ORGANISATION MONDIALE DU COMMERCE

S/C/W/378

5 octobre 2018

(18-6169) Page: 1/3

Conseil du commerce des services Original: anglais

COMMUNICATION PRÉSENTÉE PAR LES ÉTATS-UNIS

MESURES ADOPTÉES ET EN COURS D'ÉLABORATION PAR LA CHINE CONCERNANT SA LÉGISLATION EN MATIÈRE DE CYBERSÉCURITÉ

Questions posées à la Chine

La communication ci-après datée du 3 octobre 2018, présentée par la délégation des États-Unis, est distribuée aux Membres du Conseil du commerce des services.

Au cours des deux dernières années, les Membres de l'OMC, les milieux d'affaires internationaux et d'autres parties prenantes ont exprimé de fortes préoccupations concernant la Loi sur la cybersécurité adoptée par la Chine et divers projets de mesures de mise en œuvre y relatifs (et dans certains cas, à sa Loi sur la sécurité nationale). Ces préoccupations concernent, entre autres choses, des éléments de ces projets de mesures de mise en œuvre qui limiteraient les transferts transfrontières de renseignements et qui exigeraient le stockage local des données en Chine.

Les États-Unis ont déjà présenté au Conseil du commerce des services deux communications sur la législation chinoise en matière de cybersécurité. Le 26 septembre 2017, ils ont présenté la communication "Mesures adoptées et en cours d'élaboration par la Chine concernant sa législation en matière de cybersécurité" (S/C/W/374), qui mettait l'accent sur les transferts transfrontières de renseignements et le stockage local des données. Le 23 février 2018, ils ont présenté une communication complémentaire évoquant cette même question (S/C/W/376).

Dans leurs communications antérieures, les États-Unis ont appelé l'attention des Membres sur deux importants projets de mesures de mise en œuvre portant sur ces questions: "Mesures concernant l'évaluation de la sécurité des transferts transfrontières de renseignements personnels et de données importantes" et "Norme nationale – Technologie de sécurité de l'information – Lignes directrices sur l'évaluation de la sécurité des transferts transfrontières de données". S'agissant de ces projets de mesures, diverses parties prenantes ont fait part de leurs vives préoccupations concernant l'approche envisagée par la Chine, qui consiste à exiger un processus astreignant d'évaluation de la sécurité pour les transferts de toutes données considérées par les fonctionnaires chinois comme des "données importantes". Ces parties prenantes se sont également opposées à cette même approche pour le transfert de renseignements personnels car dans presque tous les cas, le consentement explicite du propriétaire des renseignements serait exigé avant qu'un transfert transfrontières puisse avoir lieu. En outre, la Chine envisageait que les "données importantes" et les "renseignements personnels" recueillis ou produits par les exploitants d'infrastructures d'information essentielles en Chine soient obligatoirement stockés sur son territoire. Considérés dans leur ensemble, ces aspects pourraient perturber, décourager, et, dans de nombreux cas, interdire les transferts transfrontières de renseignements qui ont habituellement lieu au cours d'opérations commerciales normales.

1 QUESTIONS POSÉES À LA CHINE

1. À l'heure actuelle, il demeure difficile de déterminer si la Chine révisera l'approche envisagée pour prendre en compte ces préoccupations et comment elle le fera. Étant donné l'importance et la gravité des questions suscitées par le régime de cybersécurité chinois en cours d'élaboration, les

États-Unis posent les questions ci-après, qui étaient restées sans réponse et auxquelles il est essentiel que la Chine réponde:

a. Comment la Chine entend-elle procéder pour la révision des projets de mesures de mise en œuvre susmentionnés pour répondre aux préoccupations qui ont été exprimées?

b. Comment la Chine entend-elle diffuser les nouveaux projets de mesures de mise en œuvre? Le cas échéant, peut-elle confirmer que toutes les parties prenantes en seront informées suffisamment à l'avance et auront la possibilité de formuler des observations sur ces nouveaux projets de mesures?

c. Nombre de parties prenantes se sont dites vivement préoccupées par les restrictions que la Chine envisage à l'égard de la catégorie non définie des "données importantes". Les projets de mesures de mise en œuvre susmentionnés définissent les données importantes comme les "données liées de près à la sécurité nationale, au développement économique et aux intérêts publics et sociétaux". La Chine a précisé que "les données importantes faisaient référence aux données importantes pour la nation, pas pour les entreprises ou les personnes", mais il demeure difficile de déterminer quelle serait la portée de cette catégorie, et comment et par qui elle serait définie. Qui déciderait quelles données sont "importantes pour la nation"? L'entreprise? L'Administration du cyberespace de la Chine? Un organisme de réglementation sectoriel?

d. Comment peut-on décider si des données sont "des données importantes" d'une manière qui ne soit pas arbitraire?

e. Les projets de mesures de mise en œuvre susmentionnés s'appliqueraient à tous les exploitants de réseau, définis au sens large comme "les propriétaires de réseau, les administrateurs de réseau et les prestataires de services de réseau". Cette définition se réfère-t-elle uniquement aux entreprises qui exploitent effectivement un réseau, comme les sociétés de télécommunications? S'applique-t-elle également aux entreprises qui utilisent un réseau (ce qui équivaut, dans la pratique, à toutes les entreprises)?

f. Par ailleurs, la Chine a indiqué que ses projets de mesures de mise en œuvre s'appliqueraient spécifiquement aux exploitants d'"infrastructures d'information essentielles", et non à tous les exploitants de réseau. Même si la Chine devait limiter l'application de ces mesures aux exploitants d'infrastructures d'information essentielles, la définition et l'approche qu'elle envisage à l'égard de ces infrastructures continueraient de susciter de graves préoccupations. Au moins deux des projets de normes publiés par la Chine en juin 2018 pour recueillir les observations du public concernent les infrastructures d'information essentielles: "Technologie de sécurité de l'information – contrôle de la sécurité des infrastructures d'information essentielles" et "Technologie de sécurité de l'information – exigences relatives à la protection de la cybersécurité des infrastructures d'information essentielles". La portée de la définition des infrastructures d'information essentielles dans ces projets de mesures (comme dans la Loi chinoise sur la cybersécurité elle-même) demeure générale et vague, débordant largement du cadre des définitions nationales classiques de cette notion et risquant ainsi de créer des obstacles importants pour les fournisseurs de services étrangers, à l'intérieur et à l'extérieur de la Chine. La Chine peut-elle confirmer son intention de réviser son approche et de resserrer sa définition des infrastructures d'information essentielles?

g. Certaines exigences énoncées dans le projet de mesure intitulé "Technologie de sécurité de l'information – contrôle de la sécurité des infrastructures d'information essentielles" viennent restreindre les flux transfrontières de données:

   - dans presque tous les cas, le "consentement explicite" demeure la seule condition préalable à la collecte, à l'utilisation ou à la communication élargie de "renseignements personnels" par les exploitants d'infrastructures d'information essentielles;

   - tous les "renseignements personnels" et les "données importantes" recueillis ou produits par les exploitants d'infrastructures d'information essentielles dans le cadre de leurs activités en Chine doivent être stockés en Chine; et

- si des "renseignements personnels"/"données importantes" doivent être transférés pour des raisons commerciales, l'exploitant d'infrastructures d'information essentielles devrait procéder à une "évaluation de la sécurité", ou le transfert qu'il envisage serait soumis à une "évaluation de la sécurité" réalisée par l'État, qui semble très contraignant.

h. S'agissant tout particulièrement des "renseignements personnels", les États-Unis ont suggéré que la Chine permette aux exploitants d'infrastructures d'information essentielles d'utiliser d'autres mécanismes pour satisfaire aux exigences relatives à la collecte, à l'utilisation ou à la communication de ces renseignements, par exemple le Système de règles de confidentialité transfrontières de l'APEC (CBPR). La Chine peut-elle confirmer qu'elle envisage d'adopter un autre mécanisme moins contraignant, par exemple le CBPR?

i. Le 17 mars 2018, les "Mesures pour l'administration des données scientifiques" sont entrées en vigueur. Ces mesures énoncent les règles fondamentales de la gestion des données scientifiques en Chine et auraient notamment pour effet de restreindre les transferts transfrontières de ce type de données. La Chine n'a pas publié ces mesures à l'état de projet pour recueillir les observations du public. Accepterait-elle de suspendre la mise en œuvre de ces mesures pour pouvoir solliciter des observations du public et les réviser, le cas échéant, en fonction des préoccupations exprimées par les parties prenantes?