Nations Unies TD/B/C.II/EM.5/2

Conférence des Nations Unies sur le commerce et le développement

Distr. générale
14 janvier 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 la 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
Point 3 de l'ordre du jour provisoire

La cyberlégislation et réglementation comme moyen de renforcer le commerce électronique: études de cas et enseignements tirés de l'expérience

Note du secrétariat de la CNUCED

Résumé

Les transactions électroniques revêtent une importance croissante pour les pouvoirs publics, les entreprises et les consommateurs dans la plupart des pays. Le commerce électronique se développe, créant de nombreuses possibilités, mais se heurte encore à l'obstacle majeur qu'est le manque de sécurité et de confiance. La fraude en ligne et les atteintes à la sécurité des données suscitent des inquiétudes grandissantes et appellent des réponses législatives et réglementaires adéquates, qui permettent de faire croître le commerce intérieur et extérieur. Il n'est cependant pas facile d'adopter un cadre juridique et réglementaire satisfaisant, étant donné la variété et la complexité des législations et réglementations et l'évolution rapide des technologies et des marchés. Les nouveaux modes de paiement et le recours croissant à l'informatique en nuage rendent plus urgent encore le besoin de progrès dans ce domaine.

La présente note porte sur les grandes questions juridiques dont il faut tenir compte pour faciliter le commerce électronique et améliorer la sécurité de la communication sur Internet en général. Elle passe brièvement en revue certaines des pratiques les plus indiquées pour surmonter les obstacles bien connus à l'élaboration et à l'application de la cyberlégislation, en prenant appui sur les activités que la CNUCED mène en liaison avec des groupements régionaux de pays en développement. On présente aussi dans cette note les résultats des travaux de la CNUCED sur les lois régissant actuellement ces aspects du commerce électronique, en soulignant les progrès accomplis et les lacunes à combler. On y réfléchit enfin aux moyens d'appliquer et de faire respecter efficacement les lois en

GE.15-00470 (F) 160215 170215
1500470

vigueur en tenant compte des nouvelles technologies disponibles sur Internet et les appareils mobiles. Les politiques devraient viser à garantir la compatibilité des législations et à renforcer les capacités des principales parties prenantes, notamment les autorités chargées de faire respecter les lois.

Table des matières

Page

I. Introduction 4

II. Tendances mondiales du commerce électronique 4

III. Questions juridiques clefs 7

A. Compatibilité des lois relatives aux signatures et aux contrats électroniques 8

B. Protection des consommateurs 10

C. Protection en ligne des données et de la vie privée 12

D. Lutte contre la cybercriminalité 13

E. Exemples de bonnes pratiques au niveau régional 15

IV. Recommandations et questions à examiner 16

I. Introduction

1. Les transformations intervenues dans le domaine des technologies de l'information et de la communication (TIC), en particulier le développement d'Internet dans la seconde moitié des années 1990 et, plus récemment, la grande diffusion des technologies pour appareils mobiles, sont telles que les incidences des TIC sur le commerce et le développement durable sont de plus en plus reconnues. Le commerce électronique est un domaine d'application important des TIC.

2. Il y a peu de temps encore, différents facteurs entravaient le commerce électronique dans beaucoup de pays. Les principaux obstacles au commerce électronique sont le caractère inadéquat des infrastructures informatiques et électriques, le développement insuffisant des marchés financiers, le manque de pouvoir d'achat, la méconnaissance des TIC et du commerce électronique de la part des consommateurs et des entreprises, et la faiblesse des cadres juridiques et réglementaires. Ces problèmes touchent particulièrement les pays à faible revenu, ainsi que les petites entreprises et les microentreprises.

3. Grâce à de nouvelles technologies, plates-formes de commerce électronique et solutions de paiement, certains de ces obstacles sont maintenant plus faciles à surmonter. Il importe donc que les États en développement mettent en place des cadres qui permettent aux entreprises et aux pouvoirs publics de pleinement tirer parti des possibilités offertes par différents appareils et technologies. La fraude en ligne et les atteintes à la sécurité des données préoccupent de plus en plus les consommateurs et les entreprises, et exigent que des mesures appropriées soient prises aux niveaux national et international.

4. La présente note a été établie conformément au mandat de la Réunion d'experts, qui consiste à examiner les domaines pertinents de la protection des consommateurs, notamment la protection des données relatives aux cartes de crédit et aux paiements et les règles applicables aux règlements, en tenant dûment compte des travaux complémentaires menés à l'OMC dans le cadre du Programme de travail sur le commerce électronique. Toujours au titre de ce mandat, la Réunion d'experts devrait identifier les meilleures pratiques en matière de cyberlégislation et de réglementation concernant le commerce électronique, ainsi que formuler des recommandations sur les moyens de mettre le cadre normatif, notamment la cyberlégislation, au service du commerce électronique.

5. La présente note, qui met à profit les recherches menées pour établir le *Rapport 2015 sur l'économie de l'information* (CNUCED, 2015), s'intéresse à quatre domaines juridiques: les transactions électroniques, la protection des consommateurs, la protection de la vie privée et des données, et la cybercriminalité. Elle présente d'abord les tendances récentes du commerce électronique à l'échelle mondiale. Elle recense ensuite les grandes questions juridiques à prendre en compte pour développer le commerce électronique dans les pays en développement et au niveau mondial. Elle évoque plusieurs études de cas et exemples de bonnes pratiques tirés des travaux de la CNUCED sur des groupements de pays en développement, notamment l'Association des nations de l'Asie du Sud-Est (ASEAN), la Communauté d'Afrique de l'Est (CAE), la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO), le Système économique latino-américain et caribéen et l'Association latino-américaine d'intégration. Elle soumet enfin une série de questions et de recommandations à l'examen de la Réunion d'experts.

II. Tendances mondiales du commerce électronique

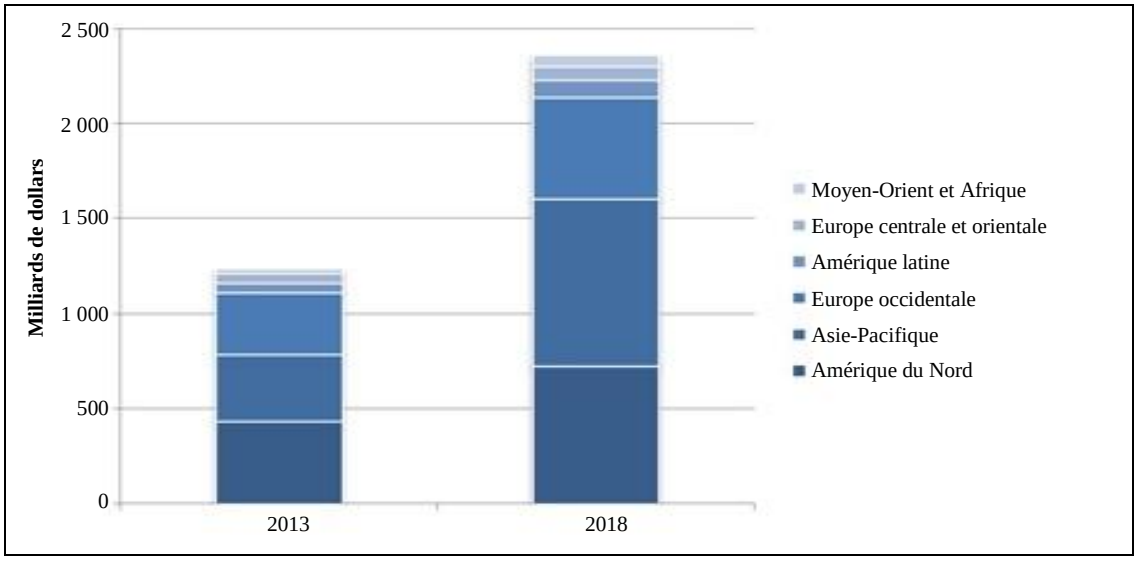
6. Le commerce électronique peut avoir plusieurs effets positifs, notamment ceux de renforcer la participation aux chaînes de valeur internationales, d'améliorer l'accès aux marchés et d'accroître l'efficacité, ainsi que de diminuer les coûts de transaction. Mais le

commerce électronique se répand lentement dans la plupart des pays en développement, après avoir été longtemps réservé à un groupe de pays et d'entreprises relativement restreint (CNUCED, 2010a).

7. À l'origine, le commerce électronique concernait essentiellement les grandes entreprises des pays développés, mais l'évolution des TIC tend à améliorer l'accès des entreprises des pays en développement à différentes formes de commerce électronique (CNUCED, 2015). La situation s'est beaucoup améliorée sur le plan de la connectivité, notamment grâce à l'usage répandu de la téléphonie mobile et des réseaux sociaux. Des applications, des plates-fornes et des services nouveaux rendent en outre le commerce électronique plus accessible et facile à utiliser, réduisant ainsi les obstacles à l'entrée. De même, les nouveaux modes de paiement multiplient les possibilités d'effectuer des transactions en ligne pour les entreprises aussi bien que les consommateurs. De plus en plus de sociétés de commerce électronique sont créées dans les pays en développement pour offrir des services adaptés aux besoins et aux exigences des utilisateurs locaux, ce qui aide à sensibiliser les entreprises et les consommateurs.

8. La grande majorité des recettes tirées du commerce électronique provient des transactions entre entreprises, c'est-à-dire entre fabricants et grossistes et entre grossistes et détaillants. La CNUCED estime que les recettes provenant de ces transactions s'élèvent à 15 200 milliards de dollars en 2013, contre 1 200 milliards de dollars provenant des transactions d'entreprise à consommateur (CNUCED, 2015). Ce dernier type de transactions, qui comprend aussi bien les ventes des entreprises exclusivement présentes en ligne que celles des détaillants et fabricants traditionnels qui se sont dotés d'un système de vente électronique, semblent connaître une croissance plus rapide. D'après la société eMarketer, les ventes d'entreprise à consommateur (B2C) devraient atteindre un montant de 2 400 milliards en 2018 (fig. 1). La croissance la plus forte devrait concerner la région Asie-Pacifique, dont la part de marché passerait de 28 à 37 %. Le Moyen-Orient et l'Afrique est la seule autre région dont la part de marché devrait augmenter − de 2,2 à 2,5 %. À l'inverse, la part totale de l'Europe occidentale et de l'Amérique du Nord devrait tomber de 61 à 53 %.

Figure 1
Ventes en ligne B2C: total mondial ventilé par région, 2013 et 2018
(En milliards de dollars)



Source: eMarketer.com, juillet 2014.

Note: Les données tiennent compte des commandes de produits et de services, ainsi que des réservations au titre de voyages d'agrément et de voyages d'affaires non gérés faites sur Internet, tous appareils et modes de paiement confondus.

9. Il est estimé que 1,1 milliard de personnes ont effectué au moins un achat en ligne en 2013, soit légèrement plus de 40 % de l'ensemble des utilisateurs d'Internet (voir tableau 1). L'Asie-Pacifique est la région comptant la plus grande proportion des consommateurs en ligne, à savoir 43 % (soit 460 millions de personnes), pourcentage qui devrait continuer de croître jusqu'en 2018. C'est en Afrique et au Moyen-Orient que le nombre de ces consommateurs devrait croître le plus entre 2013 et 2018.

Tableau 1
Nombre de personnes ayant effectué des achats en ligne, par région, 2013 et 2018

	Total (millions)		*Croissance 2013-2018 (%)*	*Proportion du total mondial (%)*	*Proportion de la population (%)*	*Proportion des utilisateurs d'Internet (%)*
	2013	*2018*		*2013*	*2013*	*2013*
Asie-Pacifique	460,3	782,4	70	42,6	14,9	42,1
Europe occidentale	182,3	210,2	15	16,9	49,0	64,0
Amérique du Nord	172,3	203,8	18	16,0	59,7	72,0
Afrique et Moyen-Orient	93,6	170,6	82	8,7	7,1	31,3
Amérique latine	84,7	139,3	64	7,8	18,6	28,2
Europe centrale et orientale	86,4	117,4	36	8,0	24,1	41,6
Total mondial	**1 079,6**	**1 623,7**	**50**	**100,0**	**15,2**	**41,3**

Source: eMarketer, juillet 2014.

10. Les cartes de crédit sont de loin le premier moyen de paiement utilisé dans le cadre du commerce électronique de détail (WorldPay, 2014). Il est cependant prévu qu'en 2017, les autres moyens de règlement compteront pour 59 % du total, dont 40 points de pourcentage pour les porte-monnaie électroniques. L'importance relative des différents moyens de paiement varie énormément d'une région à l'autre (tableau 2). En Amérique du Nord et en Europe, les cartes de crédit restent le moyen le plus utilisé, devant les porte-monnaie électroniques. Dans les pays en développement, on constate des variations considérables, mais les cartes de crédit comptent en général pour moins de la moitié du total des règlements. En Afrique et au Moyen-Orient, presque la moitié du montant total des transactions a été réglée à la livraison, ce qui s'explique en partie par la grande proportion de personnes sans compte en banque. En Inde, cette proportion est de 50 à 80 %. Le recours à la livraison contre remboursement peut freiner la croissance du commerce électronique, parce que certains clients ne règlent pas leur achat une fois le produit livré et qu'il y a un délai entre l'envoi du produit et le paiement.

11. Les paiements par appareil mobile ne représentent que 1 % de la valeur totale des règlements, chiffre qui devrait passer à 3 % d'ici à 2017. Cette proportion est cependant plus importante dans les pays où Internet n'est pas largement utilisé mais qui disposent de bons systèmes de paiement par appareil mobile. Dans plusieurs pays africains, ces systèmes sont l'infrastructure la plus viable pour le commerce électronique, étant donné le taux élevé d'exclusion financière, la rareté et le coût des lignes de téléphone fixes, et le coût des infrastructures nécessaires à l'utilisation de cartes de crédit (Innopay, 2012).

Tableau 2
Répartition de la valeur des transactions électroniques par moyen de paiement, selon la région, 2012
(En pourcentage)

Région	*Cartes de crédit*	*Porte-monnaie électroniques*	*Prélèvement automatique*	*Livraison contre remboursement*	*Virement bancaire*	*Autres moyens*
États-Unis d'Amérique et Canada	71	18	2	1	1	7
Europe	59	13	5	5	8	11
Amérique latine	47	10	4	8	13	18
Asie-Pacifique	37	23	1	11	14	14
Afrique et Moyen-Orient	34	5	0	48	3	10
Total mondial	**57**	**17**	**2**	**5**	**7**	**12**

Source: WorldPay, 2014.
Note: Les paiements par appareil mobile sont compris dans la catégorie «Autres moyens».

III. Questions juridiques clefs

12. Un cadre juridique approprié est essentiel pour accroître la confiance dans le commerce électronique et garantir la sécurité des échanges électroniques entre entreprises, consommateurs et autorités publiques. La mesure dans laquelle les régions et les pays ont adopté une législation adéquate et parviennent à l'appliquer et à la faire respecter varie considérablement. Les travaux de la CNUCED ont fait ressortir que les pays développés disposaient dans la plupart des cas de lois régissant les quatre aspects qui sont essentiels pour accroître la confiance des utilisateurs (transactions électroniques, protection des consommateurs, protection de la vie privée et des données, et cybercriminalité), contrairement aux pays de plusieurs régions (voir tableau 3).

Tableau 3
Proportion des pays disposant d'une législation sur le commerce électronique, par région, 2014
(En pourcentage)

	Pays (nombre)	*Législation sur les transactions électroniques (%)*	*Législation sur la protection des consommateurs (%)*	*Législation sur la protection de la vie privée et des données (%)*	*Législation sur la cybercriminalité (%)*
Pays développés	**42**	**97,6**	**85,7**	**97,6**	**83,3**
Pays en développement					
Afrique	**54**	**46,3**	**33,3**	**38,9**	**40,7**
Afrique de l'Est	18	38,9	16,7	27,8	50
Afrique centrale	9	22,2	22,2	22,2	11,1
Afrique du Nord	6	83,3	33,3	50	66,7
Afrique australe	5	60	40	20	40
Afrique de l'Ouest	16	50	56,3	62,5	37,5
Asie et Océanie	**48**	**72,9**	**37,5**	**29,2**	**56,3**
Asie de l'Est	4	75	50	25	50
Asie du Sud-Est	11	81,8	81,8	54,5	72,7
Asie du Sud	9	77,8	22,2	44,4	66,7
Asie occidentale	12	91,7	33,3	25	58,3

	Pays (nombre)	*Législation sur les transactions électroniques (%)*	*Législation sur la protection des consommateurs (%)*	*Législation sur la protection de la vie privée et des données (%)*	*Législation sur la cybercriminalité (%)*
Océanie	**12**	**41,7**	**8,3**	**0**	**33,3**
Amérique latine et Caraïbes	**33**	**81,8**	**54,5**	**48,5**	**63,6**
Amérique centrale	8	75	87,5	37,5	37,5
Amérique du Sud	12	83,3	75	66,7	75
Caraïbes	**13**	**84,6**	**15,4**	**38,5**	**69,2**
Pays en transition	**17**	**100**	**11,8**	**88,2**	**70,6**
Total	**194**	**74,7**	**47,4**	**55,2**	**60,3**

Source: CNUCED.

A. Compatibilité des lois relatives aux signatures et aux contrats électroniques

13. Le commerce en ligne, y compris les paiements électroniques, nécessite une équivalence juridique entre les opérations électroniques et traditionnelles, objectif premier des lois relatives aux transactions électroniques. Des lois de ce type ont déjà été adoptées par 143 pays, dont 102 pays en développement (CNUCED, 2015). Vingt-trois autres pays ont élaboré des projets de loi; restent neuf pays en développement dépourvus de toute législation en la matière et 18 pour lesquels il n'y a pas de données. En Asie, de même qu'en Amérique latine et dans les Caraïbes, quatre pays sur cinq ont déjà adopté des lois dans ce domaine, tandis que l'Afrique de l'Est et l'Afrique centrale sont les régions qui ont pris le plus de retard à cet égard.

14. Beaucoup de lois nationales dans ce domaine s'inspirent des normes législatives définies par la Commission des Nations Unies pour le droit commercial international (CNUDCI). Les dispositions de la Loi type de 1996 sur le commerce électronique (CNUDCI, 1999) ont ainsi été incorporées dans le droit interne de plus de 60 pays. De plus, 29 pays ont adopté des lois fondées sur la Loi type de 2001 sur les signatures électroniques (CNUDCI, 2002). Par ailleurs, 18 États ont signé la Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux et six États y ont adhéré ou l'ont ratifiée (CNUDCI, 2007). La Convention ne s'applique que sur le plan international, et seulement aux six États parties. Plusieurs États ont toutefois intégré tout ou partie de ses dispositions de fond dans leur législation nationale.

15. Les pays qui ont adopté les lois types ou la Convention sur l'utilisation de communications électroniques dans les contrats internationaux ont en commun certaines dispositions législatives concernant les contrats électroniques, ce qui facilite le commerce international. Ils souscrivent aux principes de la neutralité technologique, de la non-discrimination en matière de communications électroniques et de l'équivalence fonctionnelle. Malgré les progrès accomplis dans l'adoption de lois sur les transactions électroniques, trois grands problèmes subsistent.

16. Premièrement, plusieurs législations n'abordent que la question de la signature électronique (authentification) et négligent d'autres clauses contractuelles importantes, concernant notamment le moment et le lieu de l'expédition et de la réception, l'accusé de réception, l'adresse des parties et l'utilisation de systèmes de messagerie automatisés. De plus, la plupart des législations laissent de côté les problèmes d'ordre international, notamment la détermination de la législation applicable, qui est l'une des sources de

différend associées au commerce international. En outre, si plusieurs législations comportent des dispositions relatives à la reconnaissance internationale des signatures électroniques, ces dispositions ne sont souvent pas appliquées, car leur mise en œuvre nécessiterait un système de reconnaissance mutuelle qui n'est pas facile à mettre en place (Castellani, 2010).

17. Deuxièmement, les principes fondamentaux ne sont pas appliqués uniformément par tous les pays, notamment pour ce qui est de la neutralité technologique en matière de signatures électroniques. Certains pays ont adopté des lois sur les signatures électroniques qui privilégient tel ou tel type de technologie, notamment une infrastructure à clef publique. C'est le cas de certains États membres de la CEDEAO et de la Communauté d'États indépendants. Les États membres de cette dernière sont tenus de mettre en place des organes de certification qui créent des signatures numériques à l'aide de procédés cryptographiques. Certaines lois considèrent que seules les signatures ainsi produites ont valeur contraignante. Cela étant, il semblerait que les législations évoluent dans un sens favorable à la neutralité technologique. Ainsi, la Fédération de Russie a modifié sa législation en 2011 pour reconnaître toutes les formes de signatures électroniques et a adopté la Convention sur l'utilisation de communications électroniques dans les contrats internationaux, qui établit la reconnaissance internationale des signatures sur une base technologiquement neutre.

18. Certaines législations prévoient la création d'un organisme national de certification. À cause des ressources humaines et financières nécessaires à son fonctionnement, un organisme de ce type n'a cependant pas toujours été créé, notamment dans les pays en développement, ou ne l'a été qu'après un long délai. Il arrive alors que les transactions électroniques ne soient pas reconnues juridiquement, si une intervention de l'autorité nationale de certification est nécessaire à leur validité juridique. De surcroît, l'obligation d'utiliser un système cryptographique dans le cadre des transactions électroniques ou des services publics en ligne peut constituer un obstacle, par exemple en empêchant les soumissionnaires étrangers de participer aux marchés publics, sauf en cas de reconnaissance officielle de l'infrastructure à clef publique du pays concerné.

19. Les législations varient même entre les pays qui ont adopté des dispositions fondées sur les lois types de la CNUDCI ou d'autres textes uniformes, d'où des obstacles au commerce électronique intérieur et extérieur. Ainsi, les signatures électroniques ne doivent pas toujours répondre aux mêmes critères. Le cas de l'Union européenne (UE) est intéressant à cet égard. Ses États membres étaient tenus de mettre en œuvre la Directive 1999/93/CE sur un cadre communautaire pour les signatures électroniques, qui définit un cadre juridique grâce auquel les signatures électroniques et les services de certification sont juridiquement reconnus dans chaque État membre et d'un État membre à l'autre. Comme les régimes nationaux de mise en œuvre n'étaient pas harmonisés, le Parlement européen et le Conseil de l'UE ont adopté en juillet 2014 le Règlement sur l'identification électronique et les services de confiance pour les transactions électroniques. Ce texte est conforme au principe de neutralité technologique, n'énonçant pas de conditions qui ne pourraient être remplies que par tel ou tel type de technologie. Directement applicable dans tous les États membres de l'UE, il fixe les modalités de reconnaissance mutuelle des signatures électroniques. On peut également citer le cas de l'ASEAN, dont les États membres ont reconnu différents types de signatures (CNUCED, 2013a).

20. Le troisième problème, enfin, est que la capacité de faire respecter les lois en vigueur est souvent insuffisante, les juges et les juristes ayant souvent une connaissance et une expérience limitées des transactions électroniques. C'est pourquoi les entreprises peuvent hésiter à se lancer dans le commerce électronique, particulièrement dans les pays en développement.

B. Protection des consommateurs

21. Quelle que soit la forme de commerce, la protection des consommateurs vise à remédier aux asymétries entre entreprises et consommateurs. Sur Internet, le vendeur peut facilement dissimuler des informations importantes le concernant (identité, lieu de situation et renseignements influant sur sa crédibilité). Aussi ces asymétries sont-elles particulièrement marquées dans le cas du commerce électronique et les consommateurs, plus vulnérables à la tromperie et à la fraude. Mais les lois sur la protection des consommateurs sont aussi un moyen d'aider les entreprises à mieux comprendre les conditions à remplir pour effectuer des transactions électroniques dans tel ou tel pays. Ainsi, les lois, les politiques et les réglementations permettent à la fois de définir les droits des consommateurs et les pratiques commerciales à suivre, de lutter contre les comportements commerciaux frauduleux et trompeurs et d'aider les entreprises à élaborer un système d'autoréglementation (OCDE, n/d).

22. Malgré l'importance de la confiance des consommateurs pour les ventes en ligne d'entreprise à consommateur, un inventaire des législations sur la protection des consommateurs en vigueur dans le monde révèle que beaucoup de pays en développement et de pays en transition n'ont toujours pas adopté de lois traitant du commerce électronique (CNUCED, 2015). Des 119 pays pour lesquels des données sont disponibles, 90 (dont 56 pays en développement ou en transition) ont adopté des lois sur la protection des consommateurs ayant trait au commerce électronique. Pour 73 pays, il n'a pas été possible d'obtenir de données, ce qui pourrait indiquer que la protection des consommateurs en ligne n'y a pas été pleinement prise en compte.

23. En comparant les différentes régions, on constate que les lois protégeant les consommateurs en ligne sont particulièrement rares en Afrique, seuls 18 pays africains sur 54 en ayant adopté. Cette proportion est plus élevée en Amérique latine, où 16 pays sur 20 ont mis en place une législation pertinente. Il n'y a pas de données disponibles pour l'Océanie ni la plupart des pays en transition.

24. Il importe de veiller à ce que les consommateurs soient protégés lorsqu'ils achètent en ligne, qu'il s'agisse de transactions nationales ou internationales. Les différences entre les dispositions adoptées par les différents pays risquent d'entraver les transactions internationales. Elles peuvent concerner les droits et les obligations des consommateurs et des entreprises, les conditions de vente acceptables, les obligations relatives à la communication de l'information et les mécanismes internationaux de réparation applicables.

25. Au sein de l'Union européenne, par exemple, les entreprises doivent tenir compte de 28 législations différentes pour réaliser leurs transactions internationales. Elles doivent identifier les dispositions applicables dans les différents pays et assumer les frais associés à la traduction, aux conseils juridiques et à l'adaptation des contrats. Cela accroît les coûts et la complexité de leurs activités, ainsi que l'incertitude juridique. Dans le cadre d'une enquête de 2011 sur le commerce électronique international, 44 % des consommateurs ont indiqué que l'incertitude entourant leurs droits les avait dissuadés d'acheter dans d'autres pays de l'UE. Un tiers des consommateurs interrogés ont dit qu'ils envisageraient d'effectuer des achats en ligne dans un autre pays de l'UE si des règles européennes uniformes s'appliquaient, chose que seuls 7 % faisaient déjà (Commission européenne, 2011). Afin de remédier à cette situation, la Commission européenne a proposé d'établir un droit commun européen de la vente pour faciliter les transactions transfrontières sur le

Marché unique[1]. Cela permettrait aux commerçants de vendre leurs produits à des citoyens d'un autre pays de l'UE en respectant une série unique de règles contractuelles, qui représenteraient une autre possibilité à côté du droit national des contrats. Dans tout pays de l'UE, les parties à un contrat de vente pourraient choisir d'appliquer le droit commun européen de la vente en y consentant expressément.

26. L'application internationale des lois de protection des consommateurs pose aussi problème. Elle exige une coopération efficace entre les organismes nationaux compétents[2]. Certains pays ont créé des mécanismes de coopération semi-formels, chargés de coopérer sur le plan politique plutôt que juridique. Ainsi, le Réseau international de contrôle et de protection des consommateurs (RICPC) réunit des organismes publics qui s'occupent de l'application des lois relatives aux pratiques commerciales loyales et d'autres activités de protection de consommateurs. Il compte 56 pays et organisations membres, dont 24 pays en développement[3], et a pour principal objectif de trouver des moyens de prévenir et corriger les pratiques de commercialisation frauduleuses sur le plan international.

27. Le RICPC a élaboré l'initiative «econsumer.gov» pour mieux protéger les consommateurs et accroître leur confiance dans le commerce électronique. L'initiative permet aux particuliers de déposer leurs plaintes à l'aide d'un unique site Web (http://www.econsumer.gov). En 2014, 30 organismes nationaux y participaient, tous membres du RICPC. En 2013, le site Web a permis de recueillir 23 437 plaintes, dont beaucoup concernaient des transactions internationales[4].

28. Principal cadre de référence international pour la protection des consommateurs, les Lignes directrices régissant la protection des consommateurs dans le contexte du commerce électronique (Lignes directrices de l'OCDE) (OCDE, 2000) sont en cours de révision. Une fois révisées, elles tiendront compte des principes ayant trait au commerce électronique d'entreprise à consommateur qui ont été énoncés dans différents textes de l'OCDE depuis leur adoption en 1999. Les Lignes directrices étant destinées aux États membres de l'OCDE, certains États en développement souhaiteront peut-être les adapter à leurs besoins particuliers.

29. Au niveau mondial, l'ONU mène des consultations pour réviser les Principes directeurs des Nations Unies pour la protection du consommateur (CNUCED, 2001) compte tenu de l'évolution des marchés et des réglementations, notamment en ce qui concerne le commerce électronique, afin de bien cerner les besoins des pays en développement. Les Principes directeurs révisés pourraient être disponibles dès 2016. Les consultations portent notamment sur les sujets suivants: mise en place d'une protection effective non moins avantageuse que celle qui est déjà assurée pour les autres formes de commerce; droits et obligations des consommateurs et des entreprises; consommateurs vulnérables; applications mobiles; paiements; autres modes de règlement des différends; éducation et sensibilisation des consommateurs; protection des données et de la vie privée; droit applicable et juridiction compétente; coopération bilatérale, régionale et internationale.

[1] La communication à ce sujet est disponible à l'adresse http://eur-lex.europa.eu/legal-content/en/ALL/;ELX_SESSIONID=9kq3JrXb6922fTl6wCNCyJTyMZn3N6p8lYymnk4b9G32fR21QJhQ!715408534?uri=CELEX:52011DC0636 (page consultée le 5 janvier 2015).

[2] C'est ce qu'ont souligné des représentants de pays de l'ASEAN et d'Amérique latine dans le contexte de l'assistance apportée par la CNUCED; voir par exemple CNUCED (2013a).

[3] Voir https://icpen.org/ (site consulté le 5 janvier 2015).

[4] Voir http://www.econsumer.gov/francais/resources/trends.shtm (site consulté le 5 janvier 2015).

C. Protection en ligne des données et de la vie privée

30. Dans l'économie mondiale numérique d'aujourd'hui, les données à caractère personnel alimentent une grande partie des activités commerciales sur Internet. Tous les jours, d'énormes quantités de données sont transmises, recueillies et stockées en ligne, ce qui est rendu possible par l'amélioration des capacités de calcul informatique et de communication. Dans ce contexte, gouvernements, entreprises et consommateurs s'inquiètent de plus en plus de la sécurité de l'information. Compte tenu du développement des services d'informatique en nuage, qui sont fournis par-delà les frontières, et de la multiplication des atteintes à la sécurité des données, il est plus important que jamais d'adopter des politiques adéquates (CNUCED, 2013b). Les analyses de données massives visant à comprendre et à influencer le comportement des consommateurs pour augmenter les profits risquent d'aviver encore les inquiétudes.

31. Selon une source, plus de 2 100 incidents ont été signalés en 2013 et ont abouti à la divulgation de quelque 822 millions de dossiers (Risk Based Security, 2014). Lors d'un incident majeur, pas moins de 152 millions de noms de clients, mots de passe, numéros de carte de débit ou de crédit et autres renseignements concernant des commandes ont été divulgués. C'est le secteur privé qui a été le plus souvent ciblé (53 % des cas), devant les services publics (19 % des cas). Environ 60 % des incidents étaient dus à des piratages[5]. Les États-Unis ont été de loin le pays le plus visé, ayant été ciblé dans plus de la moitié des cas connus. Les données le plus fréquemment divulguées sont les mots de passe, les noms, les adresses électroniques et les identifiants.

32. En novembre 2014, 105 pays (dont 65 pays en développement) disposaient de lois pour garantir la protection des données et de la vie privée (CNUCED, 2015). Trente-quatre autres pays en développement avaient élaboré des projets de texte en attente d'adoption. Dans ce domaine, la proportion de pays disposant d'une législation pertinente est du même ordre en Asie et en Afrique, à savoir moins de 40 %.

33. Il faut aussi que les entreprises adoptent des politiques pour veiller à la sécurité des données, mettre en place des garanties techniques, élaborer des plans d'action en cas d'incident de sécurité et prévenir les pratiques frauduleuses, trompeuses et déloyales. Les lois sur la protection de la vie privée et des données étant encore à un stade embryonnaire en Afrique subsaharienne, certaines entreprises y ont pris l'initiative d'adopter des pratiques exemplaires et normes de sécurité définies au niveau international (voir encadré 1). Lorsque la protection de la vie privée et des données est difficile à assurer en raison du modèle de contenu utilisé, il peut être nécessaire que les prestataires de services prennent des mesures supplémentaires pour sensibiliser les acheteurs et les vendeurs aux moyens de déceler les tentatives de fraude et de s'en prémunir.

Encadré 1

Mesures prises par des entreprises en Afrique de l'Est pour protéger les données et la vie privée

Dans le contexte du commerce électronique qui commence à se développer en Afrique subsaharienne, la plupart des atteintes à la sécurité des données concernent jusqu'à maintenant les distributeurs automatiques et les terminaux points de vente non connectés à Internet. Dans certains cas, un appareil a été utilisé pour enregistrer les données relatives aux cartes de paiement. Des cas de fraude en ligne se produisent également et leur fréquence ne pourra qu'augmenter en même temps que le nombre de consommateurs qui effectuent des transactions électroniques. Plusieurs sites de commerce électronique ont été dotés de mécanismes visant à réduire les risques de fraude.

[5] On entend ici par «piratage» l'accès (souhaité ou non) à un ordinateur aux fins de consulter, copier ou créer des données (en laissant une trace), sans intention de détruire des données ou d'endommager l'ordinateur.

Le site de petites annonces OLX, qui est utilisé au Kenya et dans beaucoup d'autres pays, applique les principes de la «sphère de sécurité» pour la protection de la vie privée (relatifs à la notification, au choix, au transfert ultérieur, à la sécurité, à l'intégrité des données, à l'accès et à la mise en œuvre). Les conditions d'utilisation du site précisent les modalités de collecte, d'utilisation et de partage des données, ainsi que les mesures prises pour protéger les données des utilisateurs. Les utilisateurs qui soupçonnent que leur vie privée a été violée ou autrement compromise sont invités à en faire état au moyen d'un formulaire relevant les problèmes juridiques.

L'entreprise 3G Direct Pay offre un système de paiement en ligne utilisé par plus de 300 agences de voyages et voyagistes dans toute l'Afrique de l'Est. Son approche de la sécurité des données est semblable à celle qui est suivie par les banques. Servant à traiter les règlements par carte bancaire, son système utilise des données confidentielles qui, si elles sont volées, permettent d'effectuer des paiements sans le consentement du titulaire de la carte. Pour atténuer ce risque, 3G Direct Pay a introduit une série de dispositifs de sécurité pour encrypter et protéger les données tout au long de la chaîne de traitement, conformément aux critères de niveau 1 définis dans la Norme de sécurité des données de l'industrie des cartes de paiement. De plus, l'entreprise surveille activement l'utilisation des cartes pour déceler et prévenir les tentatives de fraude.

Au titre de sa politique de confidentialité, le service généraliste de petites annonces Zoom Tanzania s'engage à ne jamais partager d'informations à caractère personnel, sauf en cas d'obligation légale ou d'autorisation expresse de la part de l'utilisateur. Le modèle d'activité de l'entreprise est fondé sur l'élaboration de contenus par les utilisateurs et la vente d'espaces publicitaires au moyen d'un réseau interne, grâce auquel les publicités sont diffusées auprès des utilisateurs sans compromettre les données personnelles.

Source: CNUCED, 2015.

34. Les principaux cadres de référence internationaux pour la protection de la vie privée et des données sont les Lignes directrices de l'OCDE, la directive de l'UE sur la protection des données et le cadre pour la protection de la vie privée de l'Association de coopération économique Asie-Pacifique. Si les principes de base font l'objet d'un large consensus, ce n'est pas le cas des modalités de leur application. Certains régimes de protection des données s'appliquent uniformément à tous ceux qui utilisent des données personnelles. D'autres prévoient des règles différentes pour certains secteurs d'activité (par exemple, la santé), certains types d'entité (par exemple, les autorités publiques) ou certaines catégories de données (par exemple, les données ayant trait à des enfants). Dans ces cas, certains secteurs ne sont pas soumis aux règles en question.

35. Une distinction peut être opérée entre les régimes qui reposent essentiellement sur des procédures de contrôle engagées suite à des plaintes de particuliers, ou de groupes les représentant, et ceux qui confient des pouvoirs de contrôle à un organisme spécialisé, qui est chargé d'exercer une surveillance continue sur le traitement des données personnelles. Pour les pays en développement, une difficulté supplémentaire consiste à créer un organisme de réglementation.

D. Lutte contre la cybercriminalité

36. Quel que soit leur degré de développement, les pays sont de plus en plus préoccupés par la cybercriminalité, qui touche aussi bien les vendeurs que les acheteurs. Il est estimé qu'en 2012, les fournisseurs ont enregistré un manque à gagner de 3,5 milliards de dollars à cause de la fraude en ligne (CyberSource, 2013). En Europe, les formes de fraude qui sont signalées le plus fréquemment par le Réseau des Centres européens des consommateurs

concernent des sites Web frauduleux, des ventes de voitures d'occasion en ligne et des produits de contrefaçon. Dans tous ces cas de figure, les cybercriminels font miroiter au consommateur des produits bon marché ou gratuits afin de lui extorquer des fonds, le plus souvent au moyen d'un virement. Dans les pays en développement, le nombre de cas de fraude a également augmenté considérablement. En Amérique latine, par exemple, le commerce électronique frauduleux porte sur un montant total de 430 millions de dollars[6]; en Afrique, la cybercriminalité coûte au Kenya, au Nigéria et à l'Afrique du Sud des sommes estimées respectivement à 36 millions, 200 millions et 573 millions de dollars (International Data Group Connect, 2012).

37. Cela met en lumière les risques auxquels sont exposés les consommateurs en ligne. Certaines infractions sont commises sur Internet depuis bon nombre d'années, mais elles se sont rapidement multipliées et diffusées à travers le monde. Les cybercriminels peuvent s'attaquer à un grand nombre de personnes dans différents pays sans même quitter leur domicile. Ils peuvent communiquer par l'intermédiaire de compagnies téléphoniques locales, d'opérateurs internationaux, de fournisseurs d'accès Internet et de réseaux sans fil et satellitaires, en passant par plusieurs ordinateurs situés dans différents pays, avant d'attaquer un système en particulier. Les éléments de preuve peuvent être enregistrés sur un ordinateur situé dans un pays autre que celui d'où l'infraction a été commise.

38. La cybercriminalité peut cibler des ordinateurs portables, des tablettes, des téléphones portables ou des réseaux entiers. Parmi les différents secteurs du commerce électronique, ce sont les commerçants dont les produits sont achetés au moyen d'appareils mobiles qui subissent les pertes les plus importantes en pourcentage du chiffre d'affaires (LexisNexis, 2013). Cela est particulièrement problématique pour les pays en développement où le commerce et les paiements électroniques reposent avant tout sur les téléphones mobiles. De surcroît, les cybercriminels ciblent de plus en plus souvent les pays en développement, en premier lieu parce que la législation y est appliquée moins rigoureusement. D'après une étude, le pays le plus touché par la cybercriminalité serait la Fédération de Russie, suivie de la Chine, du Brésil, du Nigéria et du Viet Nam (*Time*, 2014).

39. Le nombre de pays ayant adopté une cyberlégislation augmente rapidement: en novembre 2014, il s'élevait à 117 (dont 82 pays en développement ou en transition), et des projets de loi étaient en cours d'adoption dans 26 pays (CNUCED, 2015). Plus de 30 pays ne disposaient cependant d'aucune cyberlégislation. L'Afrique est la région avec le plus grand nombre de pays se trouvant dans ce cas.

40. L'instrument international le plus important dans ce domaine est la Convention sur la cybercriminalité (2001) du Conseil de l'Europe. Depuis, des instruments ont été adoptés par des pays en développement, notamment la Loi type du Commonwealth sur les crimes liés aux ordinateurs (2002) et la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel, adoptée en juin 2014. Des textes ont également été adoptés au niveau européen[7].

41. Les pays en développement ont plusieurs difficultés à surmonter, notamment le fait qu'ils n'ont pas les capacités et les infrastructures nécessaires pour répondre efficacement aux cyberattaques. La cybercriminalité pose des problèmes complexes au niveau international en matière d'application des lois et de compétence juridictionnelle. Il faut faire des efforts, en particulier, pour faire respecter les lois et renforcer les capacités des équipes d'intervention d'urgence en matière de sécurité informatique. La coordination et la

[6] Voir http://prensa.lacnic.net/news/en/feb2014_en/study-on-cybercrime-in-the-lac-region-e-commerce-fraud-doubles (page consultée le 7 janvier 2015).

[7] Voir OCDE (2002) et la directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information, disponible à l'adresse http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:FR:PDF (page consultée le 8 janvier 2015).

coopération internationales sont cruciales pour créer un environnement économique sûr, qui favorise une plus grande réactivité et un meilleur partage de l'information, de façon à permettre aux pays de réagir rapidement et efficacement aux actes de cybercriminalité.

E. Exemples de bonnes pratiques au niveau régional

42. Des régions en développement qui en sont à différents stades de l'élaboration d'une cyberlégislation ont considérablement progressé dans ce processus, en suivant différentes approches. Les exemples suivants montrent qu'il est nécessaire, pour réussir à adopter et à appliquer des lois de plus en plus complexes, de renforcer la coordination et la collaboration entre les organismes de réglementation et de contrôle aux niveaux national et régional, ainsi que d'entretenir un dialogue étroit entre les secteurs public et privé.

43. L'Association des nations de l'Asie du Sud-Est, la CAE et différents groupes régionaux d'Amérique latine ont bénéficié du Programme de la CNUCED sur le commerce électronique et la réforme de la cyberlégislation. Il y a quelques années, la dimension juridique de l'économie de l'information, y compris les lois sur le commerce électronique, représentait pour eux un territoire inconnu. Aujourd'hui, les questions relatives aux TIC sont intégrées dans leurs politiques de développement, qui sont assorties des cadres juridiques et réglementaires voulus, élaborés conformément aux normes et pratiques internationales. Selon les bénéficiaires du Programme, cette évolution est le fruit des activités de sensibilisation et de renforcement des capacités, ainsi que des efforts déployés sans interruption pour suivre le processus de réforme (voir l'évaluation externe réalisée dans Balestrieri, 2011).

44. En 2004, l'Association des nations de l'Asie du Sud-Est (ASEAN) est devenue le premier groupement de pays en développement à établir un cadre juridique pour le commerce électronique harmonisé à l'échelle régionale. Définissant les objectifs et les principes communs d'une infrastructure juridique qui favorise l'intégration économique régionale par différentes mesures favorables à la croissance, ce cadre fait des TIC un outil essentiel d'intégration sociale et économique. L'élaboration du cadre a été facilitée par un projet conjoint entre l'agence australienne AusAID et l'ASEAN, qui a amené les représentants des pays membres à se réunir régulièrement pour s'accorder sur les éléments à harmoniser. La CNUCED a aidé le Cambodge et la République démocratique populaire lao à élaborer leur législation. En 2008 et en 2013, elle a examiné l'état d'avancement de l'harmonisation législative dans l'ASEAN (CNUCED, 2013a). À l'issue de cet examen, elle a notamment recommandé de poursuivre l'harmonisation des éléments intéressant la juridiction de plusieurs pays, de façon à améliorer la coopération entre les autorités de réglementation et les organismes publics chargés de faire respecter les lois.

45. L'harmonisation des transactions internationales faciliterait l'application des lois au niveau international dans divers domaines: a) validité des signatures électroniques[8]: reconnaissance mutuelle des transactions conclues au moyen d'une signature électronique; b) protection des consommateurs: conclusion d'un accord entre les autorités nationales compétentes, assorti de moyens d'enquête et de renvoi appropriés, et adhésion au RICPC, en vue de commencer à améliorer la coopération régionale; c) lutte contre la cybercriminalité: créer un centre commun de formation et d'information et établir des points de contact nationaux joignables en permanence.

[8] L'ASEAN a déjà mené des travaux préliminaires sur la question, ayant notamment élaboré un mécanisme pilote pour Singapour et la Thaïlande en 2007.

46. Dans la CAE, les États membres ont estimé qu'il était essentiel de créer un cadre juridique et réglementaire adéquat pour mettre en œuvre efficacement les stratégies relatives aux services publics en ligne et au commerce électronique aux niveaux national et régional. Avec l'aide de la CNUCED, la CAE a établi l'Équipe spéciale pour la cyberlégislation, composée d'experts des États membres. Depuis 2007, la CNUCED associe formation et conseils juridiques pour faire mieux connaître les questions de droit et de politique générale liées au commerce électronique. Une série de réunions consultatives a permis de déterminer les grands principes de l'harmonisation de la cyberlégislation et d'élaborer deux documents cadres abordant différentes questions. Il importait de ne pas se contenter d'une loi type et d'élaborer un texte de base que l'on pourra adapter pour tenir compte de la complexité croissante des TIC, qui rend nécessaire l'adoption de nouvelles règles conformes aux normes déjà codifiées.

47. La détermination dont ont fait preuve les membres de la CAE qui ont participé à ce processus a été cruciale pour entretenir la dynamique de réforme au niveau national. En Ouganda, les autorités nationales et des acteurs du secteur privé n'ont cessé de contribuer au processus de réforme législative, dont l'aboutissement suscitait un intérêt croissant.

48. Des institutions politiques régionales, telles que l'Assemblée législative de l'Afrique de l'Est, des associations de parties prenantes, telles que l'East African Business Council et l'East African Law Society, et des organismes internationaux, tels que la CNUDCI, la CNUCED et la Commission économique pour l'Afrique, ont été étroitement associés aux processus de rédaction et d'harmonisation des textes. Afin de mettre en œuvre les recommandations formulées dans les documents cadres I et II, les États membres de la CAE ont présenté une liste détaillée d'activités de formation et de sensibilisation destinées à certains publics clefs: parlementaires, juristes, autorités de réglementation, forces de police et acteurs du secteur privé. De grands progrès ont été accomplis.

49. En Amérique latine et dans les Caraïbes, une série de 12 ateliers régionaux de renforcement des capacités a été organisée à l'intention de 1 100 fonctionnaires[9], de façon à obtenir un effet multiplicateur et d'élargir le public initié aux aspects juridiques du commerce électronique. La CNUCED a examiné les progrès réalisés dans ses études comparatives sur la région (CNUCED, 2010b, 2010c)[10]. C'était l'occasion pour les participants d'approfondir leur connaissance des questions juridiques liées au commerce électronique, de partager leurs expériences, de coordonner leurs efforts d'harmonisation régionale et de sensibiliser les autorités à des questions intéressant leur pays. Le capital humain est essentiel au renforcement des capacités institutionnelles.

IV. Recommandations et questions à examiner

50. Les achats et les ventes en ligne posent des problèmes juridiques auxquels doivent s'attaquer aussi bien les pouvoirs publics que les acteurs concernés du secteur. Même dans les régions développées où les législations ont été harmonisées dans une certaine mesure, par exemple l'Union européenne, les différences entre les obligations juridiques nationales peuvent entraver le commerce électronique. Si de nombreuses régions ont accompli des progrès considérables dans l'adoption de lois pertinentes et, jusqu'à un certain point, dans l'harmonisation législative, il faut encore aligner les lois sur les principaux instruments juridiques internationaux pour favoriser le commerce électronique international. En outre,

[9] Organisés suivant les méthodes du programme TrainforTrade, les ateliers permettaient aux participants d'utiliser des outils de formation à distance, d'accéder à un forum en ligne où des experts traitaient en temps réel de questions de cyberlégislation et de partager des données d'expérience.

[10] Une étude mise à jour sera publiée en 2015.

plusieurs États, notamment des pays en développement, doivent encore adopter des lois fondamentales dans un certain nombre de domaines. Pour ce faire, ils devraient assurer la coordination entre les institutions s'occupant de la législation dans les domaines du commerce électronique, de l'informatique en nuage et des services administratifs en ligne, afin d'adopter des principes clefs propres à faciliter la prestation de ces différents types de services. Dans les pays en développement, le prochain défi qui attend les pouvoirs publics sera de faire respecter les lois aux niveaux national et international.

51. Les pays en développement devraient chercher à obtenir une assistance de la part des communautés d'intégration régionale et de leurs partenaires de développement afin de veiller à la compatibilité des lois et de favoriser le commerce électronique international. Il convient aussi de mettre en place des programmes de renforcement des capacités à long terme pour faire respecter les lois et promouvoir ainsi le commerce électronique.

52. Les experts devraient sans doute examiner les questions évoquées dans le présent document, qui concernent avant tout des faits de portée régionale, en tenant compte des processus étroitement liés qui sont menés, notamment, sous les auspices de l'OMC, de l'OCDE et de l'ONU.

53. Les cinq recommandations présentées ci-dessous portent sur des questions qui influent aujourd'hui sur le développement du commerce électronique, particulièrement dans les pays en développement. Les participants à la réunion souhaiteront peut-être réfléchir aux moyens de les mettre en œuvre et de favoriser la coordination des institutions régionales et internationales qui aident les pays à élaborer et à appliquer leur cyberlégislation.

54. **Harmoniser les lois sur les transactions électroniques:** L'harmonisation régionale et mondiale des transactions électroniques est l'un des principaux enjeux associés à l'utilisation accrue des technologies électroniques par les pouvoirs publics, les entreprises et les citoyens. Lorsqu'il élabore ou révise les lois sur le commerce électronique, le législateur devrait tenir compte des législations des autres pays de la région et de ses partenaires commerciaux pour veiller à la compatibilité des systèmes juridiques et des politiques commerciales. La reconnaissance juridique des signatures électroniques, les contrats électroniques et les questions de preuve doivent être envisagés dans une perspective non seulement nationale, mais également internationale.

55. Ces dix dernières années, plusieurs régions ont fait des progrès dans l'harmonisation législative. Différentes normes sont cependant utilisées et il reste donc nécessaire de rendre les lois plus compatibles au niveau international. La Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux peut contribuer à l'harmonisation législative. Elle propose un ensemble de dispositions législatives essentielles qui favorisent le commerce électronique international. Les pays devraient envisager d'aligner leurs lois relatives aux transactions électroniques sur les dispositions de la Convention. En adhérant à celle-ci, ils favoriseraient l'harmonisation régionale et internationale, notamment la validité transfrontalière des signatures électroniques, car la Convention énonce des principes qui pourraient servir de base à un système de reconnaissance mutuelle. La Convention reprend en les révisant certaines dispositions des lois types de la CNUDCI, notamment celles sur le lieu de situation des parties, le moment et le lieu de l'expédition et de la réception, et l'équivalence fonctionnelle des signatures. D'autres dispositions sont entièrement nouvelles, notamment celles qui concernent l'utilisation de systèmes de messagerie automatisés ou les invitations à l'offre. La Convention définit en outre des dispositions fondamentales sur les transactions électroniques afin de garantir l'harmonisation régionale et internationale. Certains pays ont déjà modifié leur législation pour y incorporer les dispositions de fond de la Convention.

56. **Rationaliser les politiques de protection des consommateurs:** Les différences entre les lois nationales sur la protection des consommateurs font obstacle au commerce électronique international. Différents groupements régionaux s'efforcent d'harmoniser celles de ces lois qui ont trait au commerce électronique.

57. Les pays qui élaborent ou révisent leurs lois sur la protection des consommateurs devraient envisager de les aligner sur les Principes directeurs des Nations Unies pour la protection du consommateur et les Lignes directrices de l'OCDE, pour contribuer à harmoniser les législations et accroître la confiance des consommateurs dans le commerce électronique.

58. Il est nécessaire de créer des organismes de protection des consommateurs dans plusieurs pays en développement et de renforcer ceux qui existent déjà dans les autres. De plus, la mise en œuvre de mécanismes régionaux pour le dépôt de plaintes en ligne et l'application des lois faciliterait le commerce électronique international. À cette fin, il faudrait que les organismes de protection des consommateurs de chaque région adoptent un accord et des mécanismes d'enquête et de renvoi. En collaborant dans le cadre de réseaux tels que le RICPC, les organismes compétents peuvent plus facilement suivre l'évolution de la situation juridique aux niveaux régional et international, partager des données d'expérience et trouver des solutions aux problèmes des consommateurs en ligne.

59. Il est également recommandé de recourir à des mécanismes non judiciaires de règlement des différends et de réparation qui soient peu coûteux et faciles à utiliser. Certains des mécanismes les plus efficaces reposent sur l'action d'organismes d'autoréglementation, d'autorités de contrôle, de médiateurs ou d'autres entités. Par ailleurs, la création de labels de confiance, tels que le label «eConfianza[11]» créé par l'Instituto Latinoamericano de Comercio Electrónico (eInstituto), est une possibilité qui mérite d'être étudiée. L'organisation sans but lucratif eInstituto a publié un code de bonnes pratiques afin d'aider les entreprises à lancer leurs activités en ligne en répondant bien aux besoins des consommateurs. Elle a également créé un outil en ligne pour le règlement des différends, intitulé «Pactanda»[12].

60. **Rationaliser les lois sur la protection des données et la cybercriminalité:** Les pays ne devraient pas agir isolément lorsqu'ils élaborent et adoptent un cadre juridique pour la protection des données personnelles et la lutte contre la cybercriminalité afin de renforcer la confiance dans l'utilisation d'Internet. Les lois et les politiques doivent être harmonisées aux niveaux régional et international. L'établissement de normes minimales aide les pays à se coordonner entre eux pour concevoir et appliquer leur législation et à renforcer les institutions chargées de la faire respecter.

61. La création d'un organisme de réglementation efficace s'occupant de la protection des données peut représenter une tâche difficile d'un point de vue aussi bien financier que politique. Des enseignements peuvent être tirés du secteur des télécommunications, dans lequel les organismes de réglementation sont largement reconnus comme une composante essentielle d'un régime réglementaire efficace. Répartir les fonctions de réglementation entre les organismes chargés de la protection des données et ceux chargés de la protection des consommateurs pourrait être un moyen de réduire les coûts.

62. Dans le domaine de la lutte contre la cybercriminalité, il faut mettre en place des cadres complets pour la coopération, la sensibilisation et l'application de la législation. Même pour enquêter sur une seule communication, il peut être nécessaire de faire coopérer les organismes (publics ou privés) chargés de faire respecter la législation dans différents pays, la répression des infractions étant en général limitée au territoire national. L'un des éléments d'une coopération régionale dans ce domaine peut être la création d'un centre commun de formation et d'information et l'établissement de points de contact nationaux joignables en permanence.

[11] Voir www.econfianza.org (site consulté le 9 janvier 2015).

[12] Disponible à l'adresse www.pactanda.com (site consulté le 9 janvier 2015).

63. Il convient d'associer différentes mesures de sécurité − d'ordre matériel, virtuel ou administratif − pour protéger les données contre les actes de malveillance. Pour mettre en place un dispositif de sécurité approprié, il faut tenir compte de la nature des données communiquées, des besoins des différentes personnes concernées, de l'entité qui traite les données personnelles et même de la société en général. De plus en plus, les décideurs reconnaissent qu'Internet est à la fois une infrastructure nationale cruciale, dont dépend une proportion croissante des activités économiques et sociales, et un facteur de vulnérabilité. Ils devraient s'attacher tout particulièrement à prendre en compte cette double nature et à mettre en œuvre des mesures de sécurité adéquates, allant de l'adoption de lois sur la cybercriminalité à la création d'équipes informatiques chargées d'intervenir en cas d'urgence ou en cas d'incident. En outre, ils devraient nouer des partenariats public-privé pour tirer parti des points forts du secteur privé et de son action contre les menaces liées aux TIC.

64. **Renforcer les capacités du législateur et de l'appareil judiciaire:** Dans beaucoup de pays en développement, il faut former le personnel judiciaire à la cyberlégislation. Les problèmes juridiques relatifs au commerce électronique sont encore relativement nouveaux. Plusieurs organisations internationales et régionales, telles que le Secrétariat du Commonwealth, l'Union internationale des télécommunications, la CNUDCI, la CNUCED, l'Office des Nations Unies contre la drogue et le crime et le Conseil de l'Europe peuvent apporter une assistance aux pays et aux régions dans différents domaines juridiques. Ces organismes collaborent de plus en plus pour augmenter l'impact de leurs activités (voir encadré 2).

Encadré 2
Assistance apportée par la CNUCED et ses partenaires

La CNUCED aide les pays en développement à élaborer et à réviser leurs lois sur le commerce électronique en les alignant sur les instruments internationaux et régionaux. L'assistance qu'elle a fournie pour que les pays de l'ASEAN, de la CAE, de la CEDEAO, de l'Amérique latine et de l'Amérique centrale harmonisent leurs législations a stimulé l'adoption de lois nationales dans ce domaine. Ces activités ont amené la CNUCED à collaborer étroitement avec des institutions régionales telles que la Commission de l'Union africaine, le secrétariat de l'ASEAN, le secrétariat de la CAE, la Commission de la CEDEAO, l'Association latino-américaine d'intégration et le Système économique latino-américain et caribéen.

Les activités de renforcement des capacités ont amélioré les connaissances des décideurs et des législateurs sur les aspects juridiques du commerce international et les meilleures pratiques internationales, leur permettant d'élaborer des lois conformes aux cadres régionaux.

Plusieurs organismes apportent une assistance aux pays en développement au titre de leur mandat. Ils collaborent de plus en plus les uns avec les autres. Ainsi, la CNUCED a assuré le secrétariat d'une séance d'information à l'intention des parlementaires du Commonwealth, qu'elle a organisée conjointement avec l'Organisation des télécommunications du Commonwealth et l'Association parlementaire du Commonwealth lors du Forum du Commonwealth sur la cybersécurité en 2013. Un autre exemple de ce type de collaboration est l'atelier conjoint sur l'harmonisation de la cyberlégislation dans la CEDEAO, organisé au Ghana en mars 2014 par la CNUCED, la CNUDCI, le Centre africain du cyberdroit et de prévention de la cybercriminalité, le Conseil de l'Europe et l'Initiative du Commonwealth contre la cybercriminalité.

La CNUCED a formé un réseau d'institutions avec lesquelles elle conclut des partenariats renforcés dans le cadre de différentes activités de projet. Bon nombre de ses partenaires ont contribué à établir la base de données consolidée qui a été utilisée dans le présent document. Disponible en ligne, cette base mondiale est le résultat du premier inventaire réalisé au niveau mondial et les pays sont invités à y contribuer pour la tenir à jour.

Source: CNUCED.

65. **Informer les consommateurs et les entreprises:** Sachant que le cadre juridique du commerce électronique évolue et varie d'un pays à l'autre, il est nécessaire de tenir les consommateurs et les entreprises au courant des lois applicables et des voies de recours. Cela est particulièrement important pour leur donner confiance dans le commerce électronique international. Les associations professionnelles et les organismes de protection des consommateurs devraient collaborer pour surmonter les obstacles imputables à l'incompatibilité des normes juridiques nationales. Des campagnes publiques nationales (notamment dans le cadre d'émissions de radio et de télévision) sur les moyens de protéger les consommateurs en ligne peuvent jouer un rôle clef dans les stratégies de sensibilisation.

Encadré 3
Activités de sensibilisation en Ouganda

En Ouganda, l'Autorité nationale des technologies de l'information et le Ministère des technologies de l'information et de la communication ont élaboré et adopté des lois subsidiaires (la loi sur les transactions électroniques et la loi sur les signatures électroniques) pour rendre opérationnel le cadre de la CAE sur la cyberlégislation (CNUCED, 2012). Depuis 2011, l'Autorité nationale des technologies de l'information a entrepris de faire mieux connaître ces lois et certains aspects de la sécurité de l'information pour inciter l'administration publique et le secteur privé à adopter des règles minimales pour garantir la sécurité des transactions. Plusieurs ateliers d'information ont été organisés à l'intention de ministères, d'associations de banquiers, d'associations de juristes, de chambres de commerce, de l'Office de l'investissement et de la bourse des valeurs. Ces ateliers ont bénéficié de la collaboration d'une équipe de juristes interinstitutionnelle et de conseillers techniques, notamment les experts du Groupe de travail de la CAE sur la cyberlégislation, auquel la CNUCED apporte un appui. Il est prévu d'organiser d'autres ateliers de ce type pour faire mieux connaître la loi sur la protection des données et la vie privée, une fois qu'elle sera adoptée.

Source: CNUCED.

66. À la lumière de ce qui précède, les experts sont invités à examiner les questions ci-après, qui concernent les principales difficultés juridiques que les pays doivent résoudre pour développer le commerce électronique national et international:

- Comment évaluer les besoins des pays en matière de cyberlégislation?
- Quelles sont les meilleures pratiques pour promouvoir les transactions internationales et rendre le commerce électronique plus sûr?
- Quel rôle devrait jouer le secteur privé dans l'amélioration de la sécurité des transactions en ligne et le renforcement de la confiance des consommateurs?
- Quelles mesures faudrait-il prendre pour suivre les progrès accomplis par les pays et régions en développement dans l'élaboration d'une cyberlégislation adéquate?
- Comment l'assistance des organisations internationales et des partenaires de développement peut-elle contribuer à la compatibilité des lois sur le commerce électronique?

Bibliographie

Balestrieri E. (2011). External evaluation of UNCTAD's E-Commerce and Law Reform Project. Disponible à l'adresse http://tft.unctad.org/wp-content/uploads/2014/03/2011Evaluation.ICT_.law_.Report.pdf (site consulté le 9 janvier 2015).

Castellani L. (2010). The United Nations electronic communications convention: Policy goals and potential benefits. *Korean Journal of International Trade and Business Law*. 19(1):1–16.

CyberSource (2013). 2013 Online Fraud Report. Disponible à l'adresse http://www.cybersource.com/resources/collateral/Resource_Center/whitepapers_and_reports/CyberSource_2013_Online_Fraud_Report.pdf (page consultée le 9 janvier 2015).

Commission européenne (2011). Attitudes des consommateurs vis-à-vis du commerce transfrontalier et de la protection des consommateurs. Eurobaromètre Flash n° 299. Commission européenne. Bruxelles.

Innopay (2012). Online payments 2012 − Moving beyond the web. Innopay B.V. Amsterdam. Disponible à l'adresse http://www.innopay.com/publications/online-payments-2012-moving-beyond-web (page consultée le 9 janvier 2015).

International Data Group Connect (2012). Africa 2013: Cyber-crime, hacking and malware. Livre blanc disponible à l'adresse www.idgconnect.com/view_abstract/11401/africa-2013-cyber-crime-hacking-malware (page consultée le 8 janvier 2015).

LexisNexis (2013). True cost of fraud 2013 study: Manage retail fraud. Disponible à l'adresse http://www.lexisnexis.com/risk/insights/2013-true-cost-fraud.aspx (page consultée le 9 janvier 2015).

OCDE (2000). *Lignes directrices régissant la protection des consommateurs dans le contexte du commerce électronique*. OCDE. Paris.

OCDE (2002). *Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information: Vers une culture de la sécurité.* OCDE. Paris.

OCDE (n/d). Recommandation du Conseil relative aux Lignes directrices régissant la protection des consommateurs dans le contexte du commerce électronique. OCDE. Paris. Disponible à l'adresse http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=183&Lang=fr&Book=False (page consultée le 13 janvier 2015).

Risk Based Security (2014). Data breach quickview: An executive's guide to 2013 data breach trends. Disponible à l'adresse https://www.riskbasedsecurity.com/reports/2013-DataBreachQuickView.pdf (page consultée le 9 janvier 2015).

Time (2014). The world's top 5 cybercrime hotspots. 7 août. Disponible à l'adresse http://time.com/3087768/the-worlds-5-cybercrime-hotspots/ (page consultée le 12 janvier 2015).

CNUDCI (1999). *Loi type de la CNUDCI sur le commerce électronique et Guide pour son incorporation (1996) avec le nouvel article 5* bis *tel qu'adopté en 1998*. Publication des Nations Unies. Numéro de vente F.99.V.4. New York.

CNUDCI (2002). *Loi type de la CNUDCI sur les signatures électroniques et Guide pour son incorporation (2001)*. Publication des Nations Unies. Numéro de vente F.02.V.8. New York.

CNUDCI (2007). *Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux*. Publication des Nations Unies. Numéro de vente F.07.V.2. New York.

CNUCED (2001). Principes directeurs des Nations Unies pour la protection du consommateur (tels qu'étendus en 1999). UNCTAD/DITC/CLP/Misc.21. New York et Genève. Disponible à l'adresse http://unctad.org/fr/Docs/poditcclpm21.fr.pdf (page consultée le 13 janvier 2015).

CNUCED (2010a). *Rapport 2010 sur l'économie de l'information: TIC, entreprises et atténuation de la pauvreté*. Publication des Nations Unies. Numéro de vente F.10.II.D.17. New York et Genève.

CNUCED (2010b). *Estudio Sobre Las Perspectivas de La Armonización de La Ciberlegislación En Centroamérica Y El Caribe*. Publication des Nations Unies. UNCTAD/DTL/STICT/2009/3. New York et Genève.

CNUCED (2010c). *Study on Prospects for Harmonizing Cyberlegislation in Latin America*. Publication des Nations Unies. UNCTAD/DTL/STICT/2009/1. New York et Genève.

CNUCED (2012). *Harmonisation de la cyberlégislation et de la réglementation: L'exemple de la Communauté d'Afrique de l'Est*. Publication des Nations Unies. UNCTAD/DTL/STICT/2012/4. New York et Genève.

CNUCED (2013a). *Review of E-commerce Legislation Harmonization in the Association of Southeast Asian Nations.* Publication des Nations Unies. UNCTAD/DTL/STICT/2013/1. New York et Genève.

CNUCED (2013b). *Rapport 2013 sur l'économie de l'information: L'économie infonuagique et les pays en développement*. Publication des Nations Unies. Numéro de vente F.13.II.D.6. New York et Genève.

CNUCED (2015). *Rapport 2015 sur l'économie de l'information: Libérer le potentiel du commerce électronique pour les pays en développement*. Publication des Nations Unies. New York et Genève (à paraître).

WorldPay (2014). Alternative payments report, 2e éd. Disponible à l'adresse http://www.worldpay.com/global/alternative-payments-2nd-edition (page consultée le 12 janvier 2015).