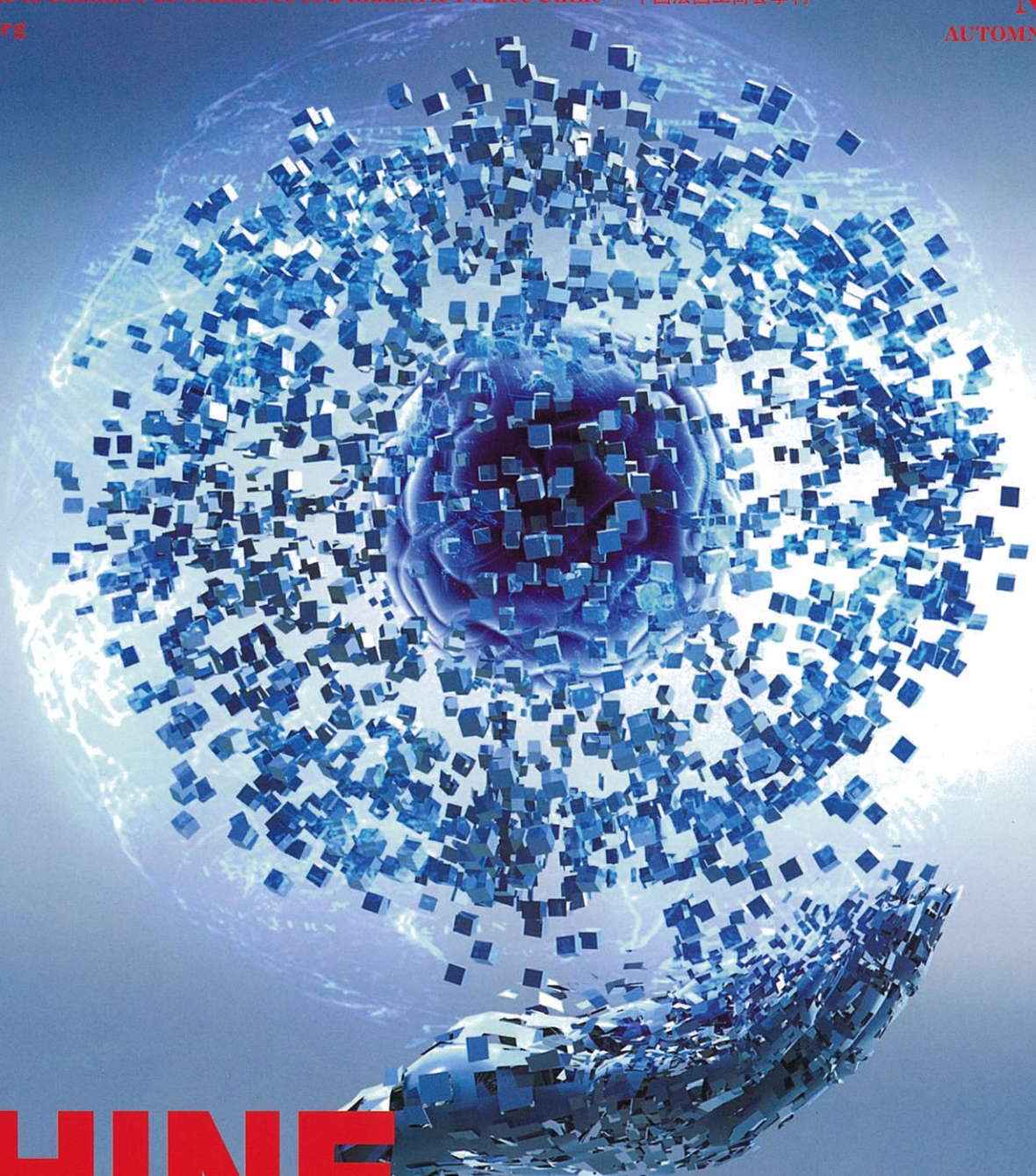
联结 CCI FRANCE CHINE 中国法国工商会

CONNEXIONS

Le Magazine de la Chambre de commerce et d'industrie France Chine | 中国法国工商会季刊
www.ccifc.org
N.79
AUTOMNE | 秋



CHINE
LA RÉVOLUTION NUMÉRIQUE
中国的数字革命

ANALYSE

ANNE LAMBERT

Avocat - Propriété Intellectuelle, Technologies Numériques et Data
Cabinet DS Avocats

Imagine China

PREMIÈRE LOI SUR LA CYBERSÉCURITÉ

Le 7 novembre dernier, le Comité Permanent de l'Assemblée Nationale Populaire a adopté la loi sur la cybersécurité.

La promulgation du texte n'est pas une surprise, la régulation du cyberespace était l'une des priorités de l'administration du Président Xi Jinping, parallèlement au développement du plan Internet Plus.

En l'espace de deux ans, le texte a fait l'objet de trois projets de lois. Cependant, malgré les nombreux commentaires apportés aux projets, notamment de la part des milieux d'affaires étrangers, la loi soulève toujours quelques problématiques :

- **Le manque de précision quant à la définition des infrastructures informatiques clés** (*« key information infrastructure »*) (article 31 de la Loi)

La loi prévoit que l'Etat se concentrera sur la protection des infrastructures informatiques clés des services d'information et de communication au public, de l'énergie, des transports, de l'eau, des finances, du service public, du e-gouvernement ainsi que celles des *« autres infrastructures informatiques clés »* qui peuvent sérieusement compromettre la sécurité nationale, l'économie du pays, la protection des citoyens ou l'intérêt public en cas de destruction, de dysfonctionnement ou de perte de données. Le terme *« infrastructures informatiques clés »* est particulièrement vague et peut théoriquement englober un grand nombre de sociétés, quelle que soit leur activité.

La promulgation du texte n'est pas une surprise, la régulation du cyberespace était l'une des priorités de l'administration du Président Xi Jinping, parallèlement au développement du plan Internet Plus.

Par ailleurs, les achats par les opérateurs d'infrastructures informatiques clés de produits et équipements dédiés aux réseaux susceptibles d'avoir un impact sur la sécurité nationale devront faire l'objet d'un examen de sécurité nationale conduit par la Cybersecurity Administration of China ci-après *« CAC »*) et les départements compétents du Conseil d'Etat (article 35). Le détail et contenu de cet examen de sécurité par la CAC ne sont pas non plus précisés.

- **L'exigence d'hébergement sur le territoire chinois des données personnelles et autres données « importantes »** (article 37)

Les données personnelles et toutes autres données « importantes » collectées et produites par les opérateurs d'infrastructures informatiques clés durant leurs activités en Chine devront être conservées sur le sol chinois (donc pas à Hong Kong). Par exception, le transfert de ces données hors de Chine sera possible, s'il est justifié par des raisons liées à l'activité de la société, et à condition d'avoir procédé à une évaluation de sécurité conduite conformément aux règles fixées par la CAC (article 66). Les données personnelles sont définies comme toute donnée électronique ou non qui, seule ou en combinaison avec d'autres, permet d'identifier une personne (ex : nom, prénom, date de naissance, numéro d'identité, données biologiques, adresse, numéro de téléphone). En revanche, s'agissant de la notion de données « importantes », aucune précision n'est apportée...

Dans la pratique, de nombreuses sociétés hébergent leurs données sur des serveurs hors de Chine pour de multiples raisons (meilleur service, back-up, serveur du siège social, etc.) ou transfèrent des données à leur siège social à l'étranger. Avec ces nouvelles dispositions, nombreuses sont celles qui vont devoir repenser le déploiement de leur infrastructure IT et revoir leurs politiques de gestion des données en local mais aussi dans certains cas, en concertation avec leur siège à l'étranger. (En Europe, il faudra également se conformer au Règlement Européen de Protection des Données Personnelles qui entrera en vigueur en mai 2018). Les fournisseurs de services cloud seront eux aussi impactés.

- **L'ambiguïté de la procédure de certification et des exigences de sécurité requises concernant les équipements réseaux et les produits destinés à la cybersécurité** (article 23)

Les équipements réseaux critiques et les produits destinés à la cybersécurité devront obtenir une certification de sécurité par des « institutions qualifiées » ou être conformes aux exigences de sécurité requises avant d'être vendus ou fournis. Rien n'est précisé à ce stade, quant à la procédure et aux exigences requises. Un catalogue des équipements et produits concernés devra être publié par la CAC prochainement. Dans l'intervalle, l'on peut se demander si les équipements et produits actuellement vendus ou utilisés au sein des sociétés correspondront aux standards et exigences de sécurité requis, sans qu'il ne soit nécessaire de les changer...

- **Le contenu exact de l'obligation de « soutien technique » apportée par les opérateurs de réseaux aux organes de sécurité de l'Etat durant les enquêtes** (article 28)

Ce que recouvre exactement l'obligation d'assistance et de soutien technique des opérateurs de réseaux aux organes de sécurité de l'Etat pour assurer la sécurité nationale et enquêter sur les infractions n'est pas davantage développé. Les sociétés devront-elles également donner accès aux backdoors de leurs systèmes ?

La loi entrera en vigueur le 1er juin 2017. Les règlements d'application de la loi sont particulièrement attendus et devraient être publiés très prochainement. Nous espérons qu'ils apporteront davantage de précisions afin de pouvoir déterminer dans quelle mesure les sociétés seront pratiquement impactées.

ANNE LAMBERT, *Avocat - Propriété Intellectuelle, Technologies Numériques et Data*
Cabinet DS Avocats

DR

RETOUR D'EXPÉRIENCE

ALEXIS BONHOMME

Fondateur de Curiosity China

« Être sur le qui-vive en permanence »

« L'évolution des solutions digitales chinoises évoluent très vite. Une technologie peut ainsi devenir obsolète moins de 90 jours après sa mise sur le marché. Ce qui impose une veille obligatoire. Ce sont les consommateurs qui font le marché et non les plateformes. On note par exemple un boom récent du lifestreaming en Chine, poussé par les digital KOL *(key opinions leaders du numérique). Cet engouement va-t-il se poursuivre ? Tout va dépendre de la réaction à moyen terme des utilisateurs.*

Le marché chinois est également très concurrentiel – les acteurs, extrêmement nombreux, sont très actifs. Ce qui pose également la question de la sécurité des données. Les entreprises étrangères cherchent à avoir des systèmes SaaS (Software as a Service) en dehors de Chine mais qui sont positionnés sur la Chine. Les entreprises dépensent beaucoup d'argent dans le digital pour obtenir de la donnée et de la vente, ce qui réclame aussi beaucoup de travail. En Chine, il est primordial de bien investir, de flécher très vite ses investissements, car ce n'est pas un marché peu cher... ni facile. »

Curiosity China est une société digitale et technologique, créée il y a 3 ans, spécialisée dans la stratégie marketing digitale et le social CRM. L'entreprise (40 personnes au total) est présente à Pékin, Shanghai, Hong-Kong, Paris et ouvre un bureau à New-York début 2017.

Imagine China