activités exportatrices et d'exporter dans un plus large éventail de pays que par les canaux commerciaux traditionnels. Les marchés émergents et les pays en développement jouaient un rôle de plus en plus important, aussi bien comme clients que comme fournisseurs. Plus d'harmonisation et de transparence était nécessaire pour que le commerce électronique soit véritablement mondial. Les intervenants ont soulevé les questions de la protection des consommateurs, du respect de la vie privée, de la protection des données et de la cybercriminalité. Il est ressorti de leurs discussions qu'il fallait investir dans les infrastructures numériques et mettre en place une cyberlégislation et réglementation qui accroît la confiance et la sécurité en ligne.

7. Plusieurs impératifs devaient être satisfaits, notamment celui d'investir dans le capital humain afin de rendre les entreprises de commerce électronique performantes et rentables. Il fallait aussi permettre à la population, par des campagnes d'information et de sensibilisation, de tirer un meilleur parti du commerce électronique. Comme un intervenant l'a souligné, les jeunes entreprises du secteur avaient besoin d'un environnement dans lequel elles pourraient prospérer. En vue d'assurer la solidité et la bonne gestion de ces entreprises, il importait de renforcer les compétences locales, surtout celles des cadres intermédiaires. Dans bon nombre de pays, le développement des infrastructures faisait aussi problème. Selon certains intervenants, les transports routiers étaient indispensables à la facilitation des livraisons nationales et internationales de marchandises. Des systèmes de paiement sécurisés étaient également essentiels. Les 660 000 bureaux de poste ouverts dans le monde entier pouvaient aussi jouer un rôle déterminant.

8. Il importait que le commerce électronique s'inscrive dans un cadre juridique conciliant réglementation, concurrence et innovation, pour être légal, sécurisé et avantageux, le commerce électronique devait aussi être servi par des institutions aux moyens suffisants et au personnel qualifié. Il nécessitait des réseaux, des systèmes et des structures juridiques interopérables et compatibles entre les pays, de manière à éviter les complications qui pouvaient naître de leurs divergences et de leurs incohérences (par exemple, dans le domaine de la fiscalité). Il convenait de promouvoir les droits individuels, de prévenir les préjudices et de faciliter les transactions grâce à un cadre juridique adéquat et à des organes propres à assurer son application. Cependant, l'adoption et l'application de cyberlégislations avaient un coût. Par exemple, on estimait que, les entreprises de l'Union européenne dépensaient environ deux milliards d'euros par an pour se mettre en conformité avec les lois sur la protection des données.

9. Selon certains experts, le commerce électronique devait faire partie des stratégies de développement. Il convenait que le commerce électronique et la cybersécurité soient considérés non seulement d'un point de vue juridique et commercial, mais aussi en fonction des objectifs de développement économique et social. L'intégration sociale et l'accès universel aux services de commerce électronique ne devaient pas être perdus de vue. Plusieurs experts ont prié la CNUCED et d'autres organisations internationales de contribuer à un plus large développement économique en aidant les pays à renforcer leurs écosystèmes, leurs marchés et leurs législations dans ce domaine.

C. Lois sur les transactions électroniques

10. Lors de la séance informelle consacrée au développement des transactions électroniques et aux questions juridiques posées par la facilitation du commerce en ligne, les participants ont débattu de la compatibilité des lois, qui était indispensable pour stimuler le commerce international, et ont analysé les différences existant dans le droit public et le droit privé de pays d'une même région ou de régions distinctes. La Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux (2005) était un exemple récent d'instrument juridique international relatif au commerce électronique.

11. Pendant longtemps, les transactions en ligne et, par voie de conséquence, le commerce électronique international, avaient pâti des problèmes d'identification et d'authentification. L'Union européenne avait fait avancer la situation en adoptant le Règlement n° 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, portant abrogation de la directive 1999/93/CE, qui impose la reconnaissance des moyens d'identification électronique entre ses États membres. Un certain nombre d'experts se sont intéressés à la possibilité d'appliquer les dispositions de ce texte aux échanges commerciaux entre l'Union européenne et des pays tiers. Selon une représentante de la Commission européenne, la chose était envisageable, sous certaines conditions, notamment le respect du principe de non-discrimination et la neutralité technologique.

12. Les lois nationales sur les transactions électroniques ne devaient pas constituer accidentellement un obstacle au commerce international. Il arrivait que la reconnaissance mutuelle des signatures électroniques soit empêchée par l'utilisation d'infrastructures à clef publique. Plusieurs experts ont insisté sur l'importance du principe de neutralité technologique, défendu par la Commission des Nations Unies pour le droit commercial international. L'internationalisation du commerce électronique exigeait une interopérabilité des systèmes nationaux de reconnaissance des signatures électroniques. Des guichets uniques de commerce dématérialisé étaient aussi utiles.

13. Les pays en développement avaient des chances de devancer les pays développés, qui devraient adapter leurs systèmes traditionnels au commerce électronique et surmonter des problèmes connexes, notamment d'infrastructure. Les experts ont examiné plusieurs options d'harmonisation des lois sur les transactions électroniques, depuis l'établissement de normes internationales − sur l'authentification, par exemple − jusqu'à la conclusion d'un traité, et sont convenus que les mesures retenues devraient être adaptées à la situation de chaque pays. Ils se sont également entretenus du rôle des intermédiaires, du manque de moyens nationaux pour la mise en œuvre des lois sur les transactions électroniques, et de cas concrets où une solution réglementaire était préférable à une solution législative.

14. Les instruments de paiement s'étaient rapidement multipliés pour le commerce électronique de détail, allant des applications mobiles jusqu'aux cartes téléphoniques prépayées. Bon nombre d'entre eux avaient amélioré l'accès des personnes non bancarisées aux paiements électroniques et favorisaient l'intégration financière, jusque dans les zones rurales. Avec ces nouveaux instruments de paiement apparaissaient aussi de nouveaux risques à chacune des grandes étapes de la procédure (avant la transaction, au moment de l'autorisation, de la compensation, du paiement et après la transaction), auxquels il fallait ajouter des risques d'ordre technologique. D'où la nécessité d'une approche globale, qui tenait compte du progrès technologique et de l'évolution des systèmes financiers.

15. Dans certains pays en développement, les innovations dans le secteur des services financiers avaient contribué à une plus grande intégration financière. Le Kenya avait fait figure de pionnier en la matière, notamment en permettant le développement des paiements

par téléphonie mobile. En 2006, la Banque centrale du pays avait autorisé un opérateur de téléphonie à fournir des services de transfert monétaire, ce qui avait considérablement modifié la structure du système de paiement, faisant préférer la plate-forme de paiement mobile au système de paiement de montants élevés.

16. Les experts ont rendu compte de la situation dans leurs pays respectifs et se sont entretenus de cette question complexe, en particulier des réticences des banques centrales à délivrer des licences bancaires à des opérateurs de téléphonie mobile. Un équilibre devait être trouvé entre la promotion de l'innovation et la protection des consommateurs. On considérait généralement que les consommateurs étaient mieux protégés sur des marchés réellement concurrentiels. Certains experts s'étaient opposés à ce que l'on établisse une distinction entre les systèmes monétaires mobiles qui relevaient d'opérateurs de télécommunications et ceux qui étaient rattachés à des établissements bancaires. Seule la qualité du service fourni par le prestataire devait importer. Dans le même temps, ce rapprochement entre le secteur bancaire et le secteur des télécommunications appelait une étroite collaboration entre leurs autorités de réglementation respectives.

D. Protection des consommateurs

17. Une autre séance informelle avait été consacrée aux préoccupations des consommateurs, notamment à l'égard du commerce électronique international. Elle avait aussi porté sur la législation et les politiques propres à garantir aux consommateurs le même niveau de protection dans leurs transactions électroniques et traditionnelles.

18. Les intervenants ont constaté que le développement du commerce électronique, national et international, était porté par l'utilisation accrue d'Internet et la diffusion des appareils mobiles. Chaque fois qu'Internet était accessible au plus grand nombre, la nature, les modalités et le rythme des transactions et des interactions avec les consommateurs étaient radicalement transformés. L'évolution rapide des technologies laissait dans son sillage de nouveaux problèmes à surmonter. De nombreux pays n'avaient toujours pas de dispositions spécifiques pour protéger les consommateurs en ligne.

19. Si le commerce électronique présentait des avantages pour les consommateurs (choix plus large, commodité), il faisait aussi craindre les fraudes, les afflux de courrier indésirable, les atteintes à la vie privée et les problèmes de sécurité des données et de sécurité de l'information. Les consommateurs étaient confrontés à des risques numériques et à des coûts, parfois cachés, associés au traitement des commandes et à la livraison, à l'exploitation des données et au respect de la vie privée, à l'opacité des conditions d'utilisation, à la structure du marché et à la qualité des services. En matière de protection des consommateurs, une distinction pouvait être faite entre les questions relatives aux paiements et celles concernant la livraison des biens et des services commandés en ligne et leur qualité. Les différences entre les principes juridiques nationaux et l'absence de mécanismes internationaux de règlement des différends rendaient problématiques les échanges commerciaux par voie électronique. Dans le même temps, certains experts faisaient observer qu'une trop grande protection des consommateurs pouvait faire obstacle au commerce.

20. Les législateurs devaient prendre en considération la vulnérabilité des consommateurs en ligne, ce qui était d'autant plus difficile que cela faisait intervenir un grand nombre de domaines du droit (droit civil, droit pénal, droit de la propriété intellectuelle, droit de la consommation) et différentes autorités de réglemention. Les consommateurs avaient besoin de voies de recours extrajudiciaires simples et efficaces, en particulier lorsque le différend portait sur des transactions de faibles montants, courantes dans le commerce électronique de détail.

21. Cherchant des moyens de renforcer la confiance en ligne, les intervenants ont évoqué des mesures juridiques et techniques ainsi qu'une plus grande coopération entre les organismes de protection des consommateurs. L'adoption de lois nationales sur la protection des consommateurs était une première étape importante. Au niveau international, l'Organisation des Nations Unies révisait actuellement les Principes directeurs pour la protection du consommateur. Les États Membres avaient décidé d'aborder le commerce électronique en s'appuyant sur les Lignes directrices de l'OCDE régissant la protection des consommateurs dans le contexte du commerce électronique (1999), elles aussi en cours de révision. Les nouveaux principes directeurs tiendraient compte de la diffusion des appareils mobiles (1,7 milliard d'appareils connectés à Internet), grâce auxquels les consommateurs, y compris les enfants, bénéficiaient d'un meilleur accès aux solutions de paiement par téléphonie mobile et en ligne, aux produits à contenu numérique et au commerce électronique participatif. Ils établiraient notamment une protection transparente et efficace d'un niveau au moins équivalent à celui de la protection assurée dans d'autres formes de commerce; la loyauté de pratiques en matière de commerce, de publicité et de marketing; et la communication en ligne d'informations claires et transparentes.

22. L'adoption de lois nationales devait s'accompagner d'un renforcement des organismes de réglementation. Il fallait aussi améliorer l'interopérabilité des systèmes proposant des règles identiques (par exemple, une même qualification juridique des produits entre les pays et des codes de conduite qui régissent les transactions électroniques internationales) ainsi que la convergence des différentes plates-formes technologiques. La coopération internationale devait également être encouragée en vue de lutter contre les fraudes en ligne et les pratiques déloyales de commerce électronique.

23. Dans le but d'améliorer les lois nationales et de mieux armer les organismes de protection des consommateurs, il avait été proposé d'étendre la coopération interinstitutions, de former les autorités de réglementation dans les pays développés et les pays en développement, d'établir des accords de coopération entre organismes de protection des consommateurs, de créer un groupe d'experts nationaux, de rendre les échanges d'informations plus efficaces et d'accorder une place aux débats intergouvernementaux dans des instances telles que la CNUCED. Il avait également été question de la participation de réseaux comme le Global Privacy Enforcement Network, l'International Competition Network et le Réseau international de contrôle et de protection des consommateurs, de campagnes d'information et des possibilités pour les consommateurs de déposer des plaintes en ligne.

24. L'autoréglementation du secteur devait être davantage encouragée et efficacement appliquée. Les intermédiaires de paiement, comme les gestionnaires de cartes de crédit, pourraient peut-être mieux protéger les consommateurs. Certains experts ont recommandé que les secteurs public et privé unissent leurs efforts pour assurer un niveau de protection équivalent, tous moyens de paiement confondus. Une plus grande transparence en cas de violation de données était également importante.

25. Selon certains experts, les sanctions encourues par les fraudeurs étaient trop clémentes et devaient être durcies. De plus, pour améliorer l'environnement général dans lequel les consommateurs évoluaient, il fallait sécuriser les méthodes de paiement; mieux connaître les formes de cybercriminalité existantes (fraude, usurpation d'identité et autres délits); prévoir des dispositifs de recours qui soient accessibles en ligne, efficaces et peu onéreux; éduquer les consommateurs et garantir la neutralité des infrastructures.

E. Protection des données et cybercriminalité

26. Les experts ont réfléchi à la manière dont les cadres légaux et réglementaires de protection des données personnelles et de respect de la vie privée pourraient accroître la confiance des internautes et combattre la cybercriminalité. D'après l'inventaire réalisé par la CNUCED, 107 pays, dont 51 pays développés, avaient une législation sur la protection des données et le respect de la vie privée, et 117 pays, dont 82 pays en développement et pays en transition, avaient adopté des lois sur la cybercriminalité.

27. L'une des principales difficultés dans l'élaboration d'une cyberlégislation était de concilier la protection des données, la fluidité des échanges de données et la liberté d'information. D'autres problèmes complexes se posaient, notamment l'externalisation éventuelle des fonctions de sécurité pour contourner les restrictions mises en place par certains pays au titre du respect de la vie privée. L'importance de plus en plus grande de l'informatique en nuage, dont les effets sur la confidentialité et la protection des données avaient été examinés dans le *Rapport 2013 sur l'économie de l'information*[2], avait aggravé la situation.

28. Les lois sur la protection des données faisaient cruellement défaut dans bon nombre de pays en développement. Pour que les données soient protégées, les mesures de cybersécurité devaient avoir pour principe de ne pas causer de tort. Un intervenant a proposé que les secteurs public et privé obéissent à ce principe, de manière à concilier la confidentialité des données et leur surveillance pour des raisons de sécurité informatique. Les mesures de cybersécurité, notamment de surveillance, devaient être adoptées uniquement en cas de nécessité, être proportionnées, avoir un objectif très précis et s'appliquer de la même façon à toutes les personnes, physiques et morales. Il en résulterait un regain de confiance dans la sécurité nationale, l'application des lois et le secteur privé. L'intégration des critères de nécessité, de proportionnalité et de précision des orientations dans les accords internationaux de cybercriminalité pourrait être un facteur de clarification et d'harmonisation, et renforcer la coopération entre pays.

29. En l'absence de ces critères, les pays risquaient d'aller à l'encontre de la cybersécurité, en affaiblissant les normes de cryptage, en exploitant les «portes dérobées» dans les infrastructures et les applications, voire en propageant des logiciels malveillants. Certaines initiatives prometteuses de renforcement de la cybersécurité, qui passaient par des partenariats public-privé et l'harmonisation des instruments juridiques, étaient déjà engagées. Une meilleure réglementation des intermédiaires était aussi envisageable.

30. Un expert a fait observer que les entreprises étaient de plus en plus victimes de la cybercriminalité. La cybercriminalité internationale pesait sur le commerce mondial et se dérobait aux enquêtes et aux poursuites. Aux fins d'une meilleure coopération internationale sur la cybercriminalité, l'Office des Nations Unies contre la drogue et le crime (ONUDC) avait récemment recensé la jurisprudence et les enseignements utiles en matière de protection des données. Le répertoire ainsi constitué avait été salué par plusieurs participants comme une référence pour l'application de la législation, en particulier dans les pays en développement. Son intérêt dépendrait toutefois en partie de la collaboration internationale, puisque la base de données était alimentée par les informations spontanément communiquées par les pays.

31. Certains experts ont appelé à renforcer la coopération internationale qui, jusque-là présent, s'était révélée moins fructueuse que la coopération régionale. Ses mécanismes

[2] CNUCED, 2013, *Rapport 2013 sur l'économie de l'information: L'économie infonuagique et les pays en développement* (New York et Genève, numéro de vente F.13.II.D.6, publication des Nations Unies).

étaient déficients, et les parties prenantes ne prenaient pas la pleine mesure de son importance. La coopération internationale pouvait être renforcée par des dispositifs formels et informels. Alors que les menaces informatiques étaient de plus en plus complexes et évoluaient rapidement, la communauté internationale n'avait pris aucune mesure concrète à leur encontre et les cybercriminels tiraient parti des différences entre les juridictions. Il y avait donc encore à faire pour harmoniser les régimes de protection de données. Pour parvenir à une véritable coopération dans ce domaine, une approche plus altruiste, au service de l'intérêt commun, semblait souhaitable. Dans un monde interconnecté, la cybersécurité ne pouvait être garantie dans un pays, tandis que les risques persistaient dans d'autres.

32. En raison des menaces d'usurpation d'identité, de vol de données, d'hameçonnage (phishing), de piratage des comptes personnels de messagerie et de cyberfraude, les consommateurs étaient réticents à adopter le commerce électronique et à placer leur confiance dans des services financiers numériques et mobiles. Les pays africains qui s'étaient dotés de politiques de cybersécurité ainsi que de lois sur la protection des données et les transactions électroniques, et qui avaient mis en place des équipes d'intervention informatique d'urgence, se heurtaient à des obstacles de taille, notamment à la méconnaissance de la cybercriminalité et à la mauvaise coordination des parties prenantes et des organes chargés de l'application des lois. De plus, la cybercriminalité était de plus en plus associée à d'autres crimes transnationaux comme le terrorisme, la traite d'êtres humains et le blanchiment d'argent. D'autres pays, qui reconnaissaient la compétence extraterritoriale dans les affaires de cybercriminalité, avaient été incapables d'obtenir des éléments de preuve électroniques en dehors de leurs frontières. Certains experts ont invité les organisations internationales à participer à la définition de principes juridiques communs pour surmonter ces problèmes. Un participant a indiqué que tous les pays avaient la possibilité de se référer au Guide sur la preuve électronique, élaboré par le Conseil de l'Europe à l'intention des fonctionnaires de police, des procureurs et des juges.

33. Plusieurs experts ont reconnu qu'il était difficile d'enquêter sur les crimes informatiques et de poursuivre leurs auteurs. Certains ont souligné les besoins de formation des responsables de l'application des lois et ont invité les organisations internationales concernées à en tenir compte dans leur action en faveur du commerce électronique et de réformes législatives. En vue d'une meilleure application de la législation, il était souhaitable que le répertoire de l'ONUDC sur la cybercriminalité bénéficie des contributions de différentes parties prenantes pour étendre sa portée et son champ d'application. Dans ce but, l'ONUDC était encouragé à accroître sa participation aux réunions multipartites sur la cyberlégislation et la cybersécurité. Un expert a proposé que la lutte contre l'utilisation des technologies à des fins criminelles relève aussi de la responsabilité des producteurs et des autorités de normalisation. De fait, il était d'autant plus difficile aux pouvoirs publics d'assurer la sécurité de grandes infrastructures d'information et de communication lorsque celles-ci appartenaient au secteur privé. Le niveau de responsabilité des entreprises pouvait être défini dans le cadre des partenariats public-privé, particulièrement importants pour la mise en place d'équipes d'intervention informatique d'urgence.

34. Un intervenant a estimé que le commerce électronique allait de plus en plus se caractériser par des communications interactives et ininterrompues entre les utilisateurs, les appareils (Internet des objets) et les services. La confiance prendrait alors une importance encore plus grande et l'intensification des échanges de données obligerait les parties prenantes à adapter leur comportement en conséquence. L'accès aux données personnelles par divers appareils et applications a conduit à une identification fragmentée et à un contrôle limité des protocoles d'échange de données par les consommateurs. Les services en ligne devenant incontournables et les renseignements personnels se monnayant de plus en plus, il importait que les parties prenantes (pouvoirs publics,

citoyens, consommateurs, employeurs et prestataires de services) se soucient davantage de protéger et de contrôler les données. La fragmentation s'expliquait aussi par les multiples identités que des personnes et des produits pouvaient avoir en ligne. Il faudrait examiner plus avant comment relier identités virtuelles et identités réelles.

35. Les consommateurs avaient besoin de savoir ce que valaient leurs données, en quoi elles étaient négociables, et comment elles étaient gérées. Pour utiliser Internet avec confiance, ils devaient aussi connaître les moyens dont ils disposaient pour assurer la protection de leurs données. Mieux informés, les consommateurs seraient moins exposés à la cybercriminalité et pourraient défendre plus activement leur droit à la vie. En fin de compte, les utilisateurs pourraient eux aussi tirer parti de leurs données personnelles.

36. Plusieurs experts ont invité la communauté internationale à continuer de sensibiliser les parties prenantes aux effets de la cybercriminalité, notamment à son lien avec d'autres formes de criminalité, afin de les rendre mieux à même de décider des données pouvant être divulguées et de la manière de les protéger. Il importait aussi de renforcer la coopération internationale en matière de cybercriminalité, par exemple, par l'harmonisation des régimes de protection des données. Actuellement, seules quelques instances internationales abordaient ces questions. La CNUCED pouvait accueillir des débats sur la protection des données et le respect de la vie privée en ligne.

F. Meilleures pratiques dans l'élaboration de cyberlégislations régionales

37. Les participants ont fait le point sur les mesures qui avaient été prises par divers groupements régionaux, la CNUCED et d'autres partenaires en vue de réformer le droit. Ils ont débattu des principaux obstacles à la mise en œuvre de lois compatibles, des meilleures pratiques et des enseignements tirés des expériences régionales.

38. À la faveur des activités menées dans plusieurs régions, la CNUCED avait constaté que l'harmonisation régionale se heurtait aux obstacles suivants:

a) Différences entre les pays sur le plan de la législation, des compétences, des ressources et de la situation politique;

b) Différences entre les régimes juridiques (droit civil ou *common law*);

c) Différences d'approche dans l'adoption des accords régionaux (approche contraignante/non contraignante);

d) Différences d'approche dans l'adoption et l'application des lois au niveau national.

39. La région de l'Association des Nations de l'Asie du Sud-Est peinait à participer au commerce électronique en raison de difficultés majeures, notamment: de réseaux à haut débit peu performants et aux coûts d'utilisation élevés; d'une diffusion insuffisante des moyens de paiement en ligne et d'une faible bancarisation, malgré des innovations; de moyens logistiques et de procédures douanières inefficaces; d'un manque de confiance à l'égard d'Internet, en partie dû aux taux élevés de cybercriminalité; des incertitudes en matière de règlement des différends; et de l'absence d'un organisme régional de défense du commerce électronique.

40. Dans la Communauté d'Afrique de l'Est (CAE), les cyberlégislations manquaient d'un environnement propice, notamment de bonnes infrastructures d'information et de communication. L'élaboration d'un cadre régional de cyberlégislation ayant été approuvée par le Conseil des Ministres, la CAE avait créé à cette fin, avec l'aide de la CNUCED, une équipe spéciale associant à la fois des représentants des pouvoirs législatif, exécutif et judiciaire, et des acteurs du secteur privé. Deux cadres, non contraignants, avaient été

adoptés. Le principal problème résidait dans le rythme de leur application au niveau national, qui n'était pas uniforme. Il était important de faire intervenir les bonnes personnes au moment opportun − d'abord, les responsables politiques pour les orientations générales, puis les technocrates pour le processus d'élaboration. Il fallait aussi renforcer les capacités, partager les expériences, continuer à surveiller la jurisprudence et aller plus loin dans la coopération internationale.

41. Plusieurs intervenants ont rappelé que le commerce électronique ne serait florissant que dans un environnement qui lui était propice. Dans la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO), les principaux obstacles étaient le manque de ressources et le non-respect des délais fixés par la Commission de la CEDEAO. Pour stimuler le commerce électronique, il fallait gagner la confiance des consommateurs.

42. Les pays arabes accusaient un retard par rapport aux pays développés dans l'adoption et l'application de cyberlégislations. Ils devaient se doter d'un cadre de référence pour les questions légales et réglementaires relatives à l'espace numérique, harmoniser leurs lois et leur terminologie, et définir clairement les rôles et les responsabilités de différentes institutions. L'adoption d'une législation exigeait aussi une collaboration plus étroite au niveau national. L'application des lois posait problème, tout comme l'absence de décisions de procédure et d'instruments de réglementation. Dans certains cas, les documents électroniques n'étaient pas pleinement reconnus.

43. Au vu des meilleures pratiques observées dans les différentes régions, il apparaissait qu'une ferme volonté politique de renforcer les cyberlégislations faisait défaut aux niveaux national et régional. Or, il était essentiel que les autorités législatives et réglementaires collaborent efficacement à ces deux niveaux pour que des lois soient adoptées et mises en œuvre − ce qui pouvait être facilité par la création d'un comité intergouvernemental de coordination. Le dialogue entre secteur public et secteur privé était tout aussi important. Des efforts devaient aussi être faits pour sensibiliser au processus de réforme de la cyberlégislation.

44. Afin que cette réforme soit menée à bien, les gouvernements devaient établir des feuilles de route détaillées et fixer des objectifs d'étape et des échéances, de manière à ce que leurs progrès soient plus facilement évalués et communiqués aux institutions régionales, aux donateurs et aux organisations internationales.

45. Plusieurs experts ont insisté sur la nécessité de renforcer les capacités, d'autres ont proposé que les ateliers techniques soient complétés par des réunions sur le commerce électronique et la cyberlégislation dans le but d'intéresser davantage les responsables politiques à ces questions. Ces initiatives pourraient faire naître une volonté politique et rattacher le commerce électronique au développement durable.

46. Plusieurs experts se sont dits favorables à l'organisation par la CNUCED de réunions sur le commerce électronique et la cyberlégislation, dans lesquelles les parties prenantes seraient plus largement représentées. Plusieurs experts ont aussi rappelé que la cyberlégislation était l'un des principaux piliers du commerce électronique.

47. Le secrétariat de la CNUCED a insisté sur la nécessité d'améliorer les statistiques et a encouragé les États membres à intégrer les questions liées au commerce électronique dans leurs enquêtes statistiques publiques. Des experts ont proposé que la CNUCED fasse l'inventaire des outils, programmes et études actuellement proposés par différentes organisations dans le domaine du commerce électronique. Un expert a recommandé que les cyberlégislations figurent dans des programmes d'études universitaires, qui pourraient être élaborés avec l'aide d'organisations internationales telles que la CNUCED.

G. Perspectives

48. Lors de la dernière séance informelle, les experts ont réfléchi à la manière dont les parties prenantes pourraient aider à renforcer les cyberlégislations dans les pays en développement et à promouvoir le commerce électronique international.

49. La cyberlégislation pouvait peut-être aider à lever les incertitudes juridiques, faire naître la confiance, encourager de meilleures pratiques et apporter des voies de recours, elle ne contribuait ni au développement technologique ni à l'innovation. À elle seule, la cyberlégislation ne favoriserait pas le commerce électronique ni ne stimulerait les échanges internationaux. Elle pouvait prévenir les pratiques discriminatoires, mais non pas être une garantie d'intégration ou influer sur la répartition des retombées du commerce électronique. La cyberlégislation devait être technologiquement neutre et, à ce titre, adaptable aux innovations futures. Elle devait faciliter le commerce, et non y faire obstacle, en proposant un cadre, en appliquant les principes de l'interopérabilité et en consacrant de bonnes pratiques.

50. Premier marché mondial du commerce électronique de détail, la Chine dispensait des enseignements précieux, par son expérience dans l'élaboration d'un cadre juridique et de politiques de plus large portée en faveur du commerce en ligne. Sa demande intérieure avait été si forte et son développement, si rapide, que les dispositions législatives et réglementaires n'avaient pas pu suivre, si bien que le pays rencontrait des difficultés pour réglementer les prestataires de services, protéger les consommateurs et effectuer des transactions internationales. Un projet de loi sur le commerce électronique devrait être adopté en 2018. Le Gouvernement chinois avait mis en place un plan d'action, appelé «Internet Plus», ainsi que des orientations stratégiques afin d'assimiler les nouveaux progrès technologiques, comme l'Internet mobile, l'informatique en nuage, les données massives et l'Internet des objets. Appuyée par des mesures déjà en place, la législation chercherait à instaurer un climat de confiance parmi les consommateurs et à mieux préparer les petites et moyennes entreprises au commerce en ligne, y compris dans les zones rurales. L'objectif était de stimuler le commerce électronique, national et international, en encourageant l'entreprenariat local et l'innovation.

51. En Ouganda, il avait fallu près d'une décennie pour jeter les bases juridiques d'une législation sur le commerce électronique. Adoptée en 2011, cette législation n'était cependant toujours pas dûment appliquée. Les décideurs, les responsables de l'application des lois et la société civile avaient mal accueilli et mal compris ses dispositions, ce qui avait compliqué les consultations et l'obtention d'un consensus. Le Gouvernement ougandais s'était notamment tourné vers la CNUCED pour l'aider à enrichir les connaissances des parties prenantes et faire en sorte que celles-ci les diffusent à leur tour. De plus, il avait créé un groupe de réflexion multisectoriel, chargé de donner des conseils sur la mise en œuvre de la cyberlégislation, et avait engagé une stratégie de sensibilisation du public, consistant à présenter aux parties prenantes (banquiers, assureurs, juges, agents de la force publique, professionnels de justice et opérateurs commerciaux), dans le cadre de réunions, les différents domaines techniques et juridiques dans lesquels leur collaboration était nécessaire pour l'application de la cyberlégislation.

52. Les experts ont constaté des chevauchements entre les cyberlégislations et le droit commercial international dans le domaine du commerce électronique. S'il était généralement entendu que le commerce électronique entrait dans le cadre des Accords de l'Organisation mondiale du commerce (OMC), cette dernière n'avait pu aller beaucoup plus loin. Le principe de neutralité technologique s'appliquant à la fourniture des services, les services de livraison électronique devraient être régis par les dispositions des accords généraux sur les services. Cependant, aucune classification ni aucune définition n'avaient encore été officiellement arrêtées dans le cadre du commerce international de services de

TIC et de services fondés sur les TIC; et un moratoire provisoire des droits de douane sur les transmissions électroniques était en place depuis 1998. Les dispositions actuelles de l'OMC sur le commerce des services pouvaient constituer un socle de principes et d'obligations propres à assurer la bonne gouvernance du commerce en ligne. Si les Accords de l'OMC avaient un caractère contraignant, aucune obligation n'était faite quant à la manière dont ils devaient être mis en œuvre. La CNUCED pouvait apporter sa contribution dans ce domaine en devenant un lieu d'échanges de bonnes pratiques dans ce domaine.

53. Aucune région n'était épargnée par les menaces informatiques, mais l'Afrique était particulièrement exposée. Faute d'infrastructures électroniques sûres et fiables et d'une cyberlégislation, elle était exclue de l'économie du savoir. Certaines sous-régions avaient déjà bien progressé dans l'harmonisation de la cyberlégislation, d'autres ne s'étaient pas encore attelées à cette tâche, et bon nombre d'activités dans le secteur des TIC échappaient à toute réglementation. Bien qu'elle doive encore être ratifiée par 15 pays avant d'entrer en vigueur, la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel (2014) a marqué une étape importante. Dans une approche qualitative, la création d'un cadre juridique de confiance exigeait d'anticiper les risques numériques, d'assurer l'application effective de la cyberlégislation et le bon fonctionnement des mécanismes de suivi et d'évaluation, ainsi que d'améliorer constamment l'environnement pour le rendre plus propice. Ce dernier point impliquait de hâter l'entrée en vigueur de la Convention et de transposer ses dispositions dans le droit interne. En plus de textes législatifs sur la protection des données, un expert a proposé qu'une commission soit chargée de contrôler leur application. Enfin, il était capital de renforcer les capacités de toutes les parties prenantes.

54. Plusieurs experts sont convenus que le commerce électronique avait un rôle essentiel à jouer pour parvenir à un développement économique qui profite à tous et que, si les lois types existantes, comme celles de la CNUDCI, étaient utiles, il fallait faire plus pour élaborer des lois types ou des lignes directrices concernant, par exemple, les voies de recours, la lutte contre les courriers indésirables, les responsabilités des prestataires de services, la taxation des transactions en ligne et l'informatique en nuage. Plus de recherches devaient aussi être consacrées à l'impact des cyberlégislations sur les consommateurs et les professionnels. Certains experts ont en outre proposé d'analyser plus attentivement le rôle des acteurs non étatiques, le secteur privé détenant de plus en plus des infrastructures et des informations essentielles. Les entreprises et les intermédiaires, les universitaires, les organisations non gouvernementales et les autres acteurs devraient être associés aux futurs débats sur la cyberlégislation.

55. Selon certains participants, des cyberlégislations efficaces étaient nécessaires, mais pas suffisantes pour faire progresser le commerce électronique dans les pays en développement. Le *Rapport 2015 sur l'économie de l'information* avait proposé un cadre de référence, couvrant huit domaines clefs, à partir duquel élaborer une stratégie nationale de commerce électronique. Le secrétariat de la CNUCED a indiqué aux experts que les pays pourraient être aidés dans cette entreprise dans le cadre du programme d'examen des politiques des TIC. La CNUCED pouvait aussi proposer des activités de formation et de renforcement des capacités en statistique, y compris dans le domaine de l'économie de l'information. De plus, le Système douanier automatisé (SYDONIA) pouvait contribuer à la facilitation du commerce par l'automatisation des procédures douanières, et la CNUCED proposait un programme de formation au commerce électronique destiné aux professionnels concernés.

56. Les organisations internationales pouvaient jouer un rôle important, notamment en renforçant durablement les capacités des législateurs dans les pays en développement, par exemple, en fournissant des services de conseil pendant le long processus de rédaction, d'adoption et d'application de la cyberlégislation. La communauté internationale pouvait

aussi encourager le dialogue entre les parties prenantes et aider à constituer des réseaux. Des experts ont demandé à la CNUCED de créer un forum de discussion en ligne pour intéresser davantage les responsables politiques à la réforme de la cyberlégislation.

57. Plusieurs experts ont rappelé qu'il faudrait rattacher l'examen décennal des textes issus du Sommet mondial sur la société de l'information (SMSI) aux débats sur les objectifs de développement durable proposés, de manière à ce que, à l'avenir, la croissance économique, notamment lorsqu'elle est fondée sur le commerce électronique, aille dans le sens d'un développement durable et de l'intégration sociale.

58. En conclusion, les experts ont indiqué que l'adoption d'une cyberlégislation devrait favoriser le commerce électronique, sans faire obstacle au commerce international. La législation n'étant pas suffisante à cette fin, elle devrait être complétée par d'autres mesures visant à créer un environnement propice. De nombreux pays en développement, surtout africains, devaient faire des progrès dans la rédaction, l'adoption, la mise en œuvre et le contrôle de l'application des cyberlégislations, et veiller à ce que ces législations soient conformes aux conventions internationales sur la cybersécurité et les transactions électroniques. Des transferts de connaissances s'imposaient pour permettre aux pays de faire respecter leurs lois de manière plus autonome. Les travaux législatifs futurs, destinés à libérer le potentiel du commerce électronique pour les pays en développement, devraient chercher à rendre l'économie de l'information profitable à tous. Ils s'inscriraient dans le cadre des objectifs de développement durable pour l'après-2015 ainsi que de l'examen et du suivi de l'application des textes issus du SMSI. Enfin, la CNUCED devrait continuer d'offrir un cadre aux discussions en cours et à l'échange de meilleures pratiques sur les questions de cyberlégislation.

II. Questions d'organisation

A. Élection du bureau

(Point 1 de l'ordre du jour)

59. À sa séance plénière d'ouverture, le 25 mars 2015, la réunion d'experts a élu M. Timo Kotilainen (Finlande) Président et M. Humberto Jiménez Vice-Président/Rapporteur.

B. Adoption de l'ordre du jour et organisation des travaux

(Point 2 de l'ordre du jour)

60. À sa séance plénière d'ouverture, la réunion d'experts a adopté l'ordre du jour provisoire, publié sous la cote TD/B/C.II/EM.5/1.

C. Résultat de la session

61. À sa séance plénière de clôture, le 27 mars 2015, la réunion d'experts a décidé que le Président établirait un résumé des débats.

D. Adoption du rapport de la réunion

(Point 4 de l'ordre du jour)

62. À sa séance plénière de clôture, la réunion d'experts a autorisé le Vice-Président/Rapporteur à établir, sous l'autorité du Président, le rapport final après la clôture de la session.

Annexe

Participation*

1. Les représentants des États membres de la CNUCED ci-après ont participé à la réunion d'experts:

Afghanistan
Algérie
Allemagne
Angola
Arabie saoudite
Argentine
Belgique
Bénin
Bhoutan
Brésil
Burkina Faso
Burundi
Cabo Verde
Cameroun
Canada
Chine
Côte d'Ivoire
Cuba
Égypte
Émirats arabes unis
Équateur
Espagne
États-Unis d'Amérique
Éthiopie
Finlande
France
Gambie
Ghana
Guatemala
Guinée
Guinée-Bissau
Hongrie
Inde
Indonésie
Japon
Jordanie
Kenya
Lesotho
Lettonie
Libéria
Libye
Madagascar
Mali
Maurice
Mauritanie
Mexique
Monténégro
Namibie
Niger
Nigéria
Oman
Ouganda
Panama
Paraguay
Philippines
Portugal

* La présente liste ne mentionne que les participants inscrits. La liste des participants porte la cote TD/B/C.II/EM.5/INF.1.

Qatar

République démocratique du Congo

République dominicaine

République tchèque

République-Unie de Tanzanie

Sénégal

Sierra Leone

Soudan

Suisse

Thaïlande

Togo

Trinité-et-Tobago

Tunisie

Turquie

Zambie

Zimbabwe

2. Les organismes intergouvernementaux ci-après étaient représentés à la session:

Communauté économique des États d'Afrique de l'Ouest

Fonds de l'Organisation de pays exportateurs de pétrole (OPEP) pour le développement international

Groupe des États d'Afrique, des Caraïbes et du Pacifique

Organisation de coopération et de développement économiques

Organisation internationale de la francophonie

Union européenne

3. Les organes, institutions et programmes des Nations Unies ci-après étaient représentés à la session:

Centre du commerce international

Forum sur la gouvernance d'Internet

Commission des Nations Unies pour le droit commercial international

4. Les institutions spécialisées et organisations apparentées ci-après étaient représentées à la session:

Banque mondiale

Organisation mondiale du commerce

Union internationale des télécommunications

Union postale universelle

5. Les organisations non gouvernementales ci-après étaient représentées à la session:

Catégorie générale

Consumers International

International Network for Standardization of Higher Education Degrees

Village Suisse ONG