Revue-IRS

Revue Internationale de la Recherche Scientifique (Revue-IRS)

ISSN: 2958-8413

Vol. 3, No. 6, Décembre 2025

Gouvernance des risques numériques à l'ère de l'IA : entre sécurité algorithmique, souveraineté numérique et risque dans les secteurs stratégiques

Auteurs :

- LABDAOUI Ahmed: Consultant en IA ;Big data ; cybersécurité et / Droit international des affaires;

-GOURB Abdeljebare: Doctorant à la FSJES de Fès

-TOUZANI Oussama: Doctorant à la FSJES de Fès

Résumé : L'intelligence artificielle redéfinit les frontières de la cybersécurité, Alors que les algorithmes optimisent la détection des menaces par prédiction et sécurisent les transactions critiques, leur opacité et leur ancrage géopolitique menacent la souveraineté numérique des États. Ce travail explore la problématique suivante : comment concilier les avantages et points forts de l'IA (prédiction des vulnérabilités, automatisation des réponses et sécurisation des transactions) avec les risques géopolitiques et les impératifs de souveraineté numérique ?

Cet Article vise à éclairer les tensions entre innovation technologique et autonomie stratégique, proposant des pistes pour une gouvernance équilibrée des risques numériques.

Mots-clés : IA explicable, souveraineté numérique, cybersécurité, gouvernance algorithmique, risques géopolitiques.

Digital Risk Governance in the Age of AI: Between Algorithmic Security, Digital Sovereignty and Risk in Strategic Sectors

Abstract: Artificial intelligence is redefining the boundaries of cybersecurity. While algorithms enhance threat detection by prediction and secure critical transactions, their opacity and geopolitical anchoring threaten nations' digital sovereignty. This study examines the following core dilemma: How can we reconcile the advantages of AI (vulnerability prediction, response automation, and transaction security) with geopolitical risks and digital sovereignty imperatives?

Our research illuminates the tensions between technological innovation and strategic autonomy, proposing pathways for balanced governance of digital risks.

Keywords: Explainable AI (XAI), digital sovereignty, cybersecurity, algorithmic governance, geopolitical risks.

Digital Object Identifier (DOI): https://doi.org/10.5281/zenodo.**17949298**

Introduction

L'intelligence artificielle transforme totalement le paysage de la cybersécurité contemporaine. Si cette révolution technologique offre des opportunités sans précédent pour la prédiction des vulnérabilités, l'automatisation des réponses et la sécurisation des transactions, elle soulève également des défis majeurs en matière de gouvernance des risques numériques. La question centrale qui émerge concerne la capacité des organisations et des États à concilier les avantages stratégiques de l'IA avec les impératifs de souveraineté numérique et les risques géopolitiques croissants. Evitant des altercations non souhaitées

Dans un contexte global où l'essor fulgurant des nouvelles technologies et l'omniprésence de services numériques (intelligence artificielle, Internet des objets, identité numérique, cloud et réseaux sociaux) placent la question de l'utilisation des données personnelles au cœur de notre quotidien, la gouvernance des risques numériques devient un enjeu stratégique majeur. Les organisations font face à une dualité complexe : exploiter le potentiel transformateur de l'IA tout en préservant leur autonomie décisionnelle et leur sécurité informationnelle.

Cette problématique s'inscrit dans un environnement réglementaire en mutation rapide, où les cadres juridiques européens et nationaux évoluent pour encadrer l'usage de l'IA. Un des supports au déploiement massif mais sécurisé des services d'IA est la définition de normes claires et de principes de gouvernance solides, servant de garde-fous à tous les acteurs du domaine. Cette nécessité de structuration réglementaire révèle l'ampleur des enjeux à adresser.

Notre analyse s'appuie sur deux hypothèses fondamentales :

H_1 L'intégration de l'IA explicable (eXplainable AI; XAI)[1] garantit une transparence indispensable pour une cybersécurité éthique et plus fiable. Cette hypothèse postule que la compréhensibilité des décisions algorithmiques constitue un prérequis à l'acceptation et à l'efficacité des systèmes de sécurité basés sur l'IA.

H_2 : Une gouvernance collaborative, associant acteurs publics et privés, est un levier critique pour concrétiser la souveraineté numérique face aux fragmentations juridiques et technologiques. Cette seconde hypothèse suggère que la résilience numérique nationale nécessite une coordination renforcée entre les différentes parties prenantes.

Notre **Plan** s'articule en trois axes :

1. L'Optimisation de la Sécurisation des Transactions dans les Secteurs Stratégiques via l'IA

1.1. Les Capacités Transformatrices de l'IA en Cybersécurité

L'intelligence artificielle révolutionne les approches traditionnelles de la cybersécurité en introduisant des capacités d'analyse et de réaction auparavant inaccessibles. L'IA transforme la cybersécurité avec une détection avancée, prédictive des menaces et une réponse automatisée, permettant aux organisations de dépasser les limites des systèmes de défense conventionnels.

[1]- OSNI. «IA Explicable (XAI) : l'impératif de transparence algorithmique », Swiftask, March 20, 2025. (https://www.swiftask.ai/fr-fr/blog/explainable-ai-xai). And; Lakshit A. & al. (2025), « Explainable Artificial Intelligence Techniques for Software Development Lifecycle: A Phase-specific Survey », 2025 IEEE 49th Annual Computers, Software, and Applications Conference (COMPSAC). p.p.:2281-2288. (http: //doi.org/10.1109/COMPSAC65507.2025.00321).

Les algorithmes[2] d'apprentissage automatique excellent dans l'identification de patterns complexes et l'analyse comportementale. Cette capacité s'avère particulièrement précieuse pour la détection d'anomalies dans les flux de données, l'identification de tentatives d'intrusion sophistiquées et la prédiction des vulnérabilités émergentes. Les systèmes d'IA peuvent traiter des volumes de données exponentiellement supérieurs à ceux qu'un analyste humain pourrait examiner, tout en maintenant une vigilance constante.

L'automatisation des réponses constitue un autre avantage majeur de l'IA en cybersécurité. Les systèmes intelligents peuvent réagir en temps réel à des menaces identifiées, isoler des segments de réseau compromis, déployer des correctifs de sécurité ou déclencher des procédures de sauvegarde. Cette réactivité automatisée réduit significativement les temps de réponse aux incidents, limitant ainsi l'impact potentiel des cyberattaques.

1.2. Applications Sectorielles Critiques

Les secteurs stratégiques comme la finance, l'énergie, la santé et les télécommunications bénéficient particulièrement de ces innovations. Dans le domaine financier, l'IA permet la détection en temps réel de transactions frauduleuses, l'analyse des comportements suspects et la sécurisation des systèmes de paiement. Les algorithmes peuvent identifier des schémas de fraude complexes qui échapperaient aux systèmes de règles traditionnels.

Le secteur énergétique utilise l'IA pour protéger les infrastructures critiques, surveiller les réseaux intelligents et prévenir les cyberattaques contre les systèmes de contrôle industriel. La capacité prédictive de l'IA permet d'anticiper les défaillances système et de renforcer la résilience des réseaux électriques.

En santé, l'IA sécurise les données patients, protège les dispositifs médicaux connectés et garantit l'intégrité des systèmes d'information hospitaliers. La sensibilité des données médicales

[2]- Un algorithme est une suite finie et non ambiguë d'instructions et d'opérations permettant de résoudre une classe de problèmes, selon; (Wikipédia https://fr.wikipedia.org › wiki › Algorithme). Voir aussi : Dongdong G. & al. (2024), « A metaheuristic algorithm for efficient aircraft sequencing and scheduling in terminal maneuvering areas », Optimization Letters (2025) 19:579–604 ; (https://doi.org/10.1007/s11590-024-02151-8).

exige des niveaux de protection particulièrement élevés, que l'IA peut fournir grâce à ses capacités d'analyse comportementale et de détection d'anomalies[3].

1.3. Défis et Limites

Malgré ces avantages, l'intégration de l'IA en cybersécurité présente des défis significatifs. Les risques ne sont plus théoriques ils se concrétisent avec une fréquence et une gravité accrues. La confiance des clients constitue le socle de toute relation commerciale et en matière d'IA et de confidentialité des données, elle s'effrite rapidement. Cette érosion de la confiance souligne l'importance cruciale de la transparence et de l'explicabilité des systèmes d'IA.

Les algorithmes d'IA peuvent également présenter des vulnérabilités spécifiques, comme la susceptibilité aux attaques adversaires où des données malveillantes sont spécifiquement conçues pour tromper les systèmes d'apprentissage automatique. La dépendance croissante aux systèmes d'IA crée de nouveaux vecteurs d'attaque que les cybercriminels apprennent progressivement à exploiter.

2. La Gestion Algorithmique des Risques et l'IA Explicable

2.1. L'impératif de Transparence : L'IA Explicable (XAI)

L'IA explicable représente une réponse fondamentale aux préoccupations croissantes concernant l'opacité des systèmes d'intelligence artificielle. Grâce à l'IA explicable, les organisations peuvent accéder au processus décisionnel sous-jacent de la technologie IA et procéder à des ajustements si nécessaire. L'IA explicable peut améliorer l'expérience utilisateur en créant un environnement de confiance et de compréhension mutuelle.

Le concept de XAI[4] dépasse la simple performance algorithmique pour intégrer la compréhensibilité humaine des décisions automatisées. L'intelligence artificielle explicable,

[3]- **Wirtz, B. & al.** (2022), « Artificial Intelligence and Public Sector Value Creation: A Systematic Review and Research Agenda », *Government Information Quarterly*, vol. 39, n°4, (https://doi.org/10.1080/01900692.2021.1947319).

[4]- pour plus d'explication voir aussi: Branka H.M & al. (2024), « Explainable AI in Credit Risk Management », March 2, 2021, p.p.1-16. (https://doi.org/10.48550/arXiv.2103.00949). Et,

c'est l'ensemble des processus et des outils qui permettent la compréhension de ces résultats. Tout système fonctionnant avec une IA doit ainsi pouvoir fournir une explication que les utilisateurs peuvent comprendre. Cette exigence devient particulièrement critique dans le domaine de la cybersécurité où les décisions automatisées peuvent avoir des conséquences majeures.

2.2. Applications de la XAI en Cybersécurité

L'intégration de la XAI en cybersécurité permet aux analystes de comprendre les raisons derrière les alertes générées par les systèmes d'IA. Cette compréhension facilite la validation des recommandations automatisées, réduit les faux positifs et améliore l'efficacité des équipes de sécurité. Les explications fournies par les systèmes XAI permettent également d'identifier les biais potentiels dans les algorithmes et d'améliorer continuellement leurs performances.

Dans des secteurs critiques comme la santé, la finance ou encore la justice, l'IA explicable permet de renforcer la confiance et de garantir des résultats justes en identifiant les biais éventuels. Cette capacité d'identification des biais s'avère cruciale pour maintenir l'équité et l'efficacité des systèmes de cybersécurité.

2.3. Défis Techniques et Organisationnels

L'implémentation de la XAI présente des défis techniques complexes. L'équilibre entre performance algorithmique et explicabilité nécessite souvent des compromis. Les modèles les plus performants, comme les réseaux de neurones profonds, sont généralement moins explicables que les algorithmes plus simples. Les organisations doivent donc évaluer le niveau d'explicabilité nécessaire en fonction du contexte d'usage et des exigences réglementaires.

Le déploiement éthique des systèmes d'IA dépend de leur transparence et explicabilité (T&E). Le niveau de T&E doit être adapté au contexte, car il peut être nécessaire de trouver un équilibre entre T&E et d'autres principes, tels que la protection de la vie privée, la sûreté. Cette tension entre transparence et confidentialité illustre la complexité des arbitrages nécessaires.

Niklas B. « Explainable AI in Fintech Risk Management », Front. Artif. Intell, 24 April 2020, Volume 3 – 2020. (https://doi.org/10.3389/frai.2020.00026).

2.4. Cadre Réglementaire et Conformité

L'évolution du cadre réglementaire européen, notamment avec l'AI Act[5], renforce l'importance de l'IA explicable. Cette législation pionnière entrera en vigueur le 1er août 2024, avec une application progressive prévue entre 2025 et 2030, créant de nouvelles obligations de transparence pour les systèmes d'IA à haut risque.

Des entreprises européennes investissent dans l'IA explicable pour se conformer aux réglementations, anticipant les exigences croissantes en matière de transparence algorithmique. Cette dynamique de conformité stimule l'innovation dans le domaine de la XAI et encourage le développement de solutions plus transparentes.

3. Enjeux et sens de Souveraineté Numérique

3.1. Enjeux de la Souveraineté Numérique

La souveraineté numérique[6] représente la capacité d'un État ou d'une organisation à exercer un contrôle effectif sur ses infrastructures, données et processus numériques. Cette notion dépasse la simple autonomie technologique pour englober la maîtrise des chaînes de valeur numériques, la protection des données sensibles et la capacité à définir ses propres règles du jeu dans l'espace numérique.

---

[5]- selon le nouveau plan stratégique de la CNIL comporte quatre grands axes: intelligence artificielle, droits des mineurs, cybersécurité et usages du quotidien numérique. Il doit permettre de protéger les données de chacun et ainsi de sécuriser l'avenir numérique de tous. Il reposera sur une action équilibrée entre prévention, accompagnement et répression.

- Députés européens ont adopté la première réglementation appelée « AI Act », le 13 mars 2024.

1 [6]- **Gerda F. & al. (2024), «Digital sovereignty Rhetoric and reality », Journal of European Public Policy, Vol.31, N°:8, 2099–2120. (https://doi.org/10.1080/13501763.2024.2358984).**

Dans le contexte de l'IA et de la cybersécurité, la souveraineté numérique implique plusieurs dimensions critiques. La maîtrise des technologies d'IA constitue un enjeu stratégique majeur, car la dépendance envers des solutions externes peut créer des vulnérabilités et limiter l'autonomie décisionnelle. Les organisations et les États doivent développer leurs propres capacités en IA tout en préservant leur indépendance technologique.

3.2. Fragmentations Juridiques et Technologiques

Le paysage réglementaire international présente une fragmentation croissante qui complique la gouvernance des risques numériques. Les approches divergentes entre les États-Unis, l'Europe et la Chine en matière de régulation de l'IA créent des défis complexes pour les organisations opérant à l'échelle internationale. Cette fragmentation juridique peut entraver l'interopérabilité des systèmes et compliquer la mise en conformité.

Elle impose des exigences strictes en matière de gestion des risques, de notification des incidents et de gouvernance. Les entreprises concernées devront mettre en œuvre des politiques de cybersécurité robustes, réaliser des audits réguliers et s'assurer de la conformité à des standards. Cette multiplication des exigences réglementaires nécessite des approches de gouvernance adaptatives et flexibles.

3.3. Gouvernance Collaborative : Acteurs Publics et Privés

La construction de la souveraineté numérique nécessite une collaboration étroite entre les secteurs public et privé. Piloter son risque numérique et valoriser sa cybersécurité pour générer de la confiance auprès de vos clients et partenaires, et en faire un atout de compétitivité devient un objectif partagé entre les organisations privées et les institutions publiques.

Cette gouvernance collaborative se matérialise à travers plusieurs mécanismes : partage d'informations sur les menaces, développement de standards communs, mutualisation des ressources de recherche et développement, et coordination des réponses aux incidents majeurs. Les partenariats public-privé permettent de combiner l'agilité du secteur privé avec la vision stratégique et les ressources du secteur public.

3.4. Stratégies Nationales et Européennes

Les stratégies nationales de cybersécurité intègrent progressivement les enjeux de souveraineté numérique liés à l'IA[7]. 59 % des collectivités françaises de plus de 3 500 habitants ont testé un projet de gestion administrative par la donnée – ou le prévoient pour 2025, illustrant la dynamique d'appropriation des technologies d'IA par les acteurs publics.

Au niveau européen, les initiatives comme l'AI Act et la stratégie numérique européenne visent à créer un écosystème numérique souverain et compétitif. Ces politiques cherchent à équilibrer innovation, protection des droits fondamentaux et autonomie stratégique.

3.5. Défis Géopolitiques et Économiques

Les tensions géopolitiques croissantes accentuent l'importance de la souveraineté numérique. Les restrictions commerciales, les sanctions technologiques et les préoccupations de sécurité nationale influencent les choix technologiques des organisations. La dépendance envers des technologies d'IA développées par des acteurs étrangers peut créer des vulnérabilités stratégiques.

Selon le PwC 2024 Global Digital Trust Insights[8], les disparités entre les entreprises en termes de cybersécurité sont énormes, révélant l'hétérogénéité des niveaux de maturité et la nécessité d'approches différenciées selon les contextes organisationnels et nationaux.

4. Synthèse et Recommandations Stratégiques

4.1. Validation des Hypothèses

[7]-Upmynt. (2025), « Les enjeux éthiques de l'intelligence artificielle en 2024 ». https://www.upmynt.com/les-enjeux-ethiques-de-ia/

[8]- Global Digital Trust Insights 2024, PwC, https://www.pwc.com › kiadvanyok › assets ›. et

- **Gary C.** & al. (2025), «Digital Transformation and Sustainability in Post-Pandemic Supply Chains: A Global Bibliometric Analysis of Technological Evolution and Research Patterns (2020–2024) », Journal: Sustainability, 2025, Volume: 17, Number: 3009. (https://www.mdpi.com/2071-1050/17/7/3009).

L'analyse menée confirme partiellement nos hypothèses initiales. Concernant l'hypothèse H_1 sur l'IA explicable, les éléments recueillis démontrent effectivement que la transparence algorithmique constitue un prérequis à l'acceptation et à l'efficacité des systèmes d'IA en cybersécurité. L'évolution réglementaire et les attentes des utilisateurs convergent vers des exigences accrues d'explicabilité.

L'hypothèse H_2 sur la gouvernance collaborative trouve également une validation dans les pratiques observées. Les partenariats public-privé et les initiatives de mutualisation se multiplient, confirmant que la souveraineté numérique nécessite une coordination renforcée entre les différents acteurs.

4.2. Modèle de Gouvernance Intégrée

Nous proposons un modèle de gouvernance intégrée articulé autour de quatre piliers fondamentaux :

Pilier 1 : Transparence et Explicabilité - Développement systématique de solutions XAI pour tous les systèmes d'IA critiques, avec des niveaux d'explicabilité adaptés aux contextes d'usage et aux exigences réglementaires.

Pilier 2 : Collaboration Écosystémique - Mise en place de mécanismes de coordination entre acteurs publics et privés, incluant le partage d'informations, la mutualisation des ressources et la coordination des réponses aux crises.

Pilier 3 : Autonomie Technologique - Développement de capacités nationales et européennes en IA, réduction des dépendances critiques et maîtrise des chaînes de valeur technologiques stratégiques.

Pilier 4 : Adaptabilité Réglementaire - Création de cadres réglementaires flexibles capables d'évoluer avec les innovations technologiques tout en préservant les objectifs de sécurité et de souveraineté.

4.3. Recommandations Opérationnelles

Pour les organisations, nous recommandons l'adoption d'une approche progressive d'intégration de l'IA explicable, en commençant par les systèmes les plus critiques. L'investissement dans la

formation des équipes et le développement de compétences internes en XAI constitue un prérequis à cette transformation[9].

La gouvernance cybersécurité est devenue un enjeu central pour assurer la protection des entreprises en 2025. Face à l'évolution des menaces et des régulations, la mise en place d'une stratégie claire et d'outils adaptés est indispensable. Cette évolution nécessite une approche holistique intégrant les dimensions technologiques, organisationnelles et réglementaires.

Pour les décideurs publics, nous préconisons le renforcement des mécanismes de coordination intersectorielle et le développement d'incitations à l'innovation responsable en IA. La création de sandbox réglementaires peut faciliter l'expérimentation de solutions innovantes tout en préservant les objectifs de sécurité.

Conclusion

L'intégration de l'intelligence artificielle dans la cybersécurité représente une transformation majeure qui redéfinit les approches traditionnelles de la gestion des risques numériques. Cette évolution s'accompagne d'opportunités considérables mais également de défis complexes qui nécessitent des réponses coordonnées et adaptées.

L'IA explicable émerge comme un élément central de cette transformation, permettant de concilier performance algorithmique et exigences de transparence. Son développement constitue un enjeu stratégique pour maintenir la confiance des utilisateurs et assurer la conformité réglementaire. La capacité à expliquer les décisions automatisées devient un avantage concurrentiel et un prérequis à l'acceptation sociale de ces technologies.

La souveraineté numérique, quant à elle, nécessite une approche collaborative associant étroitement les secteurs public et privé. Les défis géopolitiques et économiques actuels renforcent l'importance de cette collaboration pour préserver l'autonomie décisionnelle et la sécurité informationnelle des organisations et des États.

[9]- Waddah S. & al. (2023), « Explainable AI (XAI): A systematic meta-survey of current challenges and future opportunities », journal homepage: www.elsevier.com/locate/knosys, Volume 263, 5 March 2023, 110273. (https://doi.org/10.1016/j.knosys.2023.110273)

L'évolution du paysage réglementaire, notamment avec l'AI Act européen, crée de nouvelles obligations mais également de nouvelles opportunités pour les acteurs qui sauront anticiper et s'adapter à ces changements. La capacité à naviguer dans cet environnement réglementaire complexe et évolutif devient un facteur critique de succès.

Les organisations qui réussiront cette transformation seront celles capables d'intégrer harmonieusement innovation technologique, exigences éthiques et impératifs de souveraineté. Cette intégration nécessite une vision stratégique à long terme, des investissements soutenus dans le temps dans les compétences et les technologies, et une capacité d'adaptation continue aux évolutions de l'écosystème numérique.

L'avenir de la cybersécurité se dessine ainsi autour d'une intelligence artificielle plus transparente, plus explicable et mieux intégrée dans des écosystèmes de gouvernance collaborative. Cette évolution ouvre de nouvelles perspectives pour la construction d'un espace numérique plus sûr, plus éthique et plus souverain.

Bibliographie

- Alejandro Barredo A**. & al.** (2020), « Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges toward Responsible AI », *Information Fusion*, n°58, p.p. 82-115. (https://doi.org/10.1016/j.inffus.2019.12.012).

1 - Miles B. & al. (2018), « The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation », Computer Science, (https://doi.org/10.48550/arXiv.1802.07228)

- Branka H.M & al. (2024), « Explainable AI in Credit Risk Management », March 2, 2021, p.p.1-16. (https://doi.org/10.48550/arXiv.2103.00949).

- Cath, C. (2018), « Governing Artificial Intelligence: Ethical, Legal, and Technical Opportunities and Challenges », *Philosophical Transactions of the Royal Society A*. (https://doi.org/10.1098/rsta.2018.0080).

- Dongdong G. & al. (2024) « A metaheuristic algorithm for efficient aircraft sequencing and scheduling in terminal maneuvering areas », Optimization Letters (2025) 19:579–604 ; (https://doi.org/10.1007/s11590-024-02151-8).

- **ENISA** « *AI Cybersecurity Challenges: Threat Landscape for Artificial Intelligence* », Publications, December 2020. (http://www.enisa.europa.eu/).

- **Floridi, L. & al.** (2018), « AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations », *Minds and Machines*, vol. 28, n°4, pp. 689-707. (https://doi.org/10.1007/s11023-018-9482-5).

- **Gary C.** & al. (2025), «Digital Transformation and Sustainability in Post-Pandemic Supply Chains: A Global Bibliometric Analysis of Technological Evolution and Research Patterns (2020–2024) », Journal: Sustainability, 2025, Volume: 17, Number: 3009. (https://www.mdpi.com/2071-1050/17/7/3009).

2 - **Gerda F. & al. (2024), «Digital sovereignty Rhetoric and reality », Journal Of European Public Policy, Vol.31, N°:8, 2099–2120. (https://doi.org/10.1080/13501763.2024.2358984).**

- Lakshit A. & al. (2025), « Explainable Artificial Intelligence Techniques for Software Development Lifecycle: A Phase-specific Survey », 2025 IEEE 49th Annual Computers, Software, and Applications Conference (COMPSAC). p.p.:2281-2288. (http: //doi.org/10.1109/COMPSAC65507.2025.00321).

- **Leslie, D.** (2019), *Understanding Artificial Intelligence Ethics and Safety: A Guide for the Responsible Design and Implementation of AI Systems in the Public Sector*, Londres. systems in the public sector. The Alan Turing Institute. (https://doi.org/10.5281/zenodo.3240529).

3 - **Niklas B. « Explainable AI in Fintech Risk Management », Front. Artif. Intell, 24 April 2020, Volume 3 – 2020. (https://doi.org/10.3389/frai.2020.00026).**

- **OECD** (2019), *Recommendation of the Council on Artificial Intelligence*, OECD Legal Instruments.

- OSNI. « IA Explicable (XAI) : l'impératif de transparence algorithmique », Swiftask, March 20, 2025. (https://www.swiftask.ai/fr-fr/blog/explainable-ai-xai).

- **PwC** (2024), *2024 Global Digital Trust Insights: Cybersecurity Trends and Strategies*.

- **Taddeo, M. & Floridi, L.** (2018), « How AI Can Be a Force for Good », *Science*, pp. 751-752. (DOI: 10.1126/science.aat5991).

- Upmynt. (2025), « Les enjeux éthiques de l'intelligence artificielle en 2024 ». (https://www.upmynt.com/les-enjeux-ethiques-de-ia/)

- Waddah S. & al. (2023), « Explainable AI (XAI): A systematic meta-survey of current challenges and future opportunities », journal homepage: www.elsevier.com/locate/knosys, Volume 263, 5 March 2023, 110273. (https://doi.org/10.1016/j.knosys.2023.110273)

- Wirtz, B. & al. (2022), « Artificial Intelligence and Public Sector Value Creation: A Systematic Review and Research Agenda », (https://doi.org/10.1080/01900692.2021.1947319).