AVOCATS
BARREAU
• PARIS

ORDRE DES AVOCATS DE PARIS

Quand l'IA rencontre la vie privée chronique d'un duo annoncé

Séance du 16/12/2024

Commission Droit & Ethique de l'IA

aurele avocats IT

AVOCAT

Présenté par

Florence Ivanier
Avocat à la Cour
DPO

Compétences :
- Droit de la protection des données - IA
- Droit du numérique – IT – Projets de transformation digitale

Debora Cohen
Avocat à la Cour
DPO
Mandataire d'artistes

Compétences :
- Données personnelles / IA
- Propriété intellectuelle
- Droit des medias

aurele IT avocats

AVOCAT

SOMMAIRE

Introduction

Contexte

- **Risques** : discrimination, désinformation, atteintes à la vie privée, biais algorithmiques, manipulation des comportements, surveillance de masse (etc.)
- **Défis posés par l'IA générative** : entraînement des algorithmes grâce aux jeux de données

Règlement IA *(ou AI Act)*

- entrée en vigueur le 1er août 2024
- entrée en application progressive

Objectifs du RIA

- poser un cadre de responsabilité afin de renforcer la confiance sur le marché européen
- instaurer les garanties d'une IA éthique et respectueuse des droits fondamentaux
- harmoniser le cadre juridique au sein de l'U E
- protéger les droits fondamentaux, la santé et la sécurité des citoyens de l'UE
- soutenir l'innovation y compris des PME et start-up
- sanctionner la non-conformité

Introduction

Champ d'application du RIA

=> entreprises qui souhaitent développer et/ou commercialiser un SIA et qui visent le marché européen :

- siège social dans l'UE
- ou siège social hors UE tiers dès lors que le résultat du SIA est utilisé dans l'UE

=> SIA et algorithmes déjà utilisés dans l'entreprise

Périmètre d'application du RGPD à l'IA

Dès lors que la base d'entraînement de l'IA contient des données personnelles

=> que l'usage opérationnel en phase de déploiement soit défini dès la phase de développement ou qu'il s'agisse de systèmes d'IA à usage général (« GPAI ») adaptés pour différents cas d'usage

=> que l'apprentissage soit réalisé « une fois pour toutes » ou en continu

Introduction

Notions clés du RIA :

- **Système d'IA :** système "*conçu pour fonctionner avec différents niveaux d'autonomie et qui peut faire preuve d'adaptabilité après son déploiement, et qui, (…) déduit, à partir des données qu'il reçoit, comment générer des résultats tels que des prédictions, du contenu, des recommandations ou des décisions (…)* (art. 3.1 RIA)

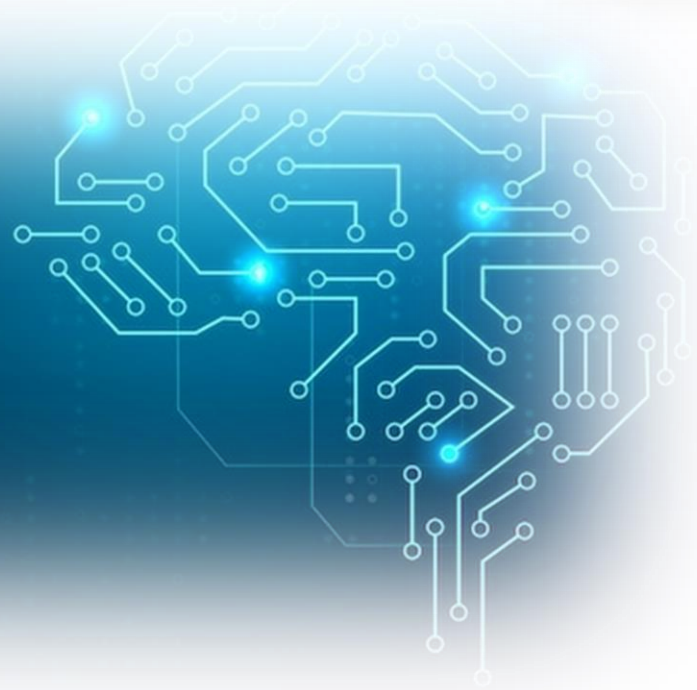
- **Modèle d'IA à usage général** : « *modèle d'IA entraîné à l'aide d'un grand nombre de données utilisant l'auto-supervision à grande échelle, qui présente une généralité significative et est capable d'exécuter de manière compétente un large éventail de tâches distinctes (…) et qui peut être intégré dans une variété de systèmes ou d'applications en aval (…)* » (article 3.63 RIA)

- **Opérateurs :**
  - **Fournisseur** : organisme qui développe ou fait développer un SIA ou un modèle d'IA à usage général et le met sur le marché ou le met en service sous son propre nom ou sa propre marque, à titre onéreux ou gratuit ;
  - **Déployeur :** organisme importateur, distributeur ou utilisateur, utilisant sous sa propre autorité un SIA (sauf utilisation dans le cadre d'une activité à caractère non professionnel)

Quelques cas d'usage

- *entraîner des SIA aux fins de créer des logiciels d'aide au diagnostic médical*
- *utiliser des caméras augmentées pour repérer notamment les risques d'actes de terrorisme (utilisé durant les JOP2024)*

Partie I - Articulation entre protection des données personnelles et RIA



aurele IT avocats

AVOCAT

I - Articulation entre protection des données

1. Le RIA mentionne explicitement l'application du RGPD

L'article 2.7 du RIA énonce :

« *Le droit de l'Union en matière de protection des données à caractère personnel, de respect de la vie privée et de confidentialité des communications s'applique aux données à caractère personnel traitées en lien avec les droits et obligations énoncés dans le présent règlement. Le présent règlement n'a pas d'incidence sur le règlement (UE) 2016/679 (…)* ».

➡ Sans préjudice d'autres règles

aurele IT avocats

AVOCAT

I - Articulation entre protection des données personnelles et RIA

2. L'application du RGPD aux SIA et aux modèles d'IA selon leur niveau de risque

REGLES APPLICABLES DU RIA	APPLICATION DU RGPD
Pratiques d'IA interdites	Systématiquement, toutes les pratiques interdites supposant le traitement de données personnelles.
Modèle d'IA à usage général (y compris à risque systémique)	Quasi-systématiquement, les modèles d'IA à usage général se fondant le plus souvent sur l'utilisation de données personnelles pour leur entrainement
Systèmes d'IA à haut risque	Dans de très nombreux cas (avec des exceptions notables comme pour les systèmes d'IA des infrastructures critiques, des véhicules agricoles, des ascenseurs, etc.)
Systèmes d'IA à risque spécifique en matière de transparence	Dans certains cas, en particulier les systèmes destinés à interagir directement avec des personnes physiques

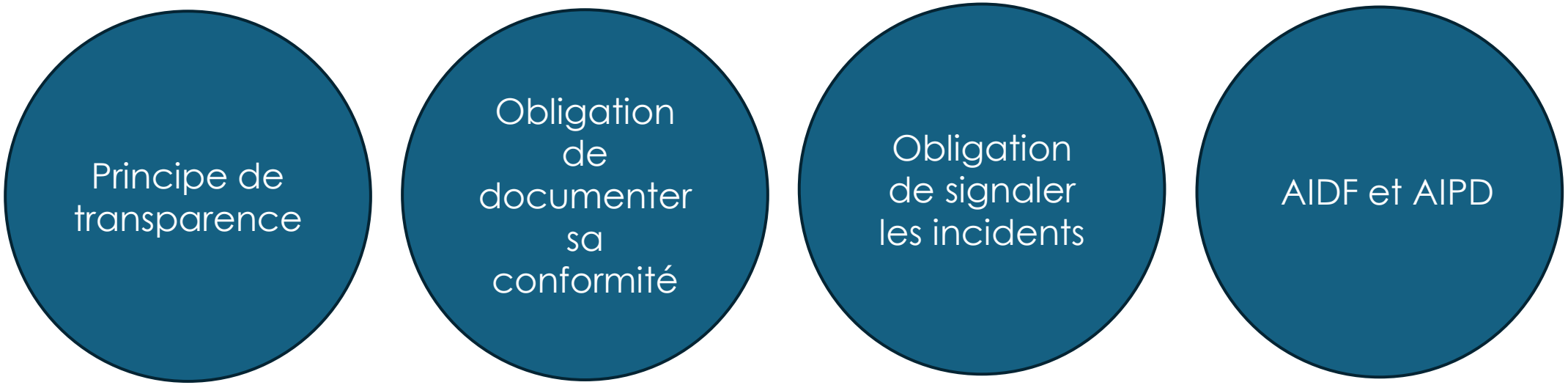
I - Articulation entre protection des données personnelles et RIA

3. Les points de divergences entre le RIA et le RGPD

	RIA	RGPD
Champ d'application	Le développement, la mise sur le marché ou le déploiement de systèmes et modèles d'IA	Tout traitement de données personnelles indépendamment des dispositifs techniques utilisés (dont les traitements visant à développer un modèle ou système d'IA (données d'entrainement), et les traitements réalisés au moyen d'un système d'IA)
Acteurs visés	Principalement les fournisseurs et déployeurs de systèmes d'IA (dans une moindre mesure les importateurs, distributeurs et mandataires)	Responsables de traitements et sous-traitants (dont les fournisseurs et déployeurs soumis au RIA)
Approche	Approche par les risques pour la santé, la sécurité ou les droits fondamentaux, notamment à travers la sécurité des produits et la surveillance du marché en ce qui concerne les systèmes et modèles d'IA	Approche fondée sur l'application de grands principes, l'évaluation des risques et la responsabilisation (accountability)
Modalité principale de l'évaluation de la conformité (non exhaustif)	Évaluation de conformité interne ou par un tiers, notamment au moyen d'un système de gestion des risques et au regard de normes harmonisées	Principe de responsabilité (documentation interne) et outils de la conformité (certification, code de conduite)
Principales sanctions applicables	Retrait du marché ou rappel de produits Amendes administratives pouvant aller jusqu'à 35 millions d'euros ou 7% du chiffre d'affaires annuel mondial	Mise en demeure (pouvant enjoindre de mettre le traitement en conformité, de le limiter temporairement ou définitivement, y compris sous astreinte) Amendes administratives pouvant aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial

I - Articulation entre protection des données personnelles et RIA

4. Les points communs entre le RIA et le RGPD



I - Articulation entre protection des données personnelles et RIA

5. Le RIA remplace le RGPD sur certains points spécifiques

L'utilisation de données biométriques à des fins répressives dans des espaces accessibles au public et en temps réel

Le traitement de données sensibles aux fins de correction de biais

La réutilisation de données dans le cadre des bacs à sable règlementaires

I - Articulation entre protection des données personnelles et RIA

6. La compétence de la CNIL

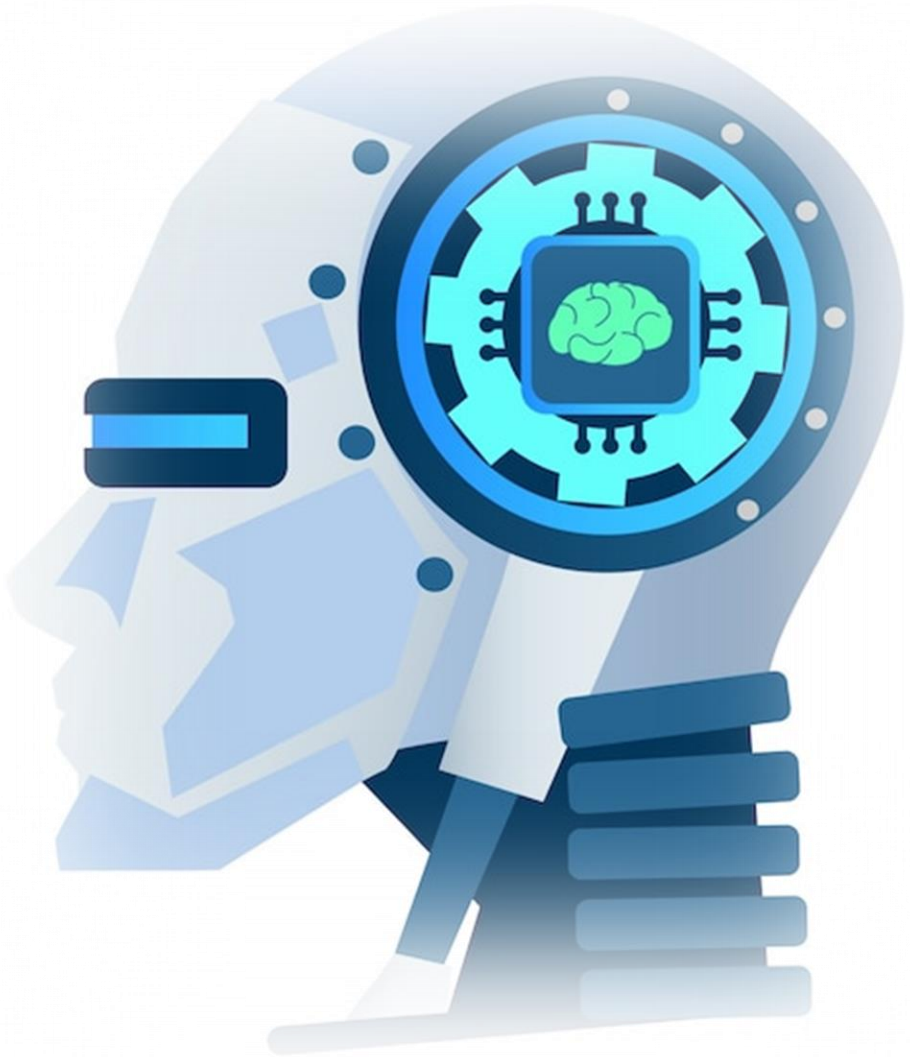
- Compétence pour traiter des manquements du RGPD par les fournisseurs et déployeurs de systèmes d'IA

  Exemple avec la société Clearview AI :

  - Clearview AI aspirait des images sur internet et au sein de dispositifs de vidéosurveillance pour développer son logiciel de reconnaissance faciale
  - La Cnil constate la violation des principes du RGPD
  - Elle inflige une amende de 20 millions d'euros à Clearview AI

- Concurrence avec les autorités de surveillance du marché

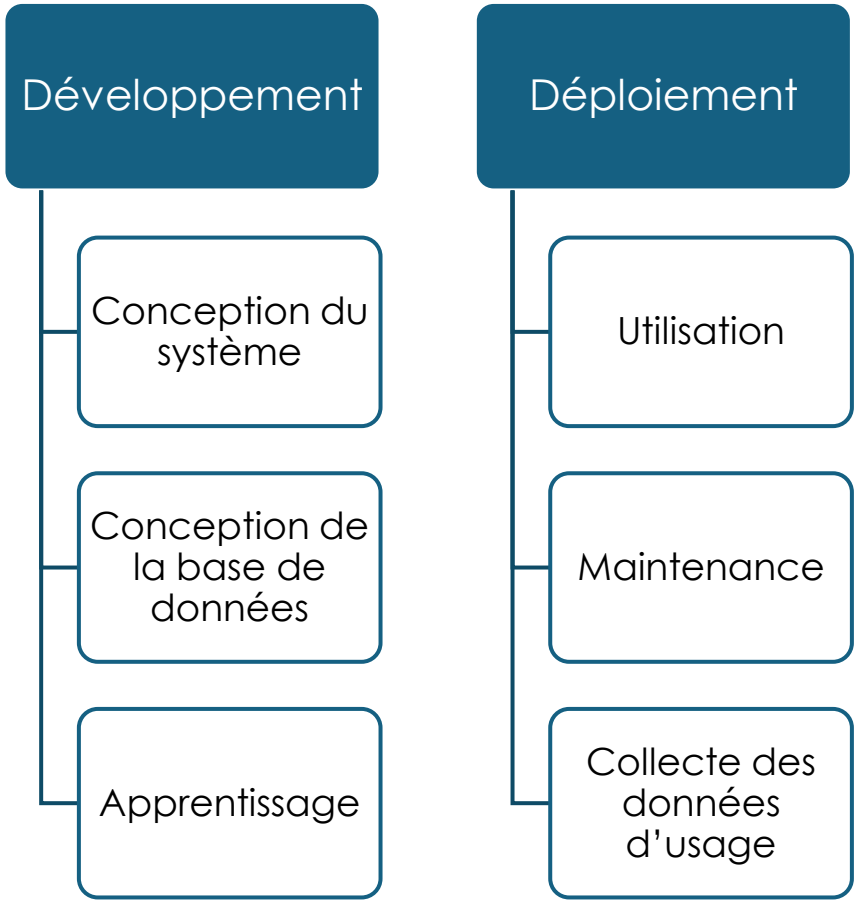
Partie II - Développer et déployer un SIA en respectant la protection des données



aurele IT avocats

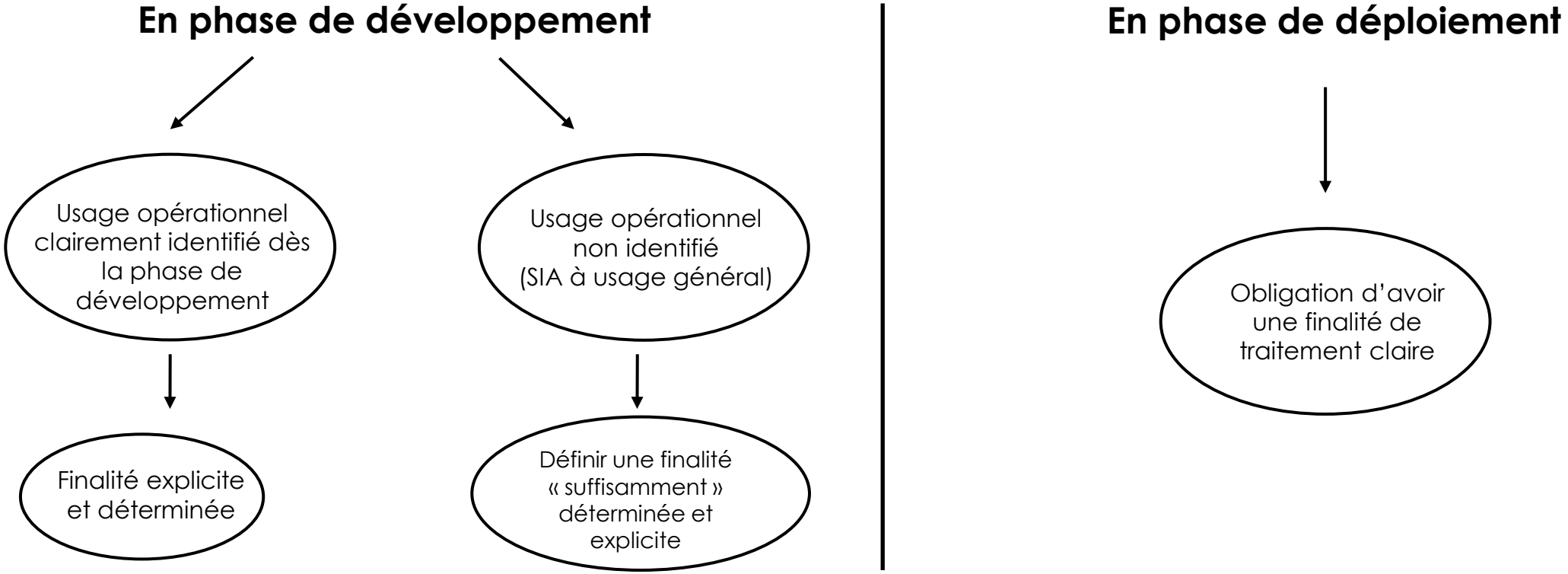
AVOCAT

II - Développer et déployer un SIA en respectant la protection des données



II - Développer et déployer un SIA en respectant la protection des données

1. Les finalités de traitement



II - Développer et déployer un SIA en respectant la protection des données

2. Les qualifications

❖ **Responsable de Traitement** Le fournisseur :

(i) qui constitue la base d'apprentissage à partir de données qu'il a sélectionnées pour son propre compte

(ii) ou qui confie la constitution d'une telle base à un prestataire au travers d'instructions précises

⇒ *Ex. le fournisseur d'une IA fondée sur un modèle de langage (LLM) entraîné à partir de données publiquement accessibles est responsable de la réutilisation des données*

❖ **Sous -Traitant**

Le fournisseur qui développe un SIA pour le compte d'un client et sur ses instructions

⇒ *Ex. reçoit des instructions précises portant sur les sources et les catégories de données, assorties d'exigences de documentation*

Focus sur la réutilisation de données collectées par un autre organisme

Le diffuseur des données qui met à disposition les données à des fins de réutilisation et le réutilisateur qui exploite cette base pour son propre compte sont deux responsables distincts.

aurele IT avocats | AVOCAT

II - Développer et déployer un SIA en respectant la protection des données

2. Les qualifications

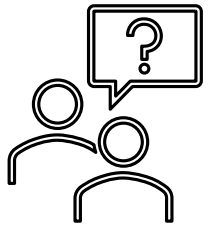
❖ Responsables conjoints

Critère: dès lors qu'une base de données est alimentée par plusieurs responsables pour un objectif commun et non des objectifs propres et distincts

Exemple: consortium composé de:
(a) le fournisseur d'un logiciel de traitement d'images par IA
(b) le fournisseur d'un dispositif video
et (c) une commune
=> mettent en place un dispositif de cameras augmentées pour analyser le flux de circulation de véhicules dans une commune. Le dispositif permet l'apprentissage du logiciel par les données collectées en temps réel.
⇒ choix conjointement d'alimenter la base de données par les données collectées afin d'entraîner le SIA. Ces fournisseurs n'agissent pas uniquement pour le compte de la commune dès lors que l'amélioration du logiciel leur bénéficient également

II - Développer et déployer un SIA en respectant la protection des données

3. Les bases légales



Quelles sont les bases légales prévues par le RGPD ?

- consentement
- contrat
- obligation légale
- mission d'intérêt public
- intérêt légitime
- sauvegarde des intérêts vitaux

II - Développer et déployer un SIA en respectant la protection des données

3. Les bases légales

L'exemple du web scrapping

Choix de la base légale : Intérêt légitime du responsable de traitement

conséquences

Mesures obligatoires au titre du principe de minimisation des données

- Définir en amont des critères de collecte des données
- Supprimer les données non pertinentes collectées malgré les mesures précédentes.

Garanties supplémentaires pour limiter l'atteinte aux droits et libertés des personnes

- Prévoir la possibilité pour les personnes concernées de s'opposer au traitement de manière discrétionnaire
- Diffuser le plus largement possible les informations relatives à la collecte et aux droits des personnes
- Inscrire ses coordonnées dans le registre qui pourrait être mis en place par la CNIL, afin de recenser les entreprises ayant recours à des outils de moissonnage

(liste non exhaustive)

II - Développer et déployer un SIA en respectant la protection des données

4. Analyse d'Impact sur la Protection des Données

Rappel : dans quel cas une AIPD est-elle requise?

- **Si le traitement de données répond à au moins 2 des critères suivants:**
  - recours à la notation (rendement au travail de la personne, sa santé, ses préférences ou centres d'intérêts, sa fiabilité ou son comportement, sa localisation et ses déplacements)
  - prise de décision automatisée avec effets significatifs sur la personne concernée
  - surveillance systématique de personnes
  - collecte de données sensibles
  - concerne des personnes vulnérables (salariés, mineurs)
  - traitement à grande échelle
  - croisement d'ensembles de données
  - utilisation d'une technologie innovante (utilisation d'objets connectés, de systèmes de reconnaissance des empreintes digitales et de reconnaissance faciale)
  - le traitement en lui-même empêche la personne concernée d'exercer un droit ou de bénéficier d'un service / contrat
- **Ou si le traitement fait partie de ceux identifiés par la CNIL comme requérant une AIPD**: liste-traitements-avec-aipd-requise-v2 (002).pdf

r

II - Développer et déployer un SIA en respectant la protection des données

4. Analyse d'Impact sur la Protection des Données

A retenir:

⇒ Le développement d'un modèle de fondation ou d'un système d'IA à usage général, nécessite la réalisation d'une AIPD lorsqu'il implique un traitement de données personnelles

⇒ le développement ou déploiement d'un SIA à haut risque implique la réalisation d'une AIPD lorsqu'is impliquent un traitement de données personnelles

Focus sur 2 des critères entraînant l'obligation d'implémenter une AIPD dans le contexte d'un SIA

- **grande échelle :** l'entraînement d'un SIA ne constitue pas nécessairement un traitement à grande échelle

- **usage innovant :**
  => relève de l'usage innovant une technique d'IA encore nouvelle ex: deep learning
  => n'en relève pas une technique d'IA validée expérimentalement depuis plusieurs années et éprouvée en conditions réelles

II - Développer et déployer un SIA en respectant la protection des données

5. L'information des personnes

Contenu de l'information RGPD

- Identité et coordonnées du responsable de traitement
- Finalité et la base légale du traitement
- Destinataires ou à minima les catégories de destinataires des données
- Durée de conservation des données
- Droits des personnes concernées
- Durée de conservation des données
- Droit d'introduire une réclamation auprès de la CNIL
- Information sur la source des données et les données traitées si réutilisation des données

Contenu de l'information RIA

- Destinataires ou catégories de destinataires du modèle
- Durée de conservation du modèle
- Droits des personnes concernées sur le modèle
- Pour les systèmes de reconnaissance des émotions ou de catégorisation biométrique, information des personnes concernées quant au fonctionnement du système
- Information des personnes concernées quant aux risques liés à la reconstruction des données à partir du modèle et des mesures prises par le fournisseur d'IA générative au cas où ces risques se manifesteraient

II - Développer et déployer un SIA en respectant la protection des données

6. La collecte et la conservation des données

Focus sur le moissonnage (web scraping)

- Définir des critères précis en amont du traitement
- Ne collecter que des données pertinentes et supprimer les autres au plus tôt

Nettoyage: constituer une base de qualité

- Identifier les données pertinentes portant sur les données, les métadonnées et les caractéristiques

Durées de conservation

- Fixer des durées distinctes pour la phase de développement du SIA et l'amélioration du produit

II - Développer et déployer un SIA en respectant la protection des données

7. L'annotation des données

Attribuer une description (étiquette) à chaque donnée qui servira de vérité de terrain (ground truth)

Ex. afin d'entraîner un modèle IA de reconnaissance intégré dans un assistant vocal, des enregistrements sont annotés avec l'identité du locuteur

Enjeux de l'annotation: minimisation et exactitude

- les annotations doivent se limiter aux informations strictement nécessaires à l'entraînement du modèle
- choisir des labels adaptés à la finalité visée pour le déploiement du SIA
- définir un protocole d'annotation documentée
- informer les personnes des opérations d'annotation

II - Développer et déployer un SIA en respectant la protection des données

8. Le principe de sécurité des données

Les aspects de la sécurité des données des SIA

- La confidentialité des données
- La performance et l'intégrité du système
- La sécurité générale du système d'information

II - Développer et déployer un SIA en respectant la protection des données

8. Le principe de sécurité des données

Les mesures de sécurité spécifiques aux SIA

Sur les données d'entrainement

- Documentation sur les modifications apportées aux jeux de données

Sur le développement du système

- Recommander un audit de sécurité
- Adresser le guide RGPD dédié aux développeurs, élaboré par la CNIL

Sur le fonctionnement du système

- Information sur les contextes d'usage prévu
- Information sur l'interprétation des résultats

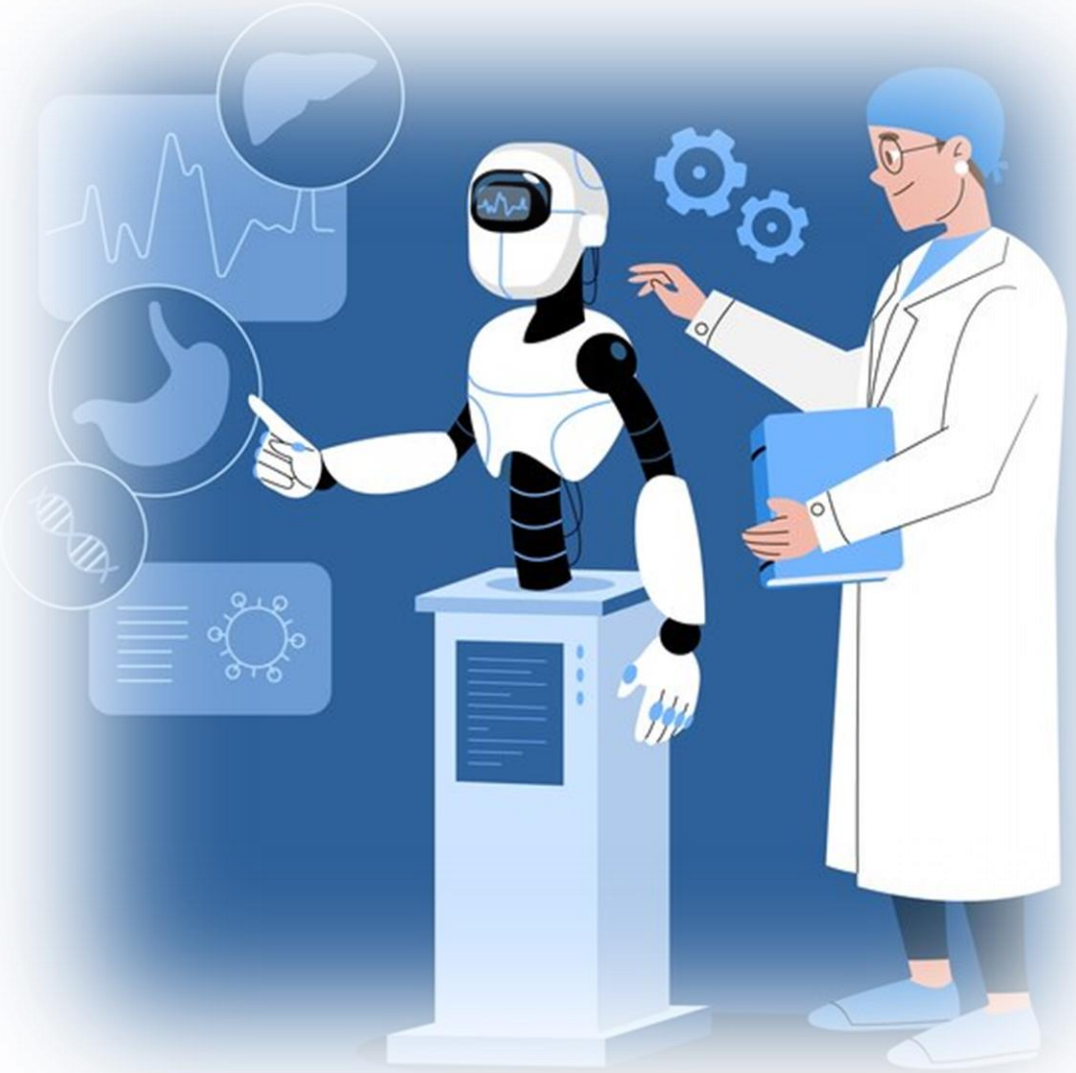
(liste non exhaustive)

II - Développer et déployer un SIA en respectant la protection des données

9. Le privacy by design & by default

II - Développer et déployer un SIA en respectant la protection des données

Partie III - Cas d'usage Doctolib : le déploiement de l'assistant de consultation

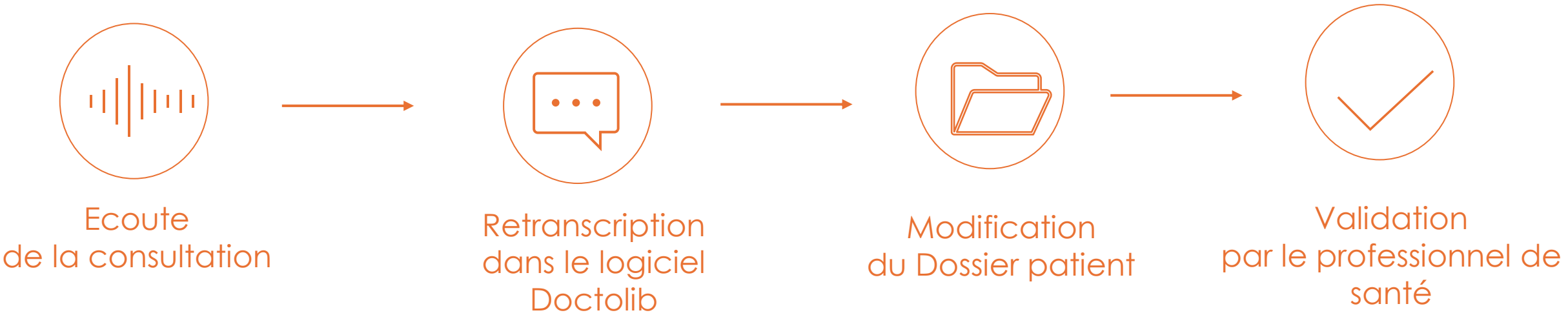


aurele IT avocats

AVOCAT

III - Cas d'usage
Doctolib : le déploiement de l'assistant de consultation

1. Présentation de l'assistant de consultation



III - Cas d'usage
Doctolib : le déploiement de l'assistant de consultation

2. Description du traitement - Finalités

Description du traitement

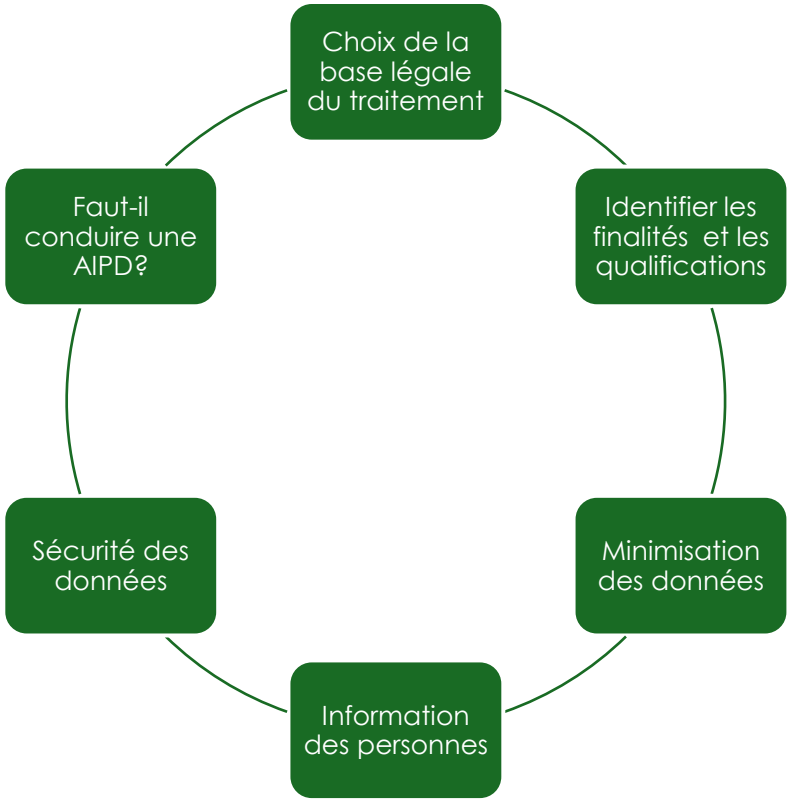
1. enregistrement enclenché par le praticien
2. l'IA écoute la consultation
3. en fin de séance, une fois l'enregistrement coupé, l'assistant numérique fournit un rapport complet avec le motif de la consultation, le dialogue entre le médecin et son patient et le diagnostic, formulé par le praticien.

Finalités :

- Transcrire l'enregistrement
- Générer des suggestions et alimenter le dossier médical du patient
- Permettre un usage optimal par le praticien de l'enregistrement réalisé
- Entraîner le système d'IA constitué par l'assistant de consultation afin d'améliorer le produit

III - Cas d'usage
Doctolib : le déploiement de l'assistant de consultation

3. Enjeux relatifs à la protection des données personnelles



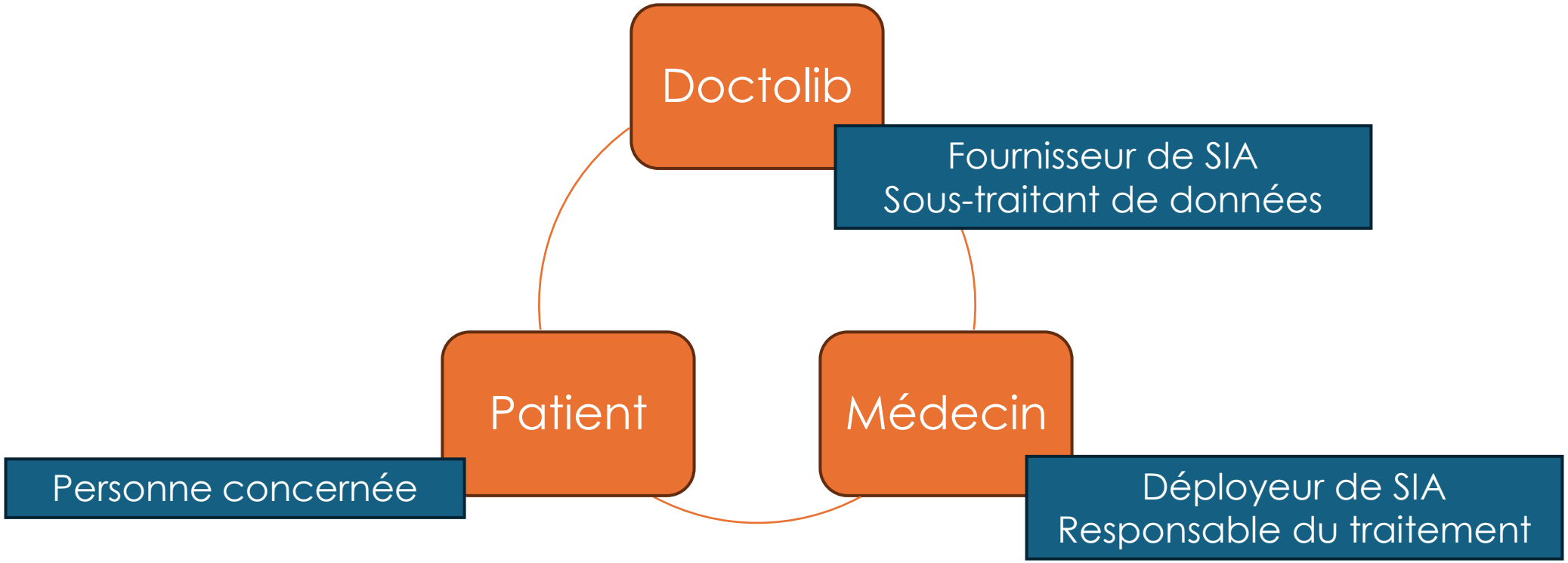
III - Cas d'usage
Doctolib : le déploiement de l'assistant de consultation

4. Questions du cas pratique

- **Quelle qualification ?**
- **Quelle base légale ? Pourquoi ?**
- **Faut-il mener une AIPD préalablement à la mise en place du système ?**
- **Quels risques spécifiques sur le plan de la protection des données ?**
- **Quelle information des personnes ?**

III - Cas d'usage
Doctolib : le déploiement de l'assistant de consultation

Qualifications



III - Cas d'usage
Doctolib : le déploiement de l'assistant de consultation

Réponse - Qualification:

Doctolib se qualifie de Responsable de Traitement dans sa politique de confidentialité pour ce qui concerne les traitements de données liés par ex. à la création du compte utilisateur ou encore à la création d'un annuaire des acteurs de santé ou à la mise en œuvre du service de téléconsultation

Notre analyse nous conduit à estimer que Doctolib agit en qualité de ST concernant la fourniture de l'assistant de consultation. Une qualification de RT conjoint avec le praticien pourrait également être retenue.

Doctolib semble retenir une qualification de sous traitant, ce qui correspond à la qualification qu'il a retenue pour les autres types de services déjà fournis aux praticiens.

Quelle est la position des concurrents ex. Nabla Copilot: se qualifie de ST y compris sur le traitement de réutilisation des données pour amélioration du SIA.

III - Cas d'usage
Doctolib : le déploiement de l'assistant de consultation

Réponse – Base légale

Le consentement est la base légale sur laquelle repose l'enregistrement.

Préciser la granularité nécessaire des finalités.

Retenir les limites du consentement (base légale précaire, pouvant être retiré à tout moment)

Le cas échéant, identifier quelles autres bases légales sont utilisées, pour quel traitement?

III - Cas d'usage
Doctolib : le déploiement de l'assistant de consultation

Réponse: faut-il mener une AIPD préalablement à la mise en place du système ?

Les critères à retenir:

Quel niveau de risque est-il retenu pour le système IA mis en œuvre?

Le traitement réunit au moins 2 critères de la liste du CEPD :

- Le critère de grande échelle est rempli. Le traitement de collecte de données sensibles également.
- L'assistant de consultation doit-il être qualifié de technologie innovante?

Dans l'hypothèse où Doctolib retiendrait une qualification de sous-traitant, la responsabilité de mener une AIPD pèserait-t-elle sur les praticiens?

III - Cas d'usage
Doctolib : le déploiement de l'assistant de consultation

Réponse – Quels risques spécifiques sur le plan de la protection des données ?

Risque de suggestion de contenu erroné, qui serait inclus dans le transcript de la consultation et le compte rendu du praticien

Risque de biais du SIA si celui-ci n'a pas été entraîné sur certaines spécialités médicales et spécificités de vocabulaire.

III - Cas d'usage
Doctolib : le déploiement de l'assistant de consultation

Réponse – Quelle information des personnes ?

- Data Processing Agreement avec les praticiens
- Politique de confidentialité accessible sur le site pour informer les patients

Merci pour votre attention

Florence IVANIER
Avocat à la Cour
DPO

T. : +33 (0) 1.89.16.81.12
P.: +33 (0)6.16.09.25.07
fivanier@aurele-it.fr

6 rue Jean de la Fontaine 75016 Paris
www.aurele-it.fr

Debora Cohen
Avocat à la Cour
DPO

T. : +33 (0) 1.40.06.92.00
P. : +33 (0) 6.50.08.23.47
debora.cohen@dcavocat.com

5 rue Georges Berger 75017 Paris
https://www.dcavocat.com/