CENTRE DE DROIT
BANCAIRE ET FINANCIER

Règlement européen sur l'IA

Les principes d'interprétation des exigences concernant les systèmes d'IA à haut risque

Par Yannick Caballero Cuevas le 7 avril 2025

Le règlement européen sur l'IA (RIA), conçu notamment comme une législation encadrant la sécurité des systèmes d'IA (SIA), impose des exigences que tout SIA à haut risque doit satisfaire avant sa mise sur le marché ou sa mise en service dans l'Union européenne, et ce, tout au long de son cycle de vie. Dans le domaine bancaire et financier, le RIA considère les SIA de *credit scoring* comme à haut risque. Les exigences sont prévues aux art. 8 à 15 RIA et portent notamment sur le système de gestion des risques (art. 9 RIA), la gouvernance des données (art. 10 RIA), le contrôle humain (art. 14 RIA), ou encore l'exactitude, la robustesse et la cybersécurité du SIA (art. 15 RIA). Ce commentaire aborde les principes d'interprétation énoncés à l'art. 8 RIA. Il convient de rappeler ici que le RIA peut avoir une portée extraterritoriale (cf. Fischer, cdbf.ch/1397/).

L'art. 8 par. 1 RIA prévoit que « [l]es systèmes d'IA à haut risque respectent les exigences énoncées dans la [section 2 du chapitre 3], en tenant compte de **leur destination** ainsi que de l'état de la **technique généralement reconnu** en matière d'IA et de technologies liées à l'IA. Pour garantir le respect de ces exigences, il est tenu compte du système de gestion des risques prévu à l'article 9 » (mise en évidence ajoutée). La disposition rappelle ensuite que tout SIA à haut risque doit satisfaire les exigences obligatoires prévues aux art. 9 à 15 RIA. Les mesures prises par le fournisseur pour se conformer aux exigences doivent prendre en compte le contexte dans lequel le SIA opère et être proportionnées par rapport aux objectifs visés par le RIA (consid. 64 RIA). Par conséquent, le principe de proportionnalité devrait guider l'examen de la conformité du SIA, en tenant compte de sa destination et des règles de l'art en matière d'IA.

Premièrement, la « destination » visée par l'art. 8 par. 1 RIA est définie à l'art. 3 ch. 12 RIA. Cette notion comprend « l'utilisation à laquelle un système d'IA est destiné par le fournisseur, y compris le contexte et les conditions spécifiques d'utilisation, tels qu'ils sont précisés dans les informations communiquées par le fournisseur dans la notice d'utilisation, les indications publicitaires ou de vente et les déclarations, ainsi que dans la documentation technique ». Autrement dit, la destination désigne l'usage principal pour lequel le fournisseur a conçu le SIA, tel que précisé dans les documents (par ex. notice d'utilisation, publicité, documentation technique) qu'il met à disposition, ainsi que dans ses déclarations. La question peut se poser de savoir si – au moment de déterminer la destination d'un SIA à haut risque – le fournisseur doit prendre en compte les utilisations abusives qui seraient raisonnablement prévisibles. À notre sens, la notion de destination devrait faire référence à l'usage prévu par le fournisseur,

sans tenir compte des utilisations abusives qui ne relèveraient pas de la finalité principale pour laquelle le SIA a été développé (dans ce sens, cf. Schneeberger et al, Art. 8, p. 226-227). La mise en œuvre concrète des exigences dépend dès lors de la destination voulue par le fournisseur, et non des éventuelles utilisations abusives que des tiers pourraient en faire, car le fournisseur n'a, en définitive, qu'un contrôle limité à cet égard. Toutefois, le fournisseur doit assurer un niveau de protection suffisant correspondant à l'usage envisagé (cf. Guide bleu, point 2.8). Cette protection devrait, à notre sens, être assurée par la mise en œuvre des exigences du RIA.

Deuxièmement, l'application des exigences et l'examen de conformité doivent nécessairement tenir compte de l'état technique généralement reconnu dans le domaine de l'IA. Ce dernier se réfère à un niveau de développement atteint en matière de capacités techniques à une période donnée, en ce qui concerne les produits, les processus et les services, sur la base des connaissances consolidées pertinentes en science, en technologie et en expérience, et qui est reconnu comme une bonne pratique dans le domaine technologique (cf. Projet de demande de standardisation sur l'IA – modification de la décision C(2023)3215, annexe, p. 1). L'état de la technique généralement reconnu doit donc être compris comme l'ensemble des règles de l'art, largement acceptées et reconnues, dans le domaine de l'IA. Toutefois, ces règles ne devraient pas inclure les recherches scientifiques les plus récentes, qui sont encore au stade expérimental ou qui ne présentent pas encore une maturité technologique suffisante.

L'art. 8 par. 2 RIA décrit le rôle du RIA dans le paysage juridique européen ainsi que son interaction avec d'autres législations d'harmonisation. À cet égard, l'examen de conformité peut être intégré dans les procédures déjà existantes prévues par des législations européennes en vigueur, énumérées dans la section A de l'annexe I. L'objectif est ainsi d'éviter des charges réglementaires supplémentaires et des doublons procéduraux, tout en garantissant la cohérence dans l'application du cadre juridique européen (consid. 46).

En conclusion, l'art. 8 RIA fournit des lignes directrices sur la mise en œuvre et l'interprétation des exigences relatives aux SIA à haut risque, dans lesquelles la destination du SIA et les règles de l'art jouent un rôle central. Par ailleurs, les exigences du RIA ne doivent pas être interprétées de manière statique, mais de manière évolutive, en fonction des avancées technologiques dans le domaine de l'IA. Cet aspect devrait encourager une amélioration continue des SIA. À notre avis, la mise en œuvre et l'interprétation des exigences en tenant compte du contexte devraient offrir une 'relative' souplesse au RIA.
