11/06/2024

IBM TechXchange

SZLEPER HENRY NAUMANN AVOCATS

IA

Quelles règles, quels risques, quelle gouvernance ?

Guillaume Henry
Docteur en droit
Avocat à la Cour
g.henry@shna.law

Victor Benincasa
Avocat à la Cour
v.benincasa@shna.law

I. RÈGLES – Textes

SZLEPER HENRY NAUMANN AVOCATS

Règlement IA (AI Act)

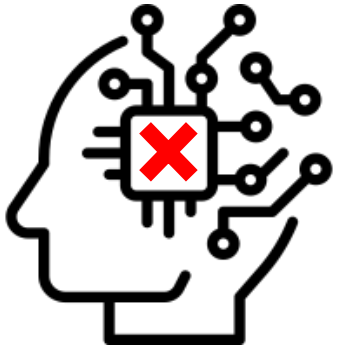
Adoption par le PE (13/03/2024)
Adoption par le Conseil (21/05/2024)
Publication JO (…)

Entrée en vigueur : 2024-2025
Application uniforme par Etats membres

Proposition de directive sur la responsabilité en matière d'IA

Proposition (29/09/2022)
Première lecture par le PE et le Conseil

Entrée en vigueur : pas avant 2025
Transposition par Etats membres



Proposition de directive sur la responsabilité du fait des produits défectueux

Proposition (29/09/2022)
Première lecture par le PE et le Conseil

Entrée en vigueur : pas avant 2025
Transposition par Etats membres

g.henry@shna.law
v.benincasa@shna.law

I. RÈGLES – Textes

Executive Order (E.O.) Safe, Secure, and Trustworthy Development and Use of AI

Publié par Adm. Biden (30/10/2023)

- Tests de sécurité (partage des résultats)
- Déclarations d'intention (tests standardisés ; étiquetage de contenus générés par IA ; respect vie privée + non-discrimination)

Generative AI Copyright Disclosure Act (bill)

Proposition de loi (09/04/2024)

- Transparence quant à l'utilisation de créations protégées par le droit d'auteur pour entraîner GenAI.
→ application rétroactive.

Droit particulier à chaque État fédéré

Session législative de 2023

25 États ont présenté des projets de loi relatifs à l'IA et 15 États ont adopté des résolutions ou promulgué des lois (Protection contre les SIA dangereux ; Protection des données ; Protection c/ discriminations ; Transparence).

g.henry@shna.law
v.benincasa@shna.law

I. RÈGLES – Textes

Veille règlementaire

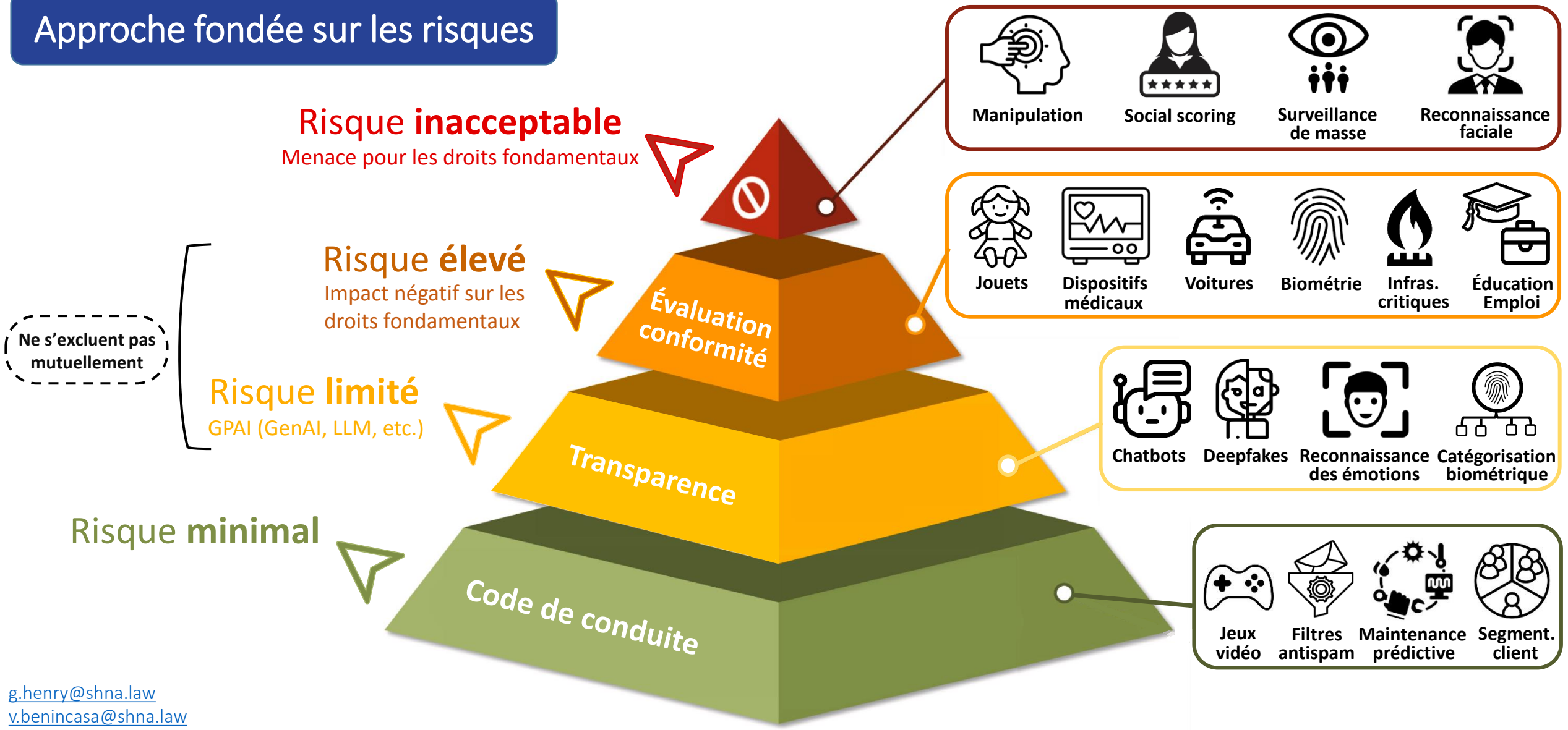
Veille au niveau international à réaliser régulièrement pour adapter le dispositif technique à mettre en place

g.henry@shna.law
v.benincasa@shna.law

I. RÈGLES – AI Act

SZLEPER HENRY NAUMANN AVOCATS

Approche fondée sur les risques



g.henry@shna.law
v.benincasa@shna.law

I. RÈGLES – AI Act

SZLEPER HENRY NAUMANN AVOCATS

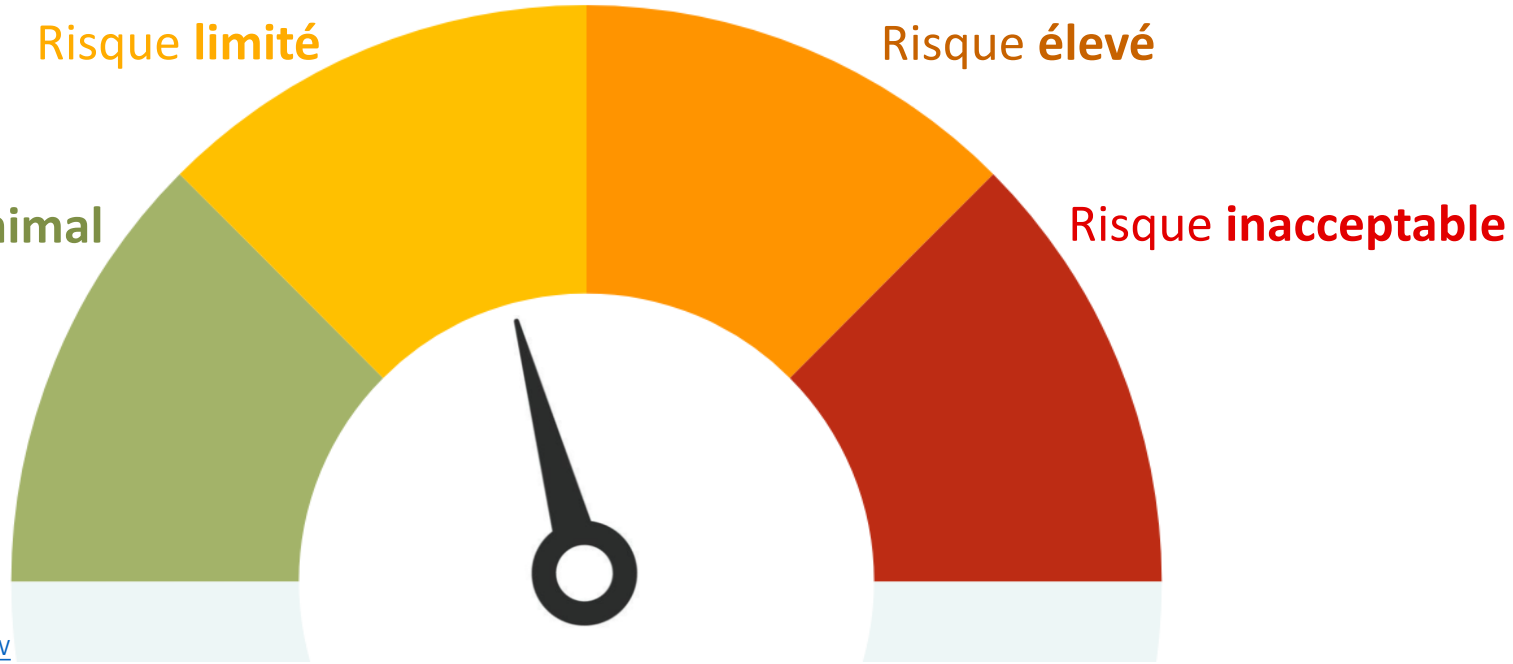
Logique de responsabilisation

Modèle combinant une auto-évaluation *ex ante* des risques et un contrôle *ex post* de l'application des règles.

Contrôle *ex post*

Autorité de surveillance

Auto-évaluation



g.henry@shna.law
v.benincasa@shna.law

I. RÈGLES – AI Act

Calendrier - Mise en conformité

Entrée en vigueur

Juin 2024

6 mois après

Déc. 2024

SIA présentant un risque inacceptable : Interdiction

12 mois après

Juin 2025

SIA présentant un risque limité : Obligation de mise en conformité

18 mois après

Déc. 2025

Commission : Acte fixant un modèle pour le plan de surveillance après commercialisation

24 mois après

Juin 2026

SIA présentant un risque élevé : Obligation de Mise en conformité

36 mois après

Juin 2027

GPAI récentes (postérieures à l'AI Act) : Obligation de Mise en conformité

Sanctions

g.henry@shna.law
v.benincasa@shna.law

I. RÈGLES – AI Act

SZLEPER HENRY NAUMANN AVOCATS

SIA à risque élevé

g.henry@shna.law
v.benincasa@shna.law

I. RÈGLES – AI Act

SZLEPER HENRY NAUMANN AVOCATS

SIA à risque limité (GPAI)

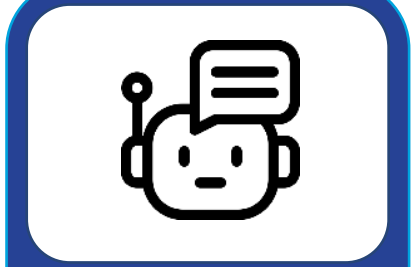
OBLIGATIONS DE TRANSPARENCE

Système de reconnaissance des émotions

- Interaction avec IA
- Fonctionnement du SIA et traitement de données perso.

Système de catégorisation biométrique

- Interaction avec IA
- Fonctionnement du SIA et traitement de données perso.



SIA à usage général (GenAI)

- Interaction avec IA
- Étiquetage des contenus générés
- Notice d'utilisation (intégration du modèle dans SIA tiers)
- Contenu utilisé pour entraîner le modèle

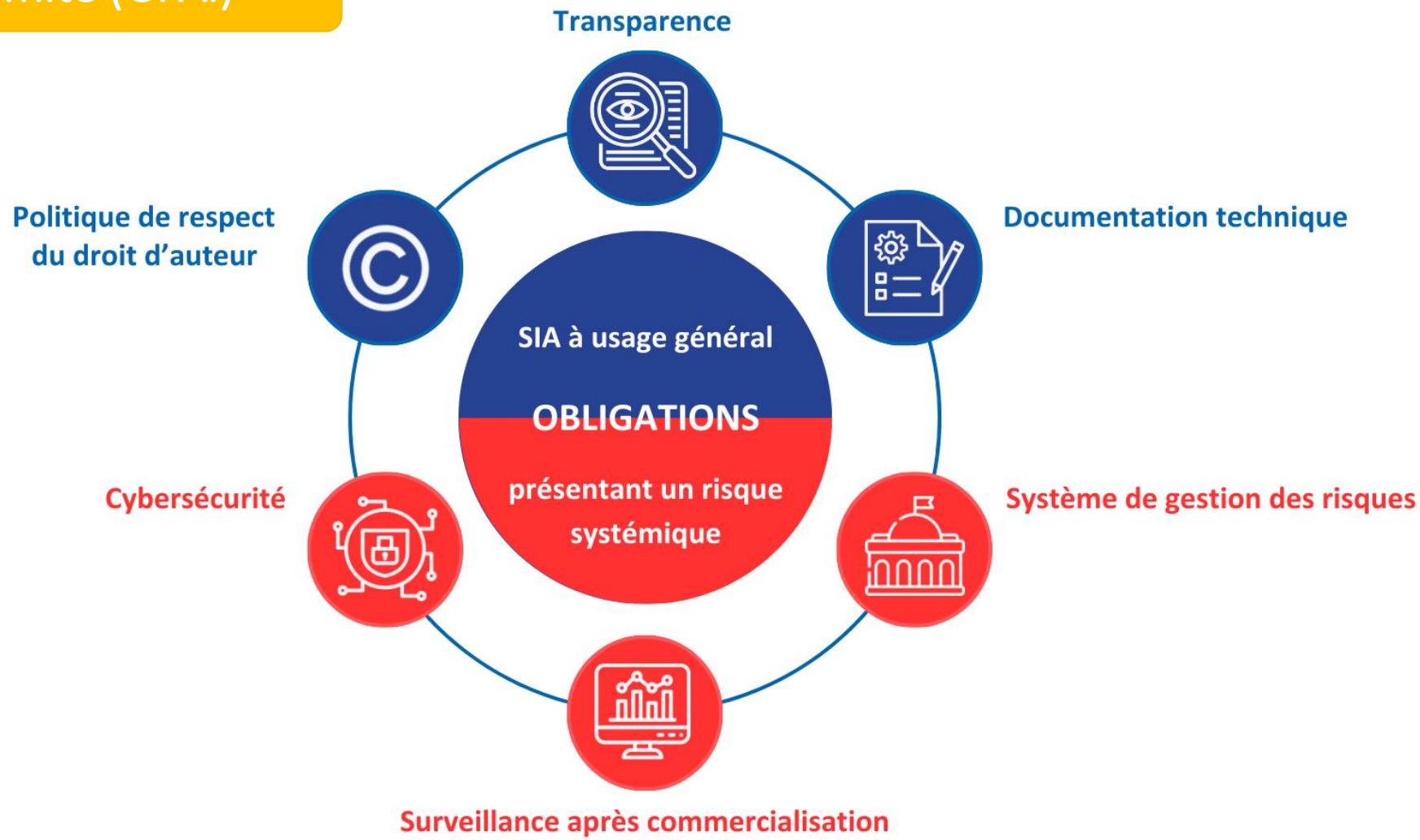
SIA à usage général présentant un risque systémique (LLM)

- Interaction avec IA
- Étiquetage des contenus générés
- Notice d'utilisation (intégration du modèle dans SIA tiers)
- Contenu utilisé pour entraîner le modèle

g.henry@shna.law
v.benincasa@shna.law

I. RÈGLES – AI Act

SIA à risque limité (GPAI)



g.henry@shna.law
v.benincasa@shna.law

II. RISQUES – Conformité

1 **Contrôle *ex post***

Autorité de surveillance

Autorité nationale (CNIL ?)
ou
Bureau de l'IA (pour GPAI)

- Évaluation de conformité
- Pouvoir de sanction

✖ **Auto-évaluation erronée**

✖ **Manquement à une ou des obligations**

2 **Sanctions**

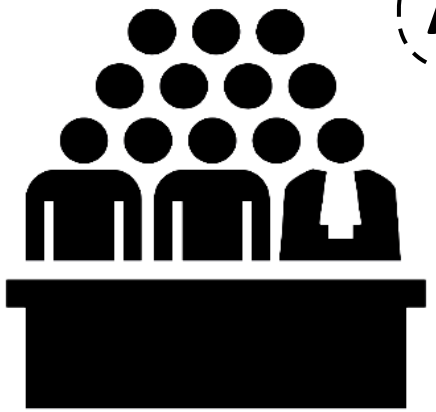
- Avertissement
- **15M€ / 3% CA mondial total**
- **15M€ / 3% CA mondial total**
- **35M€ / 7% CA mondial total**
- **Interdiction**

g.henry@shna.law
v.benincasa@shna.law

II. RISQUES – Juridique

SZLEPER HENRY NAUMANN AVOCATS

1 **Action en justice**



Tiers ayant subi un préjudice du fait de l'IA

Individus
ou
Entreprises

- ✖ **Droit d'auteur**
- ✖ **Vie privée / données personnelles**
- ✖ **Préjudice corporel, matériel, moral**
- ✖ **Conc. déloyale, secret d'affaires**

- $ **Dommages-intérêts**
- ⊘ **Interdiction**

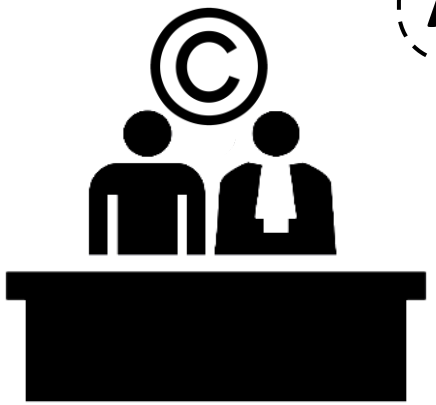
2 **Condamnations**

g.henry@shna.law
v.benincasa@shna.law

II. RISQUES – Juridique

SZLEPER HENRY NAUMANN AVOCATS

1 **Action en justice**



Titulaires de droit d'auteur ou droits voisins

Individus ou Entreprises

The New York Times VS OpenAI

❌ **Droit d'auteur**

GenAI

Jeux de données d'entraînement

2 **Condamnations** ?

AI Act
Exception 'Data mining' (fouille)

- 'Opt-out' par le titulaire ?
- Si oui, réservation des droits
  → **Autorisation nécessaire**

g.henry@shna.law
v.benincasa@shna.law

II. RISQUES – Commercial et financier

SZLEPER HENRY NAUMANN AVOCATS

Risque stratégique

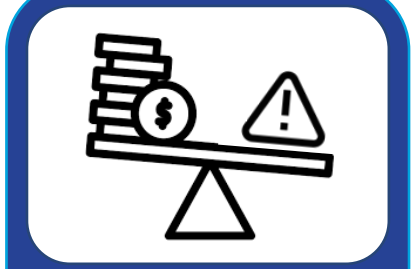
- Atteinte à la réputation
- Expérience client – Perte de confiance
- Responsabilité du fait des sous-traitants

Risque opérationnel

- Désorganisation
- Nécessité de refonte pour la mise en conformité
- Interruption d'activité

Risque de surveillance accrue

- Mesures de surveillance plus strictes
- Obligations de reporting accrues



Risque financier

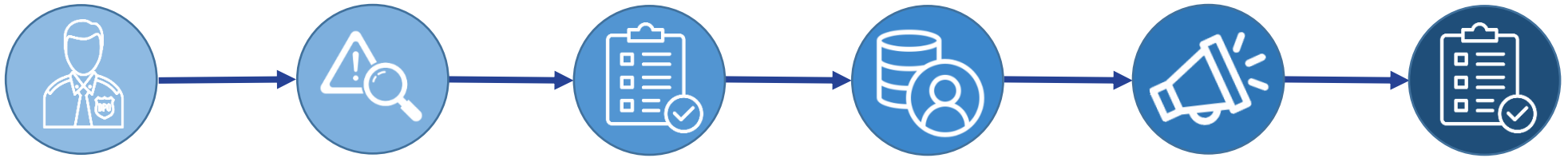
- Coûts engendrés (amendes, dommages-intérêts, mise en conformité)
- Perte de confiance des banques et investisseurs

g.henry@shna.law
v.benincasa@shna.law

III. GOUVERNANCE – Instauration

Bonnes pratiques de gouvernance

Permet de (i) *créer une sécurité juridique, commerciale et financière (maîtrise des risques)* et (ii) *d'instaurer un climat de confiance auprès des clients et investisseurs.*



Étape 1

Désignation d'un pilote

Étape 2

Évaluation du niveau de risque (au sens de l'AI Act)

Étape 3

Respect des obligations

Évaluation de la conformité pour SIA à risque élevé

Stade de développement

Étape 4

Enregistrement dans la base de données de l'UE

Étape 5

Mise sur le marché

Étape 6

Respect des obligations

Évaluation de la conformité pour SIA à risque élevé

Stade de commercialisation

g.henry@shna.law
v.benincasa@shna.law

III. GOUVERNANCE – SIA à risque élevé

SZLEPER HENRY NAUMANN AVOCATS

Respect des obligations

1. **Système de gestion des risques (ensemble du cycle de vie du SIA)** :
   - Étape 1 : Essais pendant le processus de développement (essais en conditions réelles ou bac à sable règlementaire)
   - Étape 2 : Identification et analyse des risques connus et raisonnablement prévisibles (auto-évaluation)
   - Étape 3 : Adoption de mesures appropriées et ciblées de gestion des risques

2. **Gouvernance des données** : Qualité des données de test, d'entraînement et de validation (respect de la règlementation notamment en matière de vie privée, de données personnelles, de droit d'auteur, de secret des affaires ; repérage d'éventuels biais et correction ; jeux de données représentatifs, exempts d'erreurs et complets)

3. **Documentation technique (toute la durée de vie du SIA) et Tenue des registres (journaux > 6 mois)** :
   - Description générale du SIA (logiciels, formes sous lesquelles le SIA est mis sur le marché, UI, API)
   - Description des éléments du SIA et de son processus de développement (spécifications de conception ; choix de conception et de classification ; sorties attendues ;architecture ;ressources informatiques ; jeux de données ; procédures de validation et d'essai utilisées)
   - Informations sur la surveillance, le fonctionnement et le contrôle du SIA (capacités et limites ; résultats non intentionnels et sources de risques prévisibles ; mesures de contrôle humain et de cybersécurité)
   - Description du système de gestion des risques
   - Description des modifications pertinentes apportées
   - Copie de la déclaration UE de conformité
   - Description du système en place pour évaluer les performances du système d'IA après la commercialisation

g.henry@shna.law
v.benincasa@shna.law

III. GOUVERNANCE – SIA à risque élevé

SZLEPER HENRY NAUMANN AVOCATS

Respect des obligations (suite)

4 **Transparence :** Notice d'utilisation (informations sur le fournisseur, les caractéristiques, les capacités et les limites de performance, les risques connus ou prévisibles pour la santé, la sécurité ou les droits fondamentaux, les données d'entrée, les modifications, les mesures de contrôle humain, les ressources informatiques et matérielles nécessaires – inclure des exemples illustratifs)

⚠ Bien indiquer dans la notice (et dans les éventuels contrats) que le SIA ne doit pas être transformé en un système d'IA interdit ou à haut risque (interdiction de modifier la destination du SIA)

5 **Contrôle humain** :

- Contrôle pendant la période d'utilisation au moyen d'interfaces homme-machine (détection et traitement des anomalies, dysfonctionnements et performances inattendues)
- Pour les systèmes d'identification biométrique : contrôle humain accru (vérifiée et confirmée séparément par au moins deux personnes)

6 **Exactitude, robustesse et cybersécurité** : Résilience face aux comportements préjudiciables ou indésirables pouvant résulter de limites intrinsèques aux systèmes ou dues à l'environnement dans lequel les systèmes fonctionnent. Voir la notice d'utilisation jointe au Règlement comprenant des critères de référence et de méthodes de mesures techniques et organisationnelles (ex : plans de sauvegarde, mesures de sécurité après défaillance, mesures d'atténuation des biais, mesures contre les attaques)

g.henry@shna.law
v.benincasa@shna.law

III. GOUVERNANCE – SIA à risque élevé

SZLEPER HENRY NAUMANN AVOCATS

Respect des obligations (fin)

7 **Système de gestion de la qualité** :

- Stratégie de respect de la réglementation (procédures d'évaluation de la conformité et des procédures de gestion des modifications apportées)
- Procédures destinées à la conception et au développement des SIA
- Procédures d'examen, de test et de validation
- Procédures relatives au signalement d'un incident grave
- Système de gestion des données
- Système de gestion des risques
- Système de surveillance après commercialisation
- Système de conservation des documents et informations
- Gestion des ressources
- Cadre de responsabilisation

8 **Surveillance après commercialisation et Signalement d'incidents graves** :

- Système de collecte, de documentation et d'analyse active et systématique des données pertinentes (issues de l'expérience d'utilisation des SIA), qui repose sur un plan de surveillance (un modèle sera proposé par la Commission dans les 18 mois)
- Analyse de l'interaction avec d'autres systèmes d'IA, y compris d'autres dispositifs et logiciels
- Signalement d'un incident grave à l'autorité de surveillance au plus tard 15 jours après sa connaissance

g.henry@shna.law
v.benincasa@shna.law

III. GOUVERNANCE – SIA à risque élevé

Évaluation de la conformité

1. **Évaluation de la conformité** :

   - **Contrôle interne** (sous la propre responsabilité du Fournisseur) ⇔ Normes harmonisées publiées au JO
   - Évaluation par un **organisme d'évaluation** (certification d'évaluation UE)

     L'organismes d'évaluation a 2 missions :
     - **Contrôle de la documentation technique** → Délivrance/Refus d'un **certificat d'évaluation UE de la documentation technique.** Éventuelles modifications du système d'IA susceptibles d'avoir une incidence sur la conformité du système d'IA avec les exigences ou sur sa destination sont évaluées par l'organisme notifié qui a délivré le certificat d'évaluation UE
     - **Surveillance du système de gestion de la qualité (audits dans les locaux)** → Délivrance/Refus d'une **approbation du système**

2. **Déclaration UE de conformité** identifiant le SIA à risque élevé pour lequel elle a été établie

3. Marquage CE

g.henry@shna.law
v.benincasa@shna.law

III. GOUVERNANCE – SIA à risque limité (GPAI)

SZLEPER HENRY NAUMANN AVOCATS

Respect des obligations

1. **Politique de respect du droit d'auteur** : Respect de la réservation de droits exprimée par les titulaires de droits (droits d'exclusion) → autorisation nécessaire (négociation de redevances pour l'usage)

2. **Transparence** :
   - Interaction avec IA : Information (par ex. dans CGU) que l'utilisateur interagit avec un SIA
   - Étiquetage des contenus générés : Marquage dans un format lisible par machine des contenus générés ou manipulés par une IA. Techniques suggérées par le Règlement : filigranes, identifications de métadonnées, méthodes cryptographiques permettant de prouver la provenance et l'authenticité du contenu, méthodes d'enregistrement, empreintes digitales
   - Notice d'utilisation à destination des fournisseurs en aval qui intègrent le modèle dans leur SIA
   - Contenu utilisé : Mise à disposition d'un résumé du contenu utilisé pour entraîner le modèle (données utilisées pour l'entraînement, les essais et la validation ; type, provenance et méthodes d'organisation ; nombre de points de données, portée et principales caractéristiques ; manière dont les données ont été obtenues).

3. **Documentation technique** :
   - Description générale du modèle (tâches ; type et nature des SIA dans lesquels il peut être intégré politiques applicables en matière d'utilisation acceptable ; architectures ; modalités et format des entrées et des sorties ; licence)
   - Description des éléments du modèle et de son processus de développement (moyens techniques nécessaires à l'intégration du modèle dans les SIA ; spécifications de conception et du processus d'entraînement ; ressources informatiques)

g.henry@shna.law
v.benincasa@shna.law

III. GOUVERNANCE – SIA à risque limité (GPAI)

SZLEPER HENRY NAUMANN AVOCATS

Respect des obligations (risque syst.)

1. **Système de gestion des risques (ensemble du cycle de vie du SIA)** :
   - Étape 1 : Essais pendant le processus de développement (essais en conditions réelles ou bac à sable règlementaire)
   - Étape 2 : Identification et analyse des risques connus et raisonnablement prévisibles (auto-évaluation)
   - Étape 3 : Adoption de mesures appropriées et ciblées de gestion des risques

2. **Cybersécurité** : Garantir un niveau approprié de protection en matière de cybersécurité pour le modèle et l'infrastructure physique du modèle

3. **Surveillance après commercialisation et Signalement d'incidents graves** :
   - Système de collecte, de documentation et d'analyse active et systématique des données pertinentes (issues de l'expérience d'utilisation des SIA), qui repose sur un plan de surveillance (un modèle sera proposé par la Commission dans les 18 mois)
   - Analyse de l'interaction avec d'autres systèmes d'IA, y compris d'autres dispositifs et logiciels
   - Signalement d'incidents graves à l'autorité de surveillance au plus tard 15 jours sa connaissance

g.henry@shna.law
v.benincasa@shna.law

IBM TechXchange

SZLEPER HENRY NAUMANN AVOCATS

Merci !

Guillaume Henry

+33 6 83 59 19 41

g.henry@shna.law

Victor Benincasa

+33 6 67 40 56 66

v.benincasa@shna.law