BignonLebray

PROTECTION DES DONNÉES

La législation chinoise au regard des règlements européens

FÉVRIER 2020

INTRODUCTION

Avec le RGPD, l'Europe renforce la protection des données personnelles

Qu'en est-il pour la Chine?

	Quoi ?	Depuis Quand ?	Qui ?	Pourquoi ?
	Règlement Général sur la Protection des Données	25 mai 2018	Responsable de traitement et sous-traitant	Protection et responsabilisation
	Pas de texte unique, mais une multide de référentiel	1er texte réglementaire: 2012 1er texte législatif: 2018	Controleur et sous-traitant	Sécurité et controle de l'Etat

INTRODUCTION

- Définitions
  - Voir article 4 du RGPD
  - Définition en droit chinois des données personnelles dans des normes nationales

- Historique
  - Directive 95/46/CE sur la protection des données personnelles / Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 / Règlement général sur la protection des données 2016/679
  - Règlement GB/T 35273-2017 (entrée en vigueur en 2018) et beaucoup d'autres textes

- Projet
  - RÈGLEMENT e-privacy (2020)
  - LOI pour la protection des données (2020)

PLAN

I - LES TEXTES CHINOIS

Les textes européens bien connus

- Les textes votés et promulgués
- Les textes en cours d'élaboration
- Les lignes directives de l'APEC

II- LE RÉGIME

- Les administrations compétentes
- Les responsables désignés
- Les principes de base

1

LES TEXTES

I – LES TEXTES CHNOIS

- Les textes qui sont entrés en vigueur
- Les textes en cours d'élaboration publiés pour la consultation publique
- Les lignes directives de l'APEC et les CBPR

TEXTES APPLICABLES

Sur la confidentialité des données et la sécurité des données

- Loi sur la sécurité de l'Etat (2015) ; Loi pénale modifiée (2015); Loi sur la cyber-sécurité (2017) ; Loi sur le E-commerce (2019) ; loi sur la cryptographie (2020)
- Règlement sur la gestion des crédits (2013) ; Règlement des télécommunications (modification en 2016)
- Règlement sur la protection des données personnelles des utilisateurs de télécommunications et d'Internet (2013) ; Mesures de gestion des transactions online (2014)
- Lignes directrices pour l'auto-évaluation de la collecte et de l'utilisation des informations personnelles par les App (2019) ; Guide de sécurité des informations personnelles sur Internet (2019)
- Interprétations de la Cour suprême et du Parquet suprême sur le droit applicable dans les affaires criminelles de violation des données personnelles (2017)
- Normes nationales sur la sécurité des données personnelles (2018) ; Normes nationales sur les exigences de base pour la protection par niveau de sécurité du réseau (2019)
- Normes professionnelles pour la protection des données des utilisateurs de publicités ciblées sur Internet (2014)

TEXTES APPLICABLES

Tentative de synthèse des principaux textes applicables

	Decision on Strengthening Protection of Online Information28/12/2012	***Guidelines for Personal Information protection in information systems for public and commercial services01/02/2013***	***Provisions on Protecting the Personal Information of Telecommunications and Internet Users01/09/2013***	***Amendment to the Law on the Protection of the rights and interests of consumers15/03/2014***
Contexte	Premier document de référence relatif à la protection des données personnelles	Référentiel afin d'apprécier une politique de protection des données personnelles d'une entreprise	Dispositions relatives à la protection des données personnelles des utilisateurs d'internet et des services de télécommunications	Amendement des lignes directrices
Destinataire du texte	FAI, entreprises et institutions publiques chinoises qui, dans le cadre de leurs activités, collectent et utilisent des données permettant d'identifier un individu et/ou concernant sa vie privée	Toute entreprise opérant un ou plusieurs traitements de données à caractère personnel	Fournisseurs de services internet et de télécommunication collectant et utilisant les données personnelles des utilisateurs	Toute entreprise opérant un ou plusieurs traitements de données à caractère personnel
Portée du texte	Juridiquement contraignant	Non juridiquement contraignant	Juridiquement contraignant	Non juridiquement contraignant
Apports du texte	Principes de légitimité, finalité, nécessité, confidentialité Principe du recueil du consentement (sans indiquer à quel moment ni sous quelle forme)	Définitions des termes clefs (eg. donnée personnelle)Transfert international de données personnelles Sous-traitance Sécurité	Principes de légitimité, nécessité, proportionnalité, confidentialité, d'information préalable et de recueil du consentement Principes de minimisation de la collecte, de droit de rectification, de droit à l'oubli	Domaine de protection du consommateur étendu en intégrant des dispositions relatives à la protection de ses données personnelles Conduite à suivre par les entreprises lors de la collecte et de l'usage de données personnelles

TEXTES EN COURS D'ÉLABORATION

- Deuxième rédaction pour la réforme du code civil : chapitre droit de la personne (2019)
- Décret d'application pour la loi sur la protection des droits des consommateurs (projet 2016)
- Règlement pour la protection des mineurs sur le net (2017)
- Règlement sur la protection de la sécurité des infrastructures d'information critiques (projet soumis à consultation publique 2017)
- Règlement sur la protection du niveau de sécurité du réseau (projet soumis à consultation publique 2018)
- Mesures de surveillance et d'administration des transactions de réseau (projet soumis à consultation publique 2019)
- Mesures d'examen de la cybersécurité (projet soumis à consultation publique 2019)
- Mesures de gestion de la sécurité des données (projet soumis à consultation publique 2019)
- Règlement sur la protection des réseaux de renseignements personnels pour enfants (projet soumis à consultation publique 2019)
- Mesures d'évaluation de la sécurité des informations personnelles et des données importantes destinées à des transferts transfrontaliers (projet soumis à consultation publique 2017)
- App Méthodes de détermination de la collecte et de l'utilisation des informations personnelles en violation des lois et règlements (projet soumis à consultation publique 2019)
- Normes nationales sur la sécurité des données personnels (3e projet modifié en octobre 2019)

ORGANES EN MATIÈRE DE PROTECTION DES DONNÉES

CEPD: https://edpb.europa.eu

- Organe européen indépendant
- Contribue à l'application cohérente des règles en matière de protection des données au sein de l'Union européenne et encourage la coopération entre autorités de l'UE chargées de la protection des données.

EDPS: https://edps.europa.eu

CAC (Cyberspace administration of China): www.cac.gov.cn

OCCAC (Parti communiste): http://www.cac.gov.cn/

2

LE RÉGIME

II – LE RÉGIME

- Les administrations compétentes
- Les responsables désignés
- Les principes de base

LES ADMINISTRATIONS COMPÉTENTES

- Qui sont-elles ?

- CEPD
- Autant d'autorités de contrôles que d'Etats européens
  - Cnil (France)
  - BFDI (Allemagne)
  - APD (Belgique)
  - …

- Quels sont leurs pouvoirs ?

- Réglementaire (projet / consultation)
- Information (norme/règles)
- Contrôle
- Sanction

- Qui sont-elles ?

- Cyberspace Administration of China (CAC：Gouvernement)
- Office of the Central Cyberspace Affairs Commission (OCCAC：Parti)
- Ministère de la sécurité publique
- Bureau du Ministère de l'industrie et des Technologies de l'information
- Administration de la Surveillance du Marché
- Autorités de contrôle locales

- Quels sont leurs pouvoirs ?

- Centre de dénonciation
- Cyber-surveillance : internet/messagerie
- Organisation des plateformes « désintoxication »
- Autosaisie – investigations - sanctions

LES RESPONSABLES DÉSIGNÉS

- **Le responsable de traitements**

Celui qui détermine les moyens et les finalités du traitement

- **Le sous-traitant**

Personne traitant les données pour le compte du responsable de traitement

- **Le responsable conjoint**

Lorsque 2 responsables déterminent conjointement les finalités et les moyens du traitement

- **Le rapport entre les deux** : par contrat entre le RT et le ST (article 28 RGPD) ainsi qu'entre le RT et le RC (article 26 RGPD)

- **Le contrôleur et le sous-traitant**

Les normes nationales de 2018 sur la sécurité des données personnelles modifiées en février, juin et octobre 2019 et loi sur la cyber-sécurité de 2017

- **La définition des fonctions**

Le contrôleur qui peut être une personne physique ou morale, a le pouvoir de décision quant à la finalité du traitement des données ; la notion du sous-traitant n'a pas été définie par les textes

- **Le rapport entre les deux** : par contrat de mandat

EXIGENCES POUR LE RT (1)

Le responsable de traitement

1. Met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement
2. S'assure du respect des principes de qualité des traitements (art. 5: légalité, équité et transparence, limitation des finalités, minimisation des données, précision, limitation du stockage, intégrité, confidentialité)
3. Désigner le Sous-traitant (le cas échéant) avec des garanties suffisantes au tire de la conformité du GDPR (art. 28.1)
4. Crée le registre des traitements et le documente
5. Assurer la sécurité du traitement (art. 32)
6. Désigner un DPO ou un représentant local

Le contrôleur

1. Définit les limites du mandat selon le consentement donné par la personne concernée (sauf les cas où le consentement n'est pas exigé)
2. Évalue l'impact sur la sécurité de l'information dont le traitement est confié dans la limite du mandat
3. Contrôle le mandataire ; sa responsabilité et son devoir contractuel et audit des travaux réalisés par le sous-traitant
4. Enregistre avec précision les traitements des données personnelles dans le cadre du mandat
5. Conserve ces enregistrements

DIFFÉRENCE MAJEURE POUR LE RT (2)

Assure la protection des données personnelles et en est responsable sanction administrative et pénale

Rôle purement administratif

Pas de sanction (pénale ou administrative) connue à date

EXIGENCES POUR LE ST (2)

Le sous-traitant

1. Le traitement des données doit être fait strictement selon les instructions du contrôleur, s'il y a des cas exceptionnels où le sous-traitant est contraint à ne pas les respecter, il en rapporte au contrôleur
2. En cas de sous-traitance, il lui faut une autorisation préalable de la part du contrôleur
3. Il coopère avec le contrôleur pour le respect des exigences de la personne dont les données sont confiées
4. Obligation de rapporter au RT si ses instructions enfreignent le règlement RGPD ou une loi locale
5. Ne pas conserver les données au-delà de la durée du traitement
6. Tenir un registre
7. Désigner un DPO ou un représentant local

Le sous-traitant

1. Le traitement des données doit être fait strictement selon les instructions du contrôleur, s'il y a des cas exceptionnels où le sous-traitant est contraint à ne pas les respecter, il en rapporte au contrôleur
2. En cas de sous-traitance, il lui faut un mandat préalable de la part du contrôleur
3. Il coopère avec le contrôleur pour le respect des exigences de la personne dont les données sont confiées
4. Obligation de rapporter au contrôleur en cas de manquement inévitable pour la sécurité des traitements
5. Ne pas conserver les données au-delà du lien de mandat

DIFFÉRENCE MAJEURE POUR LE ST (2)

Obligation générale de conformité à la charge du ST et d'accompagnement du RT

Obligation de notifier les risques en termes de sécurité et rapporter à sa hiérarchie

RESPONSABILITÉ DU CONTRÔLEUR ET DU SOUS-TRAITANT

- **Responsabilités délimitées par le contrat**

Pas de possibilité de délimiter la responsabilité du ST ou du RT dans le contrat

Article 83 du RGPD liste les sactions applicables au RT et au ST

Article L.226-16 et suivants du code pénal liste les sanctions applicables au RT

- **Responsabilité contractuelle définie entre responsable de traitement**

En revanche, le contrat peut déterminer les niveaux de responsabilité entre deux responsables conjoints, dans la mesure le contrat a vocation à régir les rôles des deux acteurs.

- **Responsabilités délimitées par le contrat**

Le contrôleur et le sous-traitant précisent dans un contrat les délimitations des responsabilités de chacun entre eux au sujet du traitement des données ; le but est de faire partager par le sous-traitant la responsabilité du contrôleur

- **Responsabilité contractuelle et règles non contraignantes des normes nationales et professionnelles**

Le contrôleur et le sous-traitant peuvent également insérer dans leur contrat les règles non contraignantes des normes, nationales ou professionnelles, pour qu'elles deviennent obligatoires

LIMITES : LE CONTRAT ENTRE LE CONTRÔLEUR ET LE SOUS-TRAITANT N'EST PAS OPPOSABLE AUX TIERS

Même principe

- **Cependant**

1. Le contrat entre RTs (responsable conjoints) doit être rendu public
2. Il est opposable au tiers

- **L'administration qui supervise**

1. L'autorité de contrôle n'est pas liée par la définition donnée par le contrat
2. Pouvoir de l'autorité de contrôle de redéfinir le rôle des acteurs au regard de la réalité constatée

Seuls le contrôleur et le sous-traitant sont responsables :

- **La personne concernée**

1. Responsabilité contractuelle du contrôleur
2. Responsabilité délictuelle du contrôleur et du sous-traitant

- **L'administration qui supervise**

1. Pas de notion de « contrôleur » ou de « sous-traitant » ; ils ne sont que des « exploitants de l'Internet », « exploitants » ou « exploitant du E-commerce »
2. Le contrôleur a le devoir de précaution et le devoir de contrôle
3. Le sous-traitant doit être compétent pour le traitement

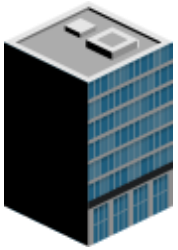
LES PRINCIPES DE BASE (1)

1. L’extraterritorialité de la règlementation
2. Le traitement des données
3. Le consentement de la personne concernée
4. Le transfert des données
5. Les droits de la personne concernée
6. Les incidents de sécurité

LES PRINCIPES DE BASE (1-1)

8. L'extraterritorialité de la règlementation

- Art. 3 RGPD



Critère de l'établissement

Etablissement dans l'UE

Critère du ciblage

Etablissement hors UE mais offre des produits ou services aux personnes se trouvant sur le territoire de l'UE ou vise à les cibler

LES PRINCIPES DE BASE (1-2)

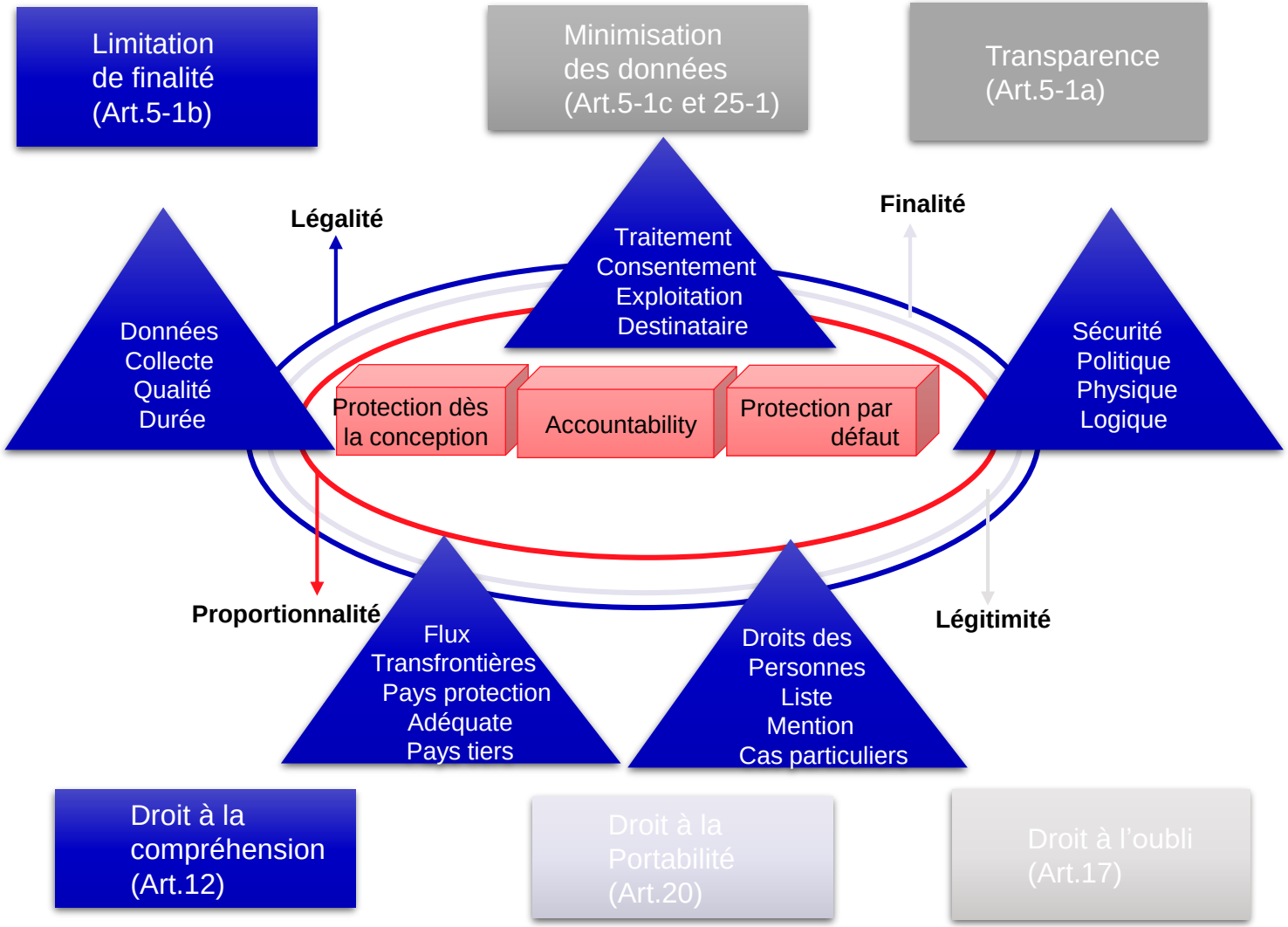
9. L'extraterritorialité de la règlementation

- Pas de dispositions similaires (art. 3 RGPD)
- Les articles 50 et 75 de la loi sur la cyber-sécurité 2017

  – Art. 50 : l'Administration nationale d'Internet et de communication ainsi que les administrations concernées exercent les fonctions de gestion et de contrôle ; elles ont le pouvoir d'ordonner l'arrêt ou de prendre des mesures de sanction à l'encontre des actes de transmission ou de diffusion des informations interdites par les lois et règlements ; lorsque ces informations sont de provenance de l'étranger, elles peuvent aviser les organisations concernées afin qu'elles prennent des mesures techniques en vue d'empêcher la diffusion.

  – Art. 75 : les actes d'attaque, d'intrusion, de trouble ou de destruction commis par des personnes morales et/ou personnes physiques étrangères portant atteinte aux infrastructures d'informations cruciales sont enquêtés par les organes de sécurité publique du Conseil des Affaires de l'Etat ; lesquels peuvent décider de bloquer les biens ou d'autres mesures de sanction.

LES PRINCIPES DE BASE (2-1)



LES PRINCIPES DE BASE (2-2)

1. **Le traitement des données: responsabilité, finalité, information et accord de la personne concernée, minimisation, transparence, sécurité, et enfin, participation de la personne concernée**

- Exactitude des données, si possible, tenues à jour art.5-d du RGPD
- Modération art.5-c : finalité et nature des info collectées
- Big data et zones « blog-notes » : point de vigilance fort pour la CNIL
- Du « droit à l'oubli » : déterminer une durée de conservation des données
- Sécurité et confidentialité : obligation de moyen renforcée
- Traitement des données et personne concernée

1. **Simple obligation d'information**

- Obligation d'information unique
- Pas de droit à la compréhension
- Possibilité de collecter les données de façon indirecte
- New: Droit à l'oubli avec durée de conservation à déterminer
- Sécurité et confidentialité : objectifs et moyens ; loi sur la cryptographie; notion de violations de données personnelles
- Données sensibles différentes, information bancaire, assurance, santé et mineur de moins de 14 ans
- Zone de commentaire libre pour la Chine

LES PRINCIPES DE BASE (3)

2. Le consentement de la personne concernée

- Article 6: base de traitement = consentement
- Base de traitement (consentement) pour:
  - Traitement des données sensibles
  - Transfert hors Union européenne
  - Collecte de données de mineur
  - Géolocalisation
  - Prospection commerciale
  - Données biométriques et génétiques

2. Le consentement de la personne concernée

- Base de licéité du traitement : ce qui est interdit:
  - Fraude / tromperie / violence
  - Dissimuler la finalité
  - Par chaine illégale
  - Information interdit par la loi et le règlement

LES PRINCIPES DE BASE (4)

3. Pas d'obligation de conserver les données localement

4. Le transfert des données

- S'installer dans un Etat avec un niveau de protection adéquate
- Prendre des garanties appropriées
- Justifier par la nécessité du transfert
- Procédures de contrôle et d'autorisation avant le transfert
- Obtenir le consentement de la personne concernée
- Le cas du transfert prévu au dernier alinéa de l'article 49 du RGPD

3. Obligation de conserver les données localement

- toutes les données définies comme sensibles ou contenant des données importantes doivent être hébergées en Chine. Aucune de ces données n'est autorisée à quitter le pays (sauf avec l'autorisation spéciale du gouvernement).
- Pour les autres: auto évaluation contrôlée par l'Administration (annuellement)

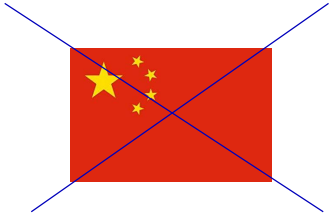
4. Le transfert des données

- Les données personnelles et les données importantes (重要数据 et 关键信息)
- Self-évaluation ; évaluation par l'administration de contrôle et évaluation annuelle avec rapport
- Contrôle de sécurité des réseaux internet ; autorisation administrative
- Procédures de contrôle et d'autorisation avant le transfert

LES PRINCIPES DE BASE (4)

Quels pays bénéficient d'une décision d'adéquation?

- Israël
- Japon
- Suisse
- Andorre
- Iles Féroés
- Liechtenstein
- Ile de Man
- Canada
- Nouvelle Zélande
- Argentine
- Uruguay
- Ile de Jersey
- Norvège
- L'Islande
- Ile de Guernesey



LES PRINCIPES DE BASE (5)

- Droit à l'information

Une information claire, intelligible, aisément accessible aux personnes concernées par les traitements de données

- Droit d'accès

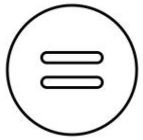
Toute personne peut, accéder à l'ensemble des informations la concernant

- Droit à la portabilité

Création d'un droit à la portabilité des données qui permet à la personne concernée de demander : la restitution de ses données / le transfert de ses données

- Droit d'opposition

A un traitement ou de s'opposer au profilage et à décisions automatisées (article 21 RGPD)



6. Les droits de la personne concernée

- Les droits d'accès, de rectification, et de portabilité des données
- Les droits d'effacement, d'opposition et de limitation des données
- Les modalités d'exercices des droits
- Les limitations apportées à l'exercice des droits

Différence dans la pratique

LES PRINCIPES DE BASE (6)

7. Les incidents de sécurité

- Articles 33 et 34

  — Obligation de notification à l'autorité de contrôle dans les 72 heures de l'incident

  — Obligation de communication à la personne concernée en cas de risque d'atteinte élevée aux droits et libertés des personnes concernées

+

- Obligation pour le sous-traitant d'apporter son concours en cas de faille de sécurité

7. Les incidents de sécurité

- Selon la politique du Gouvernement et du Parti : « gouvernance spéciale »
- Ex. Méthodes pour déterminer les App de collecte et d'utilisation des informations personnelles en violation des lois et règlements
- Convocation, « décollage » et fermeture

+

- Mesures drastiques de l'administration avec actions très énergiques en cas de faille de sécurité

CONCLUSIONS

CONCLUSIONS

Versus

Une protection des données, oui, mais pour des objectifs différents

INTERVENANTES

ELISE DUFOUR

AVOCAT ASSOCIÉ

edufour@bignonlebray.com

XIAOLIN FU-BOURGNE

AVOCAT OF COUNSEL

xlfubourgne@bignonlebray.com

MERCI

www.bignonlebray.com

PARIS
75, rue de Tocqueville
75017 Paris