IA et cybersécurité: une introduction juridique

AI Swiss, Neuchâtel

(25 novembre 2025)

Prof. Philippe Gilliéron
Avocat, Genève

B · M · G
AVOCATS

30.10.25

Qui suis-je?

Qualifications

Avocat inscrit au barreau Suisse
(propriété intellectuelle, protection des données et numérique)

Consultant spécialisé en gouvernance de l'intelligence artificielle
(certification AIGP; ISO 42001 Lead Implementer en cours)

Enseignant à la Faculté de droit
Universités de Lausanne/Fribourg/Lugano (marketing et communication)

Expertise et approche

Spécialiste des questions juridiques et éthiques liées au déploiement de l'IA en contexte d'entreprise

Accompagnement adapté aux PME suisses dans la mise en place de cadres de gouvernance IA conformes aux exigences réglementaires

Approche pragmatique combinant conformité juridique et efficacité opérationnelle

Vision

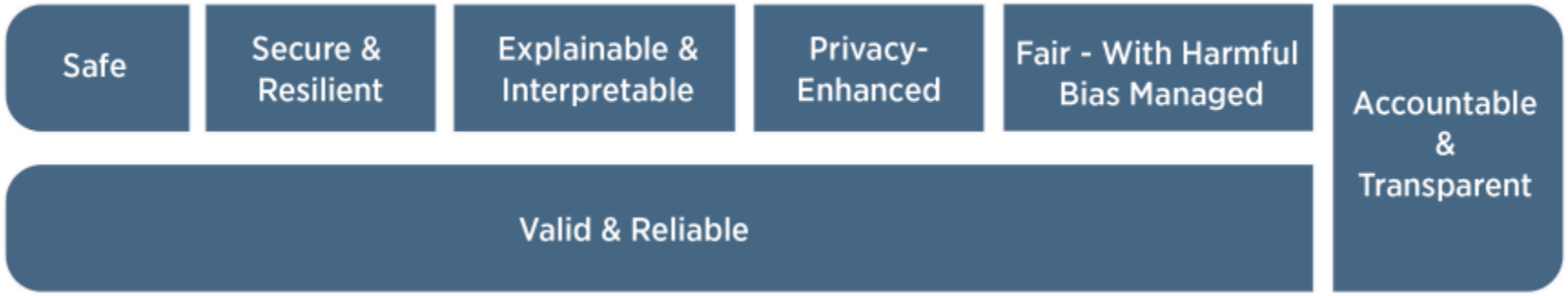
Démocratiser une IA utile, rentable et responsable pour les entreprises suisses

Un système IA génère un faux enregistrement vocal d'un CEO, provoquant un virement frauduleux de millions.

Une banque suisse utilise un système IA hébergé dans le cloud en UE. Une cyberattaque expose des données personnelles de clients.

I. IA

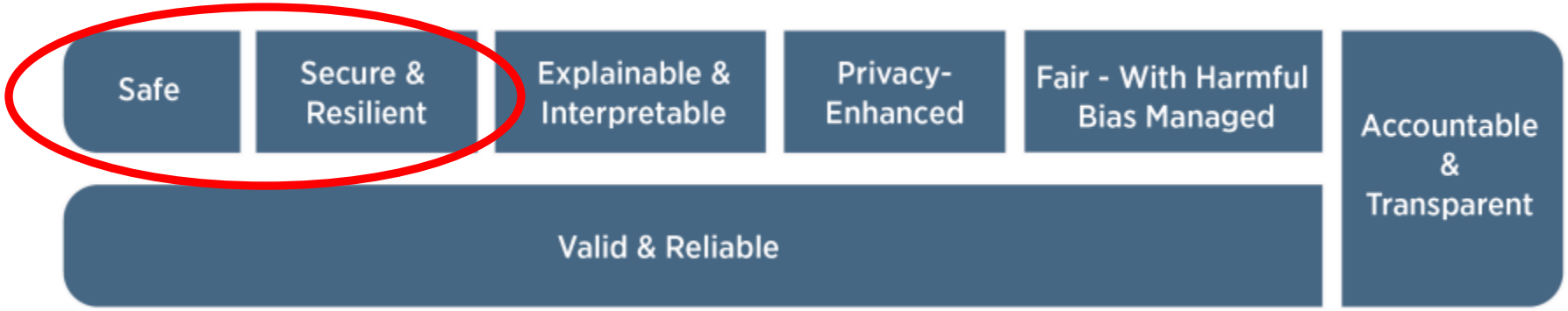
- Cadre juridique et standards reposent sur des principes éthiques visant au développement et déploiement d'une intelligence artificielle responsable



Source: NIST, AI RMF Framework

I. IA

- Cadre juridique et standards reposent sur des principes éthiques visant au développement et déploiement d'une intelligence artificielle responsable



Source: NIST, AI RMF Framework

Union européenne

- Règlement européen sur l'IA
- Réglementation de produits
- Approche fondée sur les risques
- Art. 15 (cybersécurité)
- Paquet omnibus pour une révision du Règlement

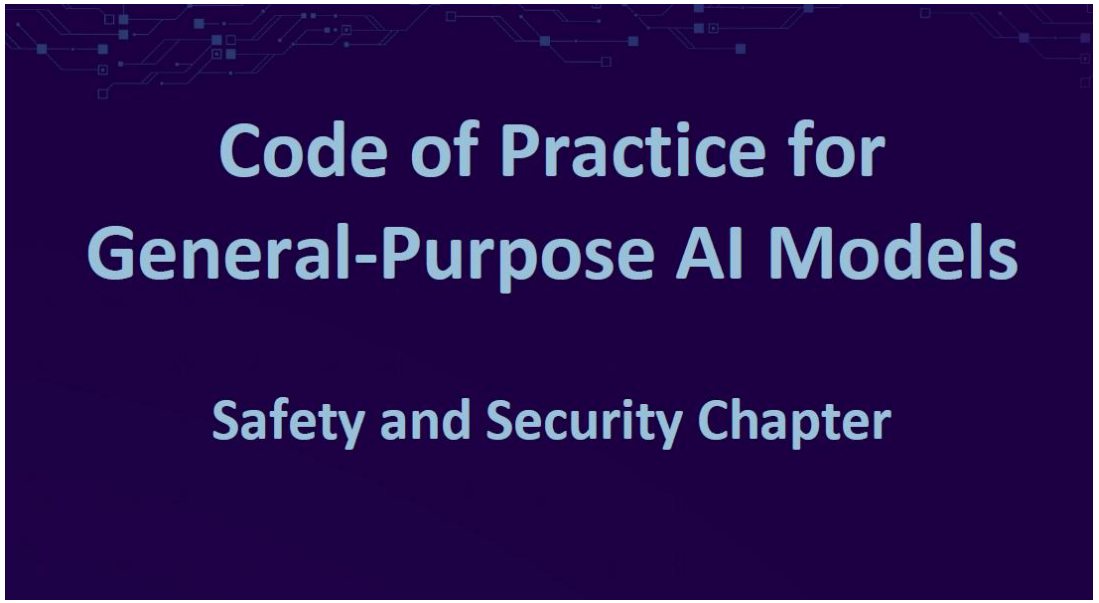
Suisse

- Aucune loi spécifique (principe de neutralité technologique)
- Rapport OFCOM février 2025
- Ratification Convention du Conseil de l'Europe (pour secteur public)
- Modifications législatives uniquement si nécessaires
- Modifications à portée générale (protection des données, droit d'auteur)
- Modifications spécifiques (domaine de la santé ou secteur financier
- Projet attendu pour fin 2026

Standards ISO: 42001 (intégration avec dispositifs en place, dont ISO 27001)

II. Cybersécurité - UE

Réglementation	Portée	Entités visées	Entrée en vigueur	Focus	Effet extraterritorial
NIS 2 (Dir. 2022/2555)	Directive	Infrastructures critiques + services essentiels (18 secteurs, dont finance et santé)	17.10.2024	Résilience des réseaux et systèmes	Si filiale UE ou services essentiels fournis dans UE
DORA (Digital Operational Resilience Act; Règl. 2022/2554)	Règlement	Secteur financier et prestataires TIC	17.1.2025	Résilience opérationnelle numérique	Si services financiers dans UE ou prsetataire TIC critique
CRA (Cyber Resilience Act) Règl. 2024/2847	Règlement	Fabricants produits numériques	Déc. 2027	Sécurité des produits	Si produits numériques dans UE
RGPD (art. 32) (Règl. 2016/679)	Règlement	Général	25.5.2018	Protection des données	Traitement de données de résidents UE
IA (art. 15)	Règlement	Général	Graduel depuis 1.8.2024	Systèmes IA	Si système dans UE ou résultat



- Mise en œuvre art. 55 Règlement IA (chapitre 3)
- Accexible, AI Alignment Solutions, Aleph Alpha, Almawave, Amazon, Anthropic, Bria AI, Cohere, Cyber Institute, Domyn, Dweve, Euc Inovação Portugal, Fastweb, Google, Humane Technology, IBM, Lawise, LINAGORA, Microsoft, Mistral AI, Open Hippo, OpenAI, Pleias, re-inventa, ServiceNow, Virtuo Turing, WRITER

III. Cybersécurité - Suisse

Règlementation	Entités visées	Entrée en vigueur	Focus	Obligations
LPD	Général	1.9.2023	Protection des données	Art. 8
LSI	Autorités et organismes fédéraux et secteurs critiques (dont banques et établissements santé)	1.4.2025	Résilience des réseaux, systèmes et opérationnelle numérique	Système de gestion de la sécurité de l'information, classification et protection des informations, personnel, locaux, signalement des incidents

- FINMA Circulaire 2023/1 Risques et résilience opérationnels – banque
- FINMA Communication 08/2024 Gouvernance et gestion des risques en lien avec l'intelligence artificielle

IV. Points de discussion possibles

- Tensions entre sécurité et innovation
- Modèle propriétaire ou open source
- Dilemme de la transparence
- Chaîne de responsabilité dans l’écosystème IA

Merci de votre attention!

Prof. Philippe Gilliéron (Stanford, ‘06)

Philippe.gillieron@bmglaw.ch

Philippe Gilliéron - BMG Avocats

B·M·G
AVOCATS