



Conférence

24 mars 2025

Marina Bojarski Sebalj

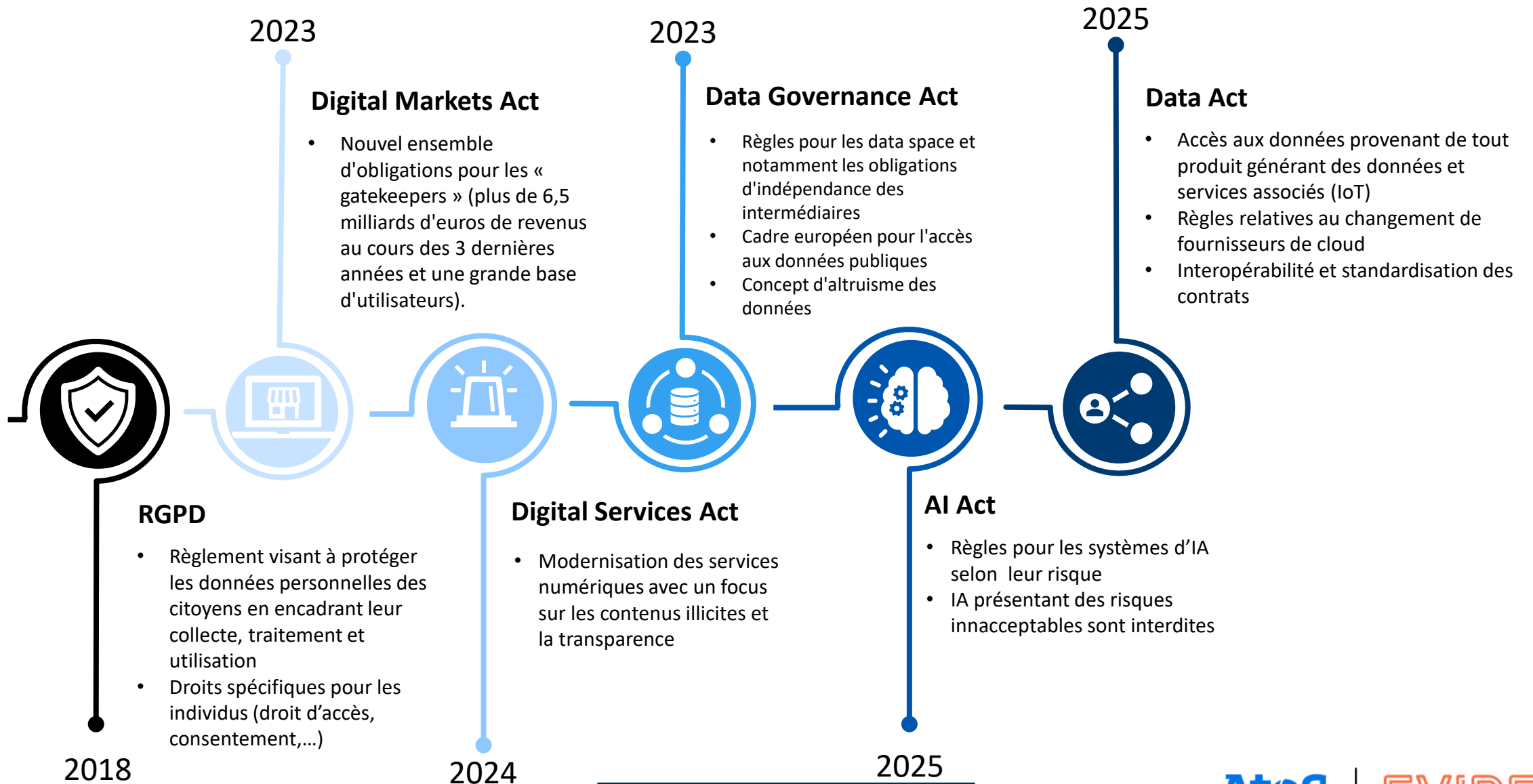
Pour usage privé

Atos | EVIDEN

01

La réglementation de l'espace numérique

Paysage réglementaire européen de l'espace numérique



Le RGPD en un coup d'œil

1) Définir les objectifs du traitement

- Identifier clairement l'objectif du traitement des données

3) Cartographie des traitements

- Identifier les types de données collectées
- Déterminer qui accède aux données
- Identifier où elles sont stockées et pendant combien de temps elles sont conservées.

5) Respect des droits des personnes

- Droit d'accès
- Droit de rectification
- Droit à l'effacement (droit à l'oubli)
- Droit à la portabilité
- Droit d'opposition et limitation du traitement

2) Définir une base légale

- Consentement
- Exécution d'un contrat
- Obligation légale
- Mission d'intérêt public
- Protection des intérêts vitaux
- Intérêt légitime

4) Mise en place de mesures de sécurité

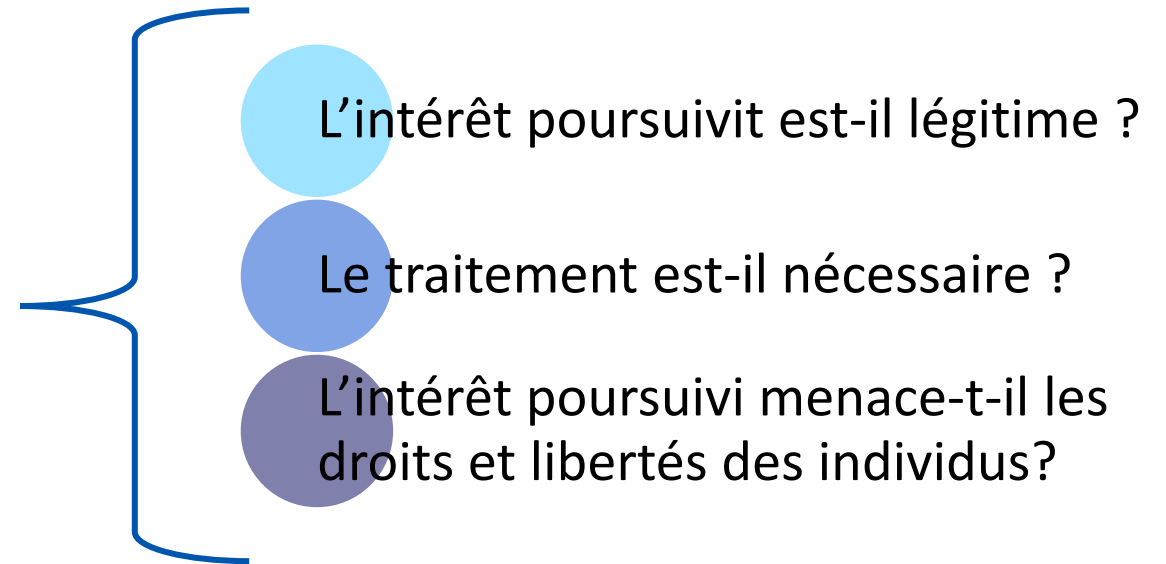
- Chiffrement, pseudonymisation, contrôle des accès
- Sensibilisation des employés et bonnes pratiques en cybersécurité

6) Documentation et gestion

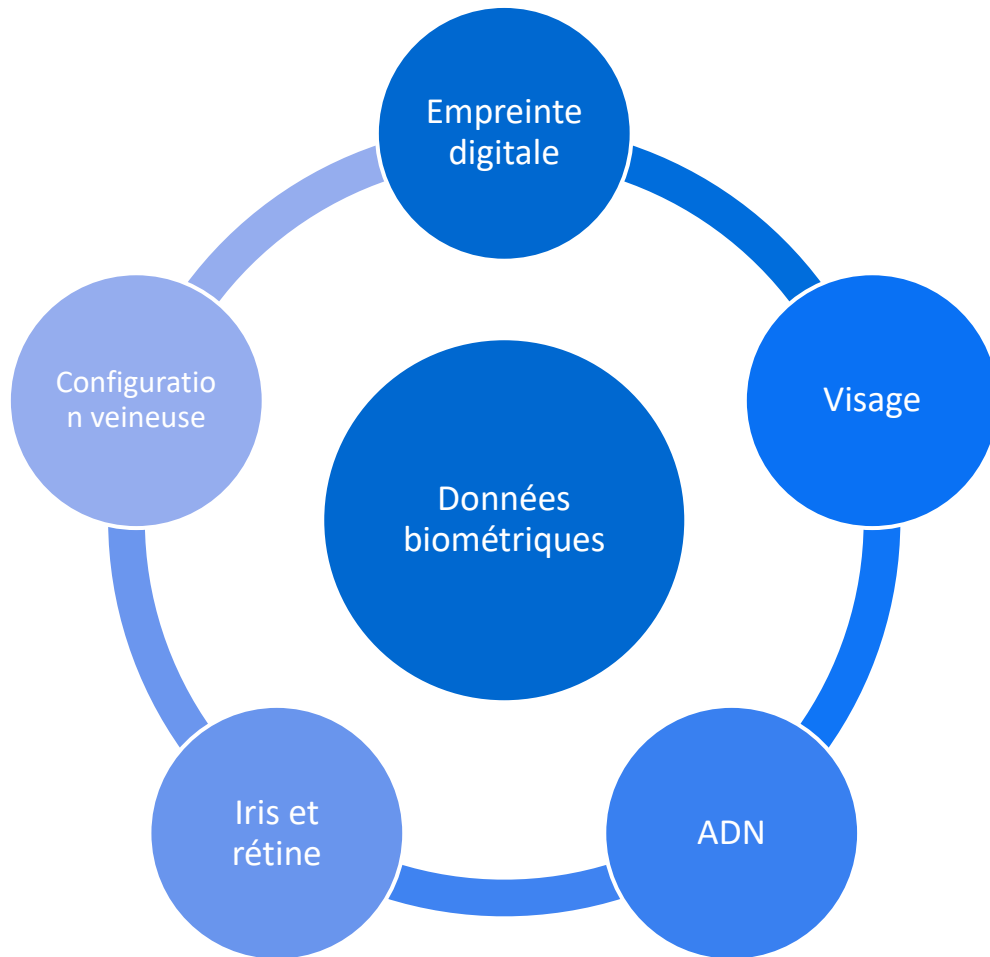
- Registre d'activités
- Gestion de la violation des données

Le RGPD par le prisme de l'IA

Consentement	• Pas appropriée • Difficile de recueillir un consentement approprié dans ce contexte et de le retirer
Intérêt légitime	• Le plus approprié • Nécessité de vérifier la légitimité
Contrat ou obligation légale	• Pourrait être utilisé exceptionnellement si le responsable du traitement parvient à prouver pourquoi le traitement est nécessaire pour se conformer à la loi ou pour l'exécution d'un contrat
Intérêt public	• Les entités publiques doivent vérifier si le traitement fait partie de leurs missions d'intérêt public



Biométrie



- Les données biométriques sont des « données sensibles ».
- Leur traitement est par principe interdit, sauf dans certains cas:
 - Consentement explicite
 - Obligation légale (ex: contrôle aux frontières)
 - Protection des intérêts vitaux
 - Exécution d'une mission d'intérêt public (ex : la sécurité publique)
 - Traitement nécessaire pour des raisons de sécurité ou d'identification (ex : accès sécurisé à un site sensible)
 - Réglementation spécifique pour l'emploi

Data Act



- Règlement concernant principalement les données non personnelles générées par les objets connectés, les machines et les services cloud.
- Il oblige les entreprises à partager ces données avec leurs clients et d'autres entreprises sous certaines conditions, pour éviter le monopole des géants du numérique et favoriser l'innovation.
- Il facilite aussi le changement de fournisseur de cloud pour éviter la dépendance aux GAFAM.

Data governance Act



- Règlement visant à faciliter le partage sécurisé des données tout en garantissant la protection des droits et de la vie privée.
- Objectifs du DGA:
 - Encourager la réutilisation des données détenues par les organismes publics
 - Soutenir le développement des intermédiaires de données de confiance
 - Promouvoir l'altruisme des données pour des fins d'intérêt général
- Mutualisation des données grâce à l'accès à des données publiques

02

La réglementation de l'IA



Normes relatives à l'IA dans le monde



Des objectifs identiques

2019 - Principes de l'IA de l'OCDE Établissement des principes internationaux de l'IA

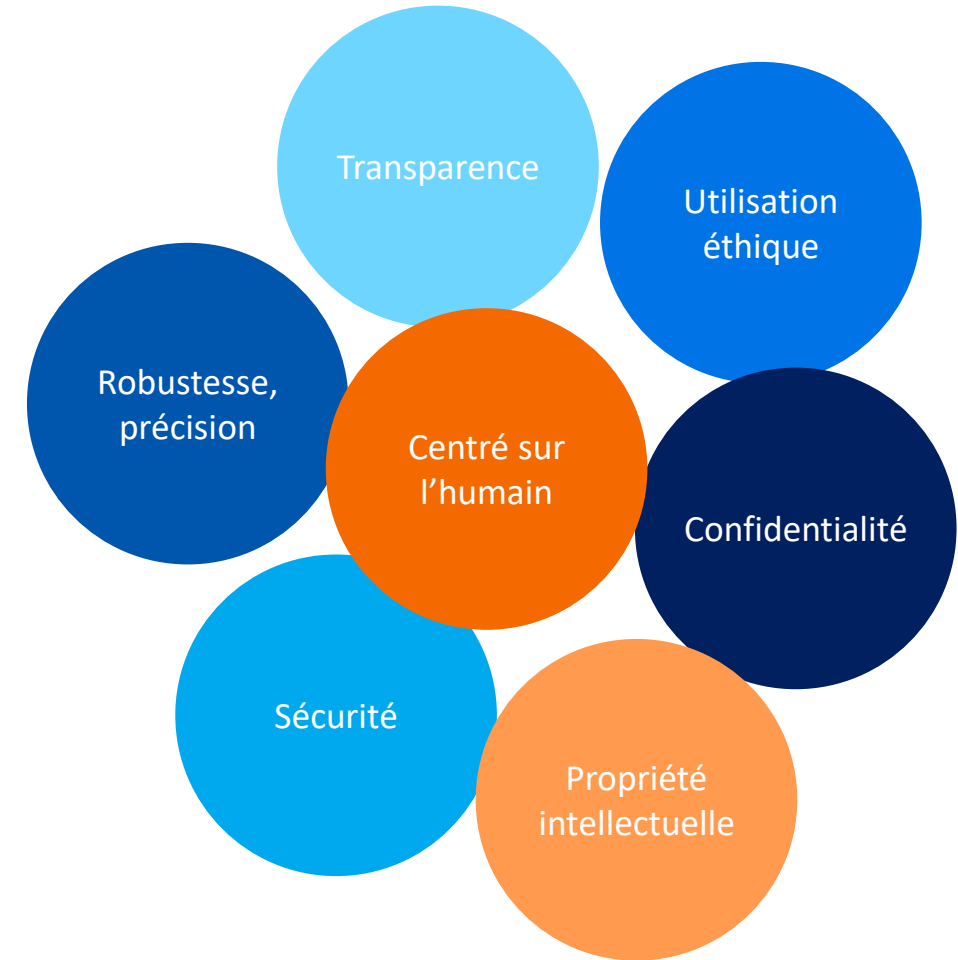
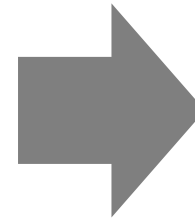
2021 – Acte sur l'IA de l'UE Première réglementation sur l'IA
Basée sur une approche de risque

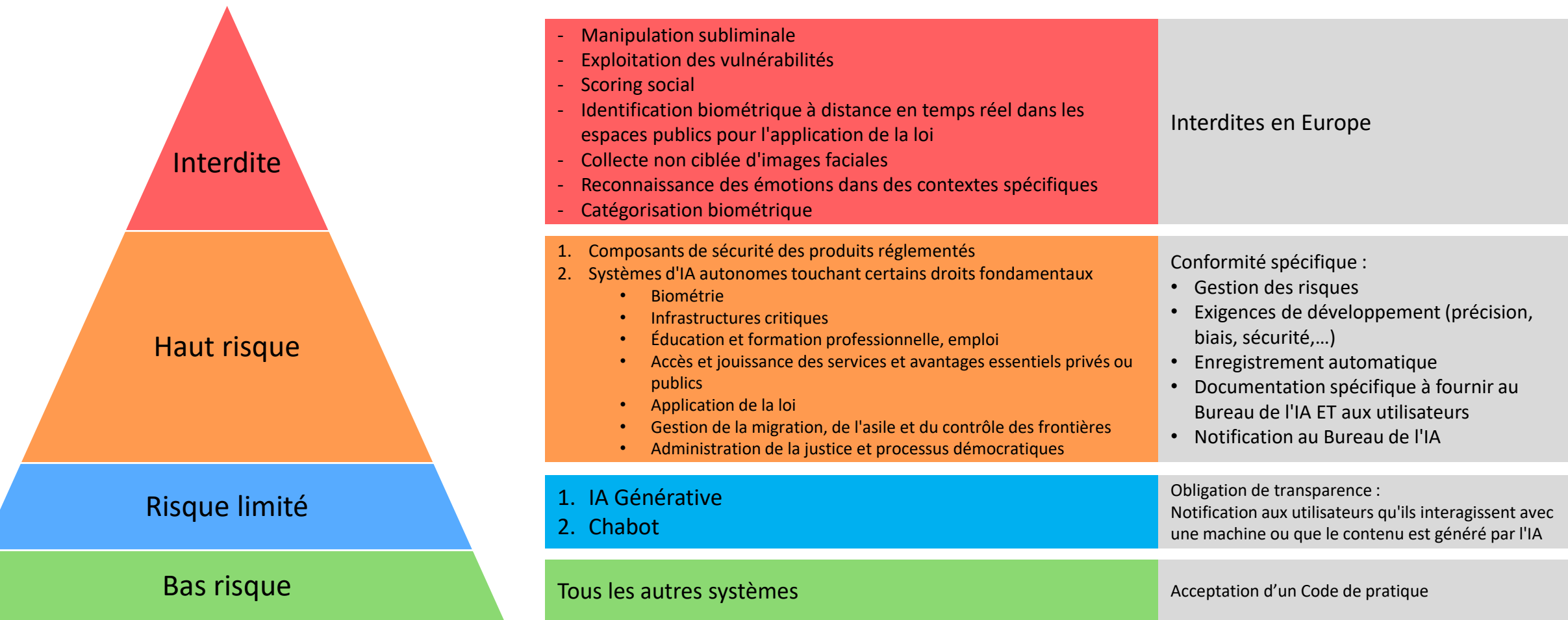
2022 - Proposition américaine pour la loi sur la responsabilité algorithmique Évaluations d'impact pour les systèmes de décision automatisés déployés pour un ensemble de décisions critiques

2023 - Plan américain pour la Charte des droits de l'IA Principes et pratiques associées pour guider la conception, l'utilisation et le déploiement des systèmes automatisés

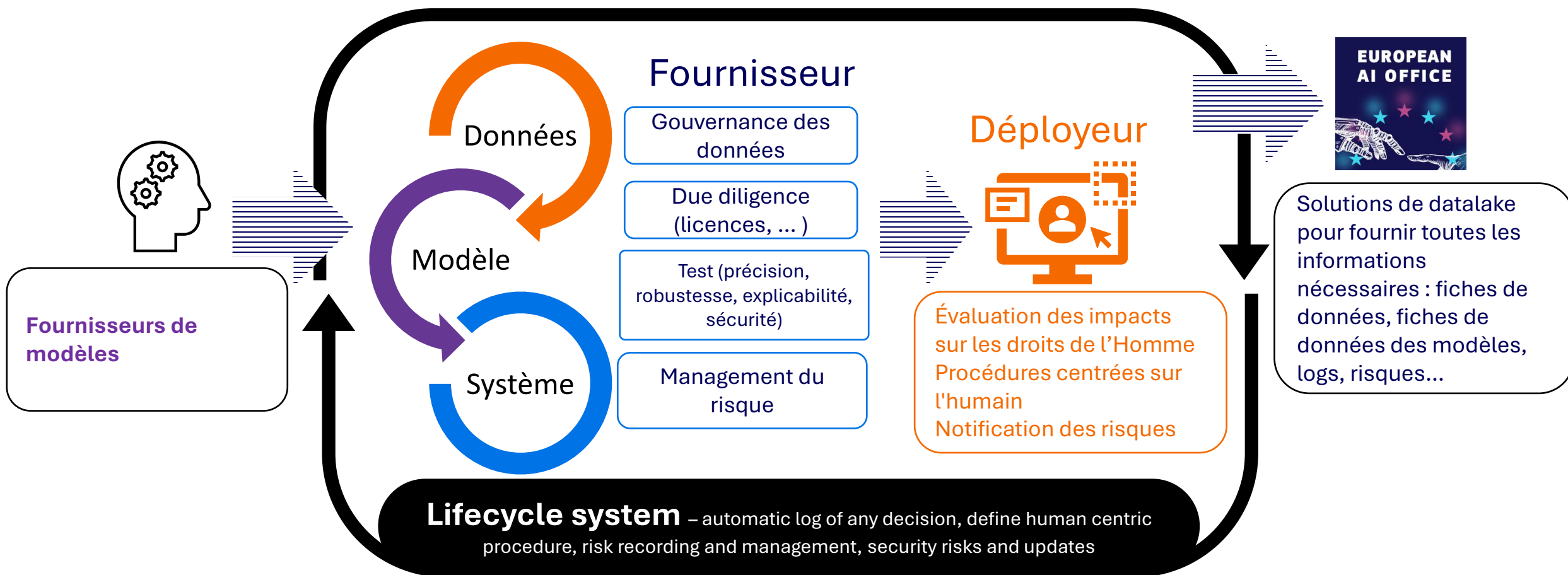
2023 – Ordre exécutif américain sur l'intelligence artificielle sûre, sécurisée et digne de confiance Normes de sécurité et de sûreté de l'IA, protection de la vie privée des Américains, promotion de l'équité et des droits civils, défense des consommateurs et des travailleurs

2023 - Déclaration de Bletchley du Sommet sur la sécurité de l'IA





La conformité des systèmes d'IA



03

L'utilisation de l'IA dans le cadre militaire

Conséquences des mésusages

Cela va au-delà de l'AI Act

AI ACT

Emploi

- Lois contre la discrimination
- RGPD
- Responsabilité civile

Infrastructures critiques

- Droit pénal
- Directive européenne sur les entités critiques
- Responsabilité civile

Transports

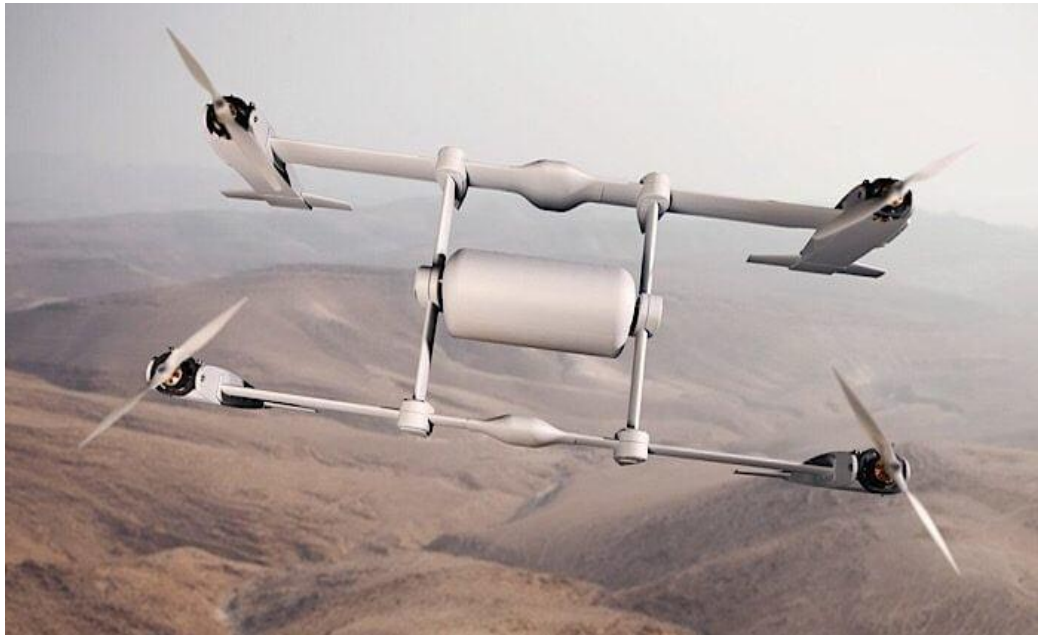
- Réglementation dans le domaine maritime ou ferroviaire

Gestion de la migration

- Charte des droits fondamentaux de l'UE
- Convention européenne des droits de l'homme
- Règlement Dublin III

Les systèmes d'armes létales autonomes

L'absence de règles



- Aucun traité international
- Discussions depuis 2013 par la Convention sur certaines armes classiques (CCAC) pour réglementer ou interdire les SALA.
- Adoption en 2018 par le Parlement européen d'une résolution appelant à une interdiction des SALA, mais cela reste une position politique sans force contraignante.
- Approche de la France et de l'Allemagne : pour un "contrôle humain significatif" sur l'usage de ces armes, sans demander une interdiction totale.
- Approche des États-Unis, Russie, Chine : opposition à toute interdiction stricte, mais une réglementation plus souple pour préserver leur avance technologique.

Droit international humanitaire

Convention de Genève et ses protocoles additionnels



Principe de distinction

- Obligation de distinction entre combattants et civils, ainsi qu'entre objectifs militaires et biens civils.
- x L'autonomie des SALA pourrait entraîner des erreurs d'identification, notamment dans des contextes où la reconnaissance faciale et l'IA sont limitées.



Principe de proportionnalité

- Obligation d Une attaque ne doit pas causer de dommages collatéraux excessifs par rapport à l'avantage militaire recherché.
- x Les machines ne sont pas forcément capables d'évaluer si une attaque est « proportionnée » en fonction de la situation



Principe de responsabilité humaine

- Un acteur humain doit être tenu responsable des décisions prises pendant un conflit armé.
- x L'autonomie des SALA pose la question de savoir qui est responsable en cas d'erreur : le programmeur, l'opérateur, le commandant militaire, ou l'État



Principe de nécessité militaire

- Obligation d'un usage de la force limité aux objectifs strictement militaires nécessaires pour atteindre un but légitime
- x Ces systèmes peuvent agir sans supervision humaine, ce qui peut entraîner des frappes injustifiées

Merci !



Marina Bojarski Sebalj
marina.bojarski@atos.net

Atos is a registered trademark of Atos SE. © 2024 Atos. Confidential information owned by Atos, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval from Atos.

Pour usage privé

