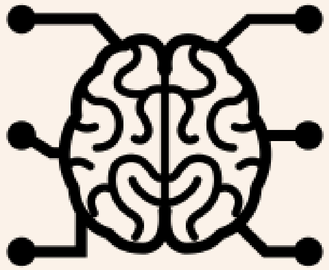
klein • wenner

Les enjeux réglementaires liés à l'intelligence artificielle

(Machine Learning)

Jeudi 21 Octobre 2021

SOMMAIRE



PARTIE I : NOTION ET CONTEXTE

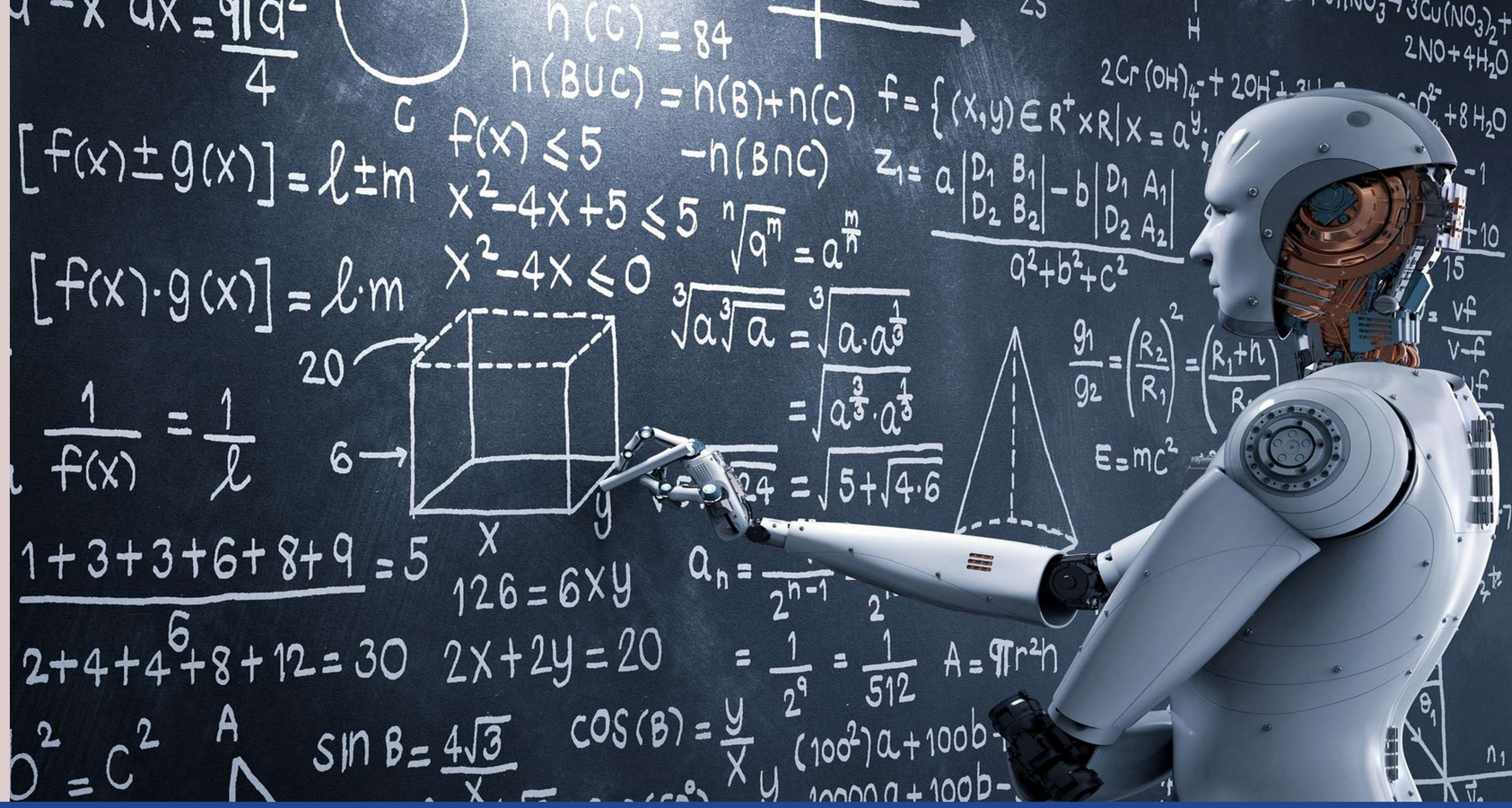
A. La définition de l’IA
B. Les différents types d’IA
C. Les risques associés aux IA
D. Le rôle clé de la donnée

PARTIE II : LE RÉGIME JURIDIQUE À VENIR

A. Le champ d’application
B. Le régime du système IA à haut risque

k • w

klein • wenner

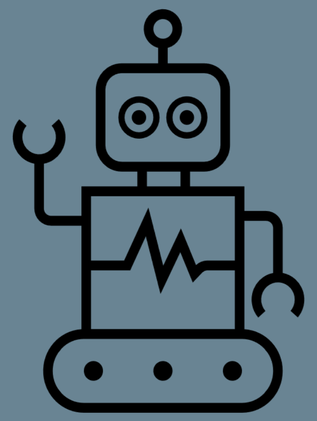


PARTIE I : NOTION ET CONTEXTE

A. La définition de l'IA

« ***système automatisé*** *qui, pour un ensemble donné d'objectifs définis par l'homme, est en mesure* ***d'établir des prévisions****, de* ***formuler des recommandations****, ou de* ***prendre des décisions*** *influant sur des environnements réels ou virtuels* » (*OCDE, 22 mai 2019*)

→ Ensemble de théories et de techniques mises en œuvre en vue de réaliser des machines capables de simuler l'intelligence



B. Les différents types d'IA

On distingue deux dimensions :

➢ **La dimension conceptuelle**

- **L'IA « forte »** => véritable « *conscience de soi* » de la machine.
- **L'IA « faible »** => simple application des instructions de l'utilisateur.

➢ **La dimension technique**

- **L'IA « symbolique » *(modèle expert)*** => s'appuie sur moteur d'inférences utilisant des règles prédéfinies permettant à la machine de déduire une conclusion face à une situation donnée.
- **L'IA « connexionniste » (numérique)** => utilise une logique inductive (consistant à tirer de plusieurs cas particuliers des conclusions générales).

« LA PETITE HISTOIRE DE L'IA »

- **L'IA, une idée ancienne**
  - Imaginée à la fin de la seconde guerre mondiale
  - Années 1960-1970 : système expert
  - Années 1980
    - Invention d'algorithmes d'apprentissage *(Machine Learning)*
    - Mauvais fonctionnement, en raison de faibles capacités de calcul et des quantités de données (à l'époque rares et coûteuses).

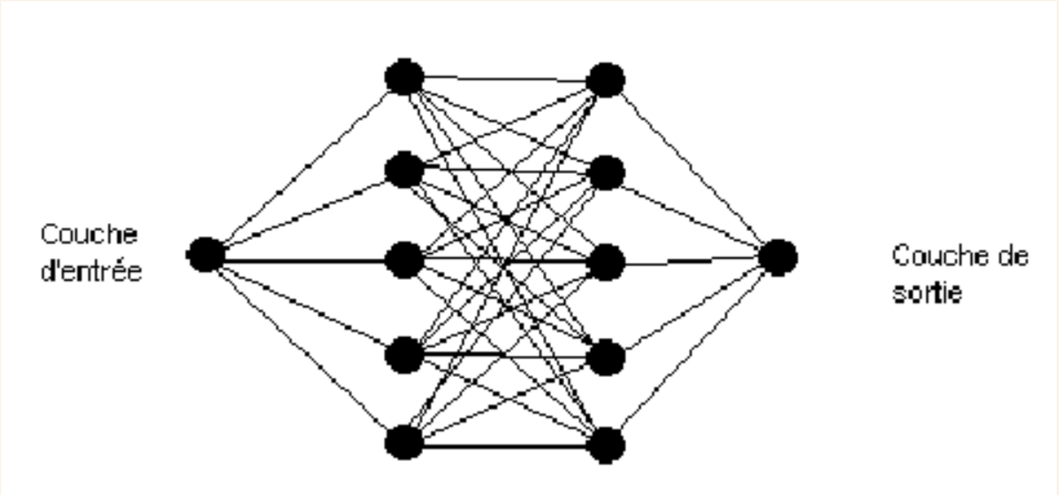
- **Les bouleversements technologiques des années 2000-2010 : Big Data et capacités de calcul décuplées**
  - Développement récent et fulgurant des capacités de calcul des microprocesseurs
  - Accroissement sans précédent de données disponibles

- **Un engouement récent, du fait des performances atteintes**
  - Travaux du chercheur français Yann LeCun, l'un des lauréats du prix Turing en 2019
  - Résultats, rendus publics par certaines entreprises, extrêmement prometteurs => taggage automatique de vidéos, reconnaissance automatique de langage (multi-locuteur)

FOCUS SUR L'IA CONNEXIONNISTE => *MACHINE LEARNING*

(algorithme de rétropropagation du gradient)

Le fonctionnement de l'IA connexionniste (algorithme d'apprentissage automatique) : par essais et erreurs.



En simplifiant cet algorithme constitué d'un réseau de neurones artificiels va recevoir des données d'apprentissage, dites « étiquetées », (c'est-à-dire accompagnées d'une information nommant ou décrivant la donnée - ce que l'on appelle aussi une « métadonnée ») à partir desquelles l'IA va être sollicitée pour « deviner » l'étiquette sur la base d'un scénario (dit le « modèle »).

Dès lors :

- si le résultat est erroné, le dispositif s'appliquera – via un mécanisme mathématique utilisant une fonction dérivée – un score qui va réduire ce type de réponse à l'avenir, devant une donnée similaire;
- à l'inverse, lorsque le dispositif aura prédit une réponse s'avérant exacte, il lui sera appliqué un score destiné à renforcer ce type de réponse devant des données semblables.

En multipliant cet exercice (dit d'apprentissage « par essais et erreurs »), le dispositif sera amené à généraliser.

Une fois que le taux d'erreurs sera suffisamment faible sur les données d'apprentissage, l'IA sera alors déployée sur des données de production non étiquetées : il s'agira alors de faire travailler l'IA dans un environnement réel, dans lequel, grâce à l'opération de généralisation précitée, elle sera *a priori* capable de fournir des réponses cohérentes dans un contexte inconnu.

C. Le rôle clé de la donnée

Les biais. L'IA ne fait que reproduire ce que révèle les données qui lui sont fournies, et qui peuvent reproduire des anomalies matérielles ou éthiques, fruits de biais culturels ou sociologiques.

L'IA ne dit pas la vérité, mais seulement la probabilité

- Les résultats produits par une IA ne devront jamais être regardés comme reflétant une vérité, mais simplement une probabilité.
- Ces résultats sont fortement dépendants de la qualité du jeu de données, reproduisant lui-même souvent nos propres biais, qu'ils soient sociologiques ou culturels.

Pour être « *intelligente* », l'IA doit utiliser les bonnes données.

D. Les risques associés aux IA

Deux risques majeurs sont associés aux IA :

- **Des résultats biaisés, pouvant susciter des discriminations**
  - ⇒ *Amazon* a tenté d'automatiser le recrutement de ses futurs salariés en ayant recours à une intelligence artificielle : l'IA a finalement été désactivée, car elle pénalisait les candidatures de femmes (2018)

- **Le phénomène « boîte noire » de l'IA connexionniste**
  - ⇒ Généralisation opérée par l'IA, sans restitution sous une forme intelligible pour l'homme de la règle de généralisation induite à partir des données d'apprentissage (défaut d'explicabilité)

PARTIE II : LE RÉGIME JURIDIQUE À VENIR

Propos liminaire

Une initiative européenne, fruit d'une prise de conscience et d'une volonté politique

Pour rester dans la course, et même reprendre une suprématie que les Etats-Unis ainsi que la Chine possèdent aujourd'hui sur les technologies d'IA, le Parlement et la Commission européenne ont pris conscience que l'UE doit investir massivement et efficacement sur l'IA et la construction de plateformes favorisant la réunion de vastes quantités de données.

Pour cette raison, le Parlement a pris une série d'initiatives :

- une proposition de règlement relatif à la gouvernance des données est à l'étude (depuis novembre 2020 / *open data*) ;
- Une proposition de Règlement relatif à l'Intelligence Artificielle (rendue publique en avril 2021).

A. Le champ d'application

1- Champ d'application matériel : la nouvelle classification

- **L'IA interdite entraînant un risque inacceptable (Art. 5) :** système d'IA :

  - permettant la diffusion de messages cachés,
  - exploitant la vulnérabilité d'un groupe (âge, handicap),
  - fournissant une notation sociale d'un comportement A aux fins de sanction d'un contexte B ou conduisant à un traitement injustifié ou disproportionné,
  - utilisant un système d'identification biométrique dans des espaces publics en vue du maintien de l'ordre (sauf exception).

- **L'IA à haut risque entraînant un risque élevé (Art. 6) :** système d'IA, alternativement :

  - destiné à être utilisé comme composant de sécurité d'un produit, ou est lui-même un produit, devant faire l'objet d'une évaluation de conformité (Annexe II : *machines, ascenseurs, équipements radioélectriques ou sous pression, installations à câbles, appareils à gaz, dispositifs médicaux, équipements marins, sécurité des jouets, véhicules à moteurs,* etc.) ;
  - autonome, ayant principalement des implications en matière de droits fondamentaux (Annexe III : *identification biométrique, gestion et exploitation des infrastructures critiques, éducation et formation professionnelle, emploi, gestion des travailleurs et accès au travail,* etc.).

- **L'IA à faible risque (Art. 69 et s.) :** système d'IA autre qu'une IA interdite et une IA à haut risque.

k • w

A. Le champ d'application

2- Champ d'application temporel (art. 85)

- **Version définitive** attendue fin 2022 début 2023
- **Entrée en vigueur** : 20ème jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.
- **Application** : 24 mois à compter de l'entrée en vigueur.

3- Champ d'application territorial et personnel (art. 2)

Les critères s'articulent en fonction du lieu de l'activité puisque le Règlement s'applique dès lors que sont situés dans l'UE :

- Les systèmes d'IA (sur le marché ou en service) ;
- Les utilisateurs des systèmes d'IA sous réserve **qu'ils agissent à des fins professionnelles** ➔*exclusion des personnes agissant dans le cadre d'une activité personnelle*
- L'utilisation des résultats produits par les systèmes d'IA, y compris quand ces derniers ne sont pas mis sur le marché ni mis en service.

B. Régime du système d'IA à haut risque

1- Obligations de conformité du système d'IA

1.1. Obligations pesant sur les fournisseurs *(Art. 16)*

➢ Le fournisseur, qui développe ou fait développer un système d'IA à haut risque, **assume la responsabilité** de sa mise sur le marché ou de sa mise en service et doit, notamment :

1) S'assurer que le système est conforme aux exigences du chapitre 2 (art. 16) :

- **Système de gestion des risques**. Processus de gestion des risques pour la vie du système d'IA, sous la forme d'une suite d'instructions répétitives, régulièrement mises à jour (art. 9) ;
- **Gouvernance des données**. Surveillance, détection et correction des biais par une politique contraignante de gouvernance des données d'entraînement, de validation et de test (art. 10) ;
- **Documentation technique**. Dossier technique notamment composé d'une description de la logique, du fonctionnement et l'architecture du système (art. 11) ;
- **Tenue de registres**. Journaux enregistrant les actions du système d'IA pour en garantir la traçabilité (art. 12) ;
- **Transparence et fourniture d'informations aux utilisateurs**. Mode d'emploi sur la finalité et la bonne utilisation du système, y compris le cadre spécifique dans lequel il est censé être utilisé, et permettre à l'utilisateur d'en contrôler le fonctionnement (art. 13) ;
- **Surveillance de l'homme**. Contrôle humain du système par l'utilisateur, visant à prévenir/réduire les risques (santé, sécurité et droits fondamentaux) (art. 14) ;
- **Précision, robustesse et cybersécurité**. Solutions de redondance technique (plan de sauvegarde ou de sécurité intégré) en vue d'une performance constante (art. 15).

k • w

2) Établir un système de gestion de qualité (art. 17) ;

3) Établir la documentation technique pertinente (art. 18) ;

4) Conserver les journaux générés automatiquement (art. 20) ;

5) Veiller à ce que le système d'IA soit soumis à la procédure d'évaluation de la conformité (art. 19) ;

6) Se conformer aux obligations d'enregistrement dans la base de données de l'UE (art. 51) ;

7) Prendre des mesures correctives, en cas de non-conformité (art. 21) ;

8) Mettre en place un système de surveillance après la mise sur le marché;

9) Apposer le marquage CE sur le système d'IA (art. 49);

10) Informer les autorités des Etats de mise en service du système d'IA;

11) Coopérer avec les autorités nationales compétentes.

1.2. Obligations pesant sur les distributeurs *(Art. 27)*

- Le distributeur est défini comme « *toute personne physique ou morale de la chaîne d'approvisionnement, autre que le fournisseur ou l'importateur, qui met un système d'IA à disposition sur le marché de l'Union sans en modifier les propriétés* ».

- Il est soumis aux **obligations suivantes**:

1) S'assurer que le système d'IA porte bien le marquage de conformité CE requis, qu'il est accompagné de la documentation et que ses prédécesseurs ont respecté leurs obligations ;

2) Vérifier que les conditions de stockage et de transport n'endommagent pas la conformité ;

3) Prendre des mesures correctives pour mettre le système en conformité, le retirer, le rappeler ou s'assurer que le fournisseur, l'importateur ou tout autre acteur, prend bien les mesures correctives;

4) Coopérer avec les autorités.

k • w

1.3. OBLIGATIONS PESANT SUR LES UTILISATEURS ***(ART. 28-29)***

- L'utilisateur, qui désigne toute personne « *utilisant un système d'IA sous son autorité, sauf lorsque le système d'IA est utilisé dans le cadre d'une activité personnelle non professionnelle* », est **soumis aux obligations suivantes**:

  1) Respecter les instructions d'utilisation du fournisseur ;
  2) Mettre en place les mesures de surveillance que le fournisseur a indiquées ;
  3) S'assurer que les données d'entrées sont pertinentes et adéquates ;
  4) Avertir le fournisseur ou, à défaut le distributeur, le cas échéant :
     - que l'instruction entraîne un risque sur la santé et la sécurité ou les droits fondamentaux des consommateurs, à l'environnement, à la sécurité et aux intérêts publics;
     - en cas de dysfonctionnement ou d'incident grave qui porte atteinte aux droits fondamentaux.
  5) Conserver, lorsqu'ils sont sous leur contrôle, les journaux générés automatiquement.

- S'il modifie substantiellement le système d'IA à haut risque, l'utilisateur est **soumis aux mêmes obligations que le fournisseur** par création d'un nouveau système d'IA à haut risque.

B. Régime du système d'IA à haut risque

2- Sanctions et responsabilité

2.1. Sanctions (art. 71-72)

(I) PÉNALITÉS INFLIGÉES AUX OPÉRATEURS

Les Etats membres peuvent imposer les amendes administratives suivantes (le montant retenu étant le plus élevé) :

- **30 M € d'amende ou jusqu'à 6% du CA annuel mondial total :**
  - Non-respect de l'interdiction des pratiques d'intelligences artificielle (article 5);
  - Non-conformité du système d'IA aux mesures de gouvernance des données (article 10).

- **20 M € d'amende ou jusqu'à 4% du CA annuel mondial total :**
  - Non-respect de toute autre exigence ou obligation prévue par le Règlement.

- **10 M € d'amende ou 2% du CA annuel mondial total:**
  - La fourniture d'informations incorrectes, incomplètes ou trompeuses aux organismes notifiés et aux autorités nationales compétentes.

(II) CRITÈRES PRIS EN COMPTE

- Nature, gravité, durée de l'infraction et ses conséquences,
- Si des amendes administratives ont déjà été appliquées pour la même infraction
- Taille et part de marché de l'opérateur qui commet l'infraction.

2.2. Responsabilité (hors Règlement)

Contrairement à l'homme, les IA ne possèdent aucune personnalité juridique, ce qui interdit, dans la législation actuelle, toute possibilité d'indemnisation du dommage par l'IA.

Quel type de régime juridique appliquer, en l'absence de décision rendue à ce jour ?

- la **responsabilité du fait des choses**, qui va dépendre du gardien de la chose selon la distinction structure / comportement :

Exemple 1 : Utilisateur d'une IA lui délivrant des résultats financiers incohérents au regard des données sources – exactes et vérifiées – mises à sa disposition, pourrait engager la responsabilité du fournisseur de l'IA en raison d'un défaut de structure du système à sa conception.
Exemple 2 : Utilisateur d'une IA qui en fait un mauvais usage ou un usage détourné, entraînant un incident grave, pourrait engager la responsabilité de l'utilisateur de l'IA en raison d'un vice de comportement de ce dernier.

→ *Ouvrier tué en voulant installer une robot sur une chaîne de montage dans une usine de Volkswagen en 2015, dans lequel il semblerait que l'accident serait dû à une erreur humaine et non à un dysfonctionnement du robot.*
→ *Accident survenu en Arizona en mars 2021 lors duquel l'un des modèles autonomes de Uber a percuté un piéton, décédé des suites de ses blessures ou encore un accident survenu également en mars 2021 lors duquel la conductrice d'une voiture Tesla (Modèle X) est décédé au volant de la voiture, et pour lesquels ont été pointés le comportement des victimes.*

- la **responsabilité du fait des produits défectueux**, qui instaure une responsabilité de plein droit du producteur pour tout dommage causé par un défaut de sécurité du produit.

☑ Application cumulative des dispositions du Règlement IA et des dispositions relatives à la responsabilité des prestataires de services intermédiaires (modifiée par la LCEN)
☒ Pour les établissements de crédit, renvoi aux dispositions relatives aux partages des responsabilités prévues par la Directive 2013/36/UE concernant les obligations du fournisseur, notamment transposée par la loi n° 2014-1 du 2 janvier 2014 habilitant le Gouvernement à simplifier et sécuriser la vie des entreprises.

CONCLUSION :

Le Règlement harmonisant les règles en matière d’intelligence artificielle entrera prochainement en vigueur.

Il est donc fortement recommandé aux différents acteurs de s’y préparer activement.

L’ÉQUIPE DU DROIT IMMATÉRIEL & NUMÉRIQUE

Laurent Badiane
Avocat associé

Matthieu Bourgeois
Avocat associé

Julie Dehavay
Avocat

Lisa Bataille
Avocat

Sophie de Kermenguy
Avocat

Publications

Le Département IP-IT a conçu **la Lettre du DPO**, lettre d'information mensuelle dont il gère en interne la rédaction, et qui a pour ambition de permettre à tous ses lecteurs (DPO, mais aussi tous les juristes, responsables compliance, DSI, RSSI, et responsables métiers...) de se tenir informés à travers :

- ✓ des informations pratiques (interviews, éclairages…),
- ✓ des actualités juridiques et métiers (tendances, brèves, agenda),
- ✓ des points de vue originaux sur cette matière qui nécessite réflexion et échanges interdisciplinaires.

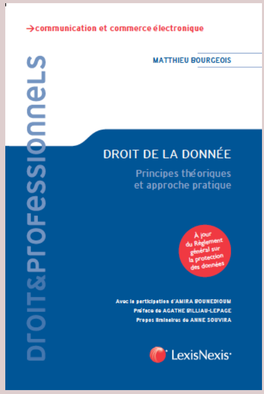
Pour vous abonner à notre Lettre du DPO
✉ ldpo@kleinwenner.eu

Les membres du département IP/IT collaborent régulièrement avec des revues juridiques de renom, en rédigeant des commentaires, articles et études sur des textes législatifs ou réglementaires ainsi que des décisions de jurisprudence, notamment auprès des maisons d'édition suivantes :

- ✓ LexisNexis (JCPE, JCPG, Revue Internationale de la Compliance et de l'Ethique, Cahier Législatif…)
- ✓ Expertises

OUVRAGE:

« Droit de la Donnée : principes théoriques et approche pratique » (LexisNexis, 2017, M. Bourgeois)



MERCI POUR VOTRE ATTENTION!

Matthieu Bourgeois
Avocat-Associé

matthieu.bourgeois@kleinwenner.eu

Pour en savoir plus sur notre cabinet, scannez ici: