ORGANISATION MONDIALE DU COMMERCE

G/TBT/W/637

9 avril 2019

(19-2261) Page: 1/2

**Comité des obstacles techniques au commerce** Original: anglais

# CHINE – LOI SUR LA CYBERSÉCURITÉ

## DÉCLARATION DE L'UNION EUROPÉENNE AU COMITÉ DES OBSTACLES TECHNIQUES AU COMMERCE 6 ET 7 MARS 2019

La communication ci-après, datée du 5 avril 2019, est distribuée à la demande de la délégation de l'Union européenne.

---

1. L'UE tient à réitérer ses préoccupations concernant l'entrée en vigueur de la Loi sur la cybersécurité le 1er juin 2017.

2. La portée des prescriptions n'est pas claire car les termes clés n'ont pas été définis de manière suffisamment précise. Des concepts tels qu'"infrastructures essentielles de l'information" et "produits sûrs et fiables" ne sont pas assez clairement définis.

3. L'UE a des préoccupations au sujet de la norme elle-même. Nous notons que la Chine a communiqué la version finale des normes sûres et contrôlables en septembre 2018.

4. Nous nous réjouissons de la suppression de la référence au "code source". Toutefois, nous maintenons notre préoccupation au sujet de la méthodologie révisée. Les références au code source ont certes été retirées de la version finale, mais la simple obligation de fournir les "documents pertinents" pour que soient vérifiées la sécurité et la contrôlabilité des produits pourrait tout à fait entraîner la divulgation du code source.

5. L'UE rappelle l'importance des normes internationales et note que la loi se réfère uniquement aux normes nationales. Cela pourrait empêcher l'interopérabilité avec les normes internationales. Lors de l'élaboration de normes nationales, il serait approprié de se baser sur les normes internationales existantes et d'inviter toutes les parties prenantes concernées, y compris les entreprises à participation étrangère et les entreprises à capital entièrement étranger, à participer aux comités techniques pertinents de manière non discriminatoire.

6. L'UE tient à demander des éclaircissements concernant plusieurs des mesures d'application prévues par la Loi sur la cybersécurité de la Chine. Par exemple, l'Administration du cyberespace présentée dans les Règles de transfert de données transfrontières de la Chine (*Réglementation sur la protection de l'infrastructure essentielle de l'information* et *Mesures administratives concernant l'évaluation de la sécurité des transferts transfrontières de renseignements personnels et de données importantes*) suscite des inquiétudes quant à la largeur du champ d'application de ces règlements en ce qui concerne ce que l'on considère comme constituant l'infrastructure essentielle de l'information et les types de transferts de données transfrontières touchés, ainsi qu'en raison de l'insécurité juridique qui en résulte. Il apparaît que la définition des renseignements essentiels couvre de nombreuses activités commerciales et des secteurs entiers qui n'ont aucune influence sur la sécurité nationale. En outre, la liste des données considérées comme importantes n'est pas exhaustive. Du fait des prescriptions en matière de localisation des données et d'évaluation de la sécurité, les entreprises étrangères opérant en Chine pourraient se retrouver dans une position *de facto* moins concurrentielle par rapport aux opérateurs nationaux en Chine.

7. En ce qui concerne les prescriptions en matière de certification et de sécurité applicables aux infrastructures essentielles de l'information, l'UE craint qu'elles ne conduisent à l'interdiction *de facto* des produits et services des entreprises à participation étrangère qui fournissent des produits et des services aux entreprises relevant de la notion d'"infrastructures essentielles de l'information".

8. L'UE appelle la Chine à appliquer ces dispositions de manière non discriminatoire en respectant les principes de proportionnalité, de nécessité et de neutralité technologique et en garantissant une protection adéquate de la propriété intellectuelle. En outre, l'UE tient à réitérer ses précédentes demandes d'éclaircissements sur la relation avec les systèmes de protection multiniveaux (MLPS) existants et sur le calendrier prévu pour la mise en œuvre.

9. L'UE note avec préoccupation que la Loi sur la cybersécurité s'applique déjà et est exécutoire (avec des amendes et des sanctions possibles), alors que les mesures d'application qui en clarifieraient la mise en œuvre ne sont pas encore en place. La situation actuelle crée une forte incertitude pour les opérateurs économiques. La Chine pourrait-elle préciser au Comité quand les mesures d'application seront adoptées?

10. L'UE demande à la Chine de notifier au Comité OTC les projets de mesures concernant toute mise en œuvre sectorielle afin de permettre aux Membres de l'OMC et à leurs parties prenantes de présenter des observations sur tout développement ultérieur.

_____