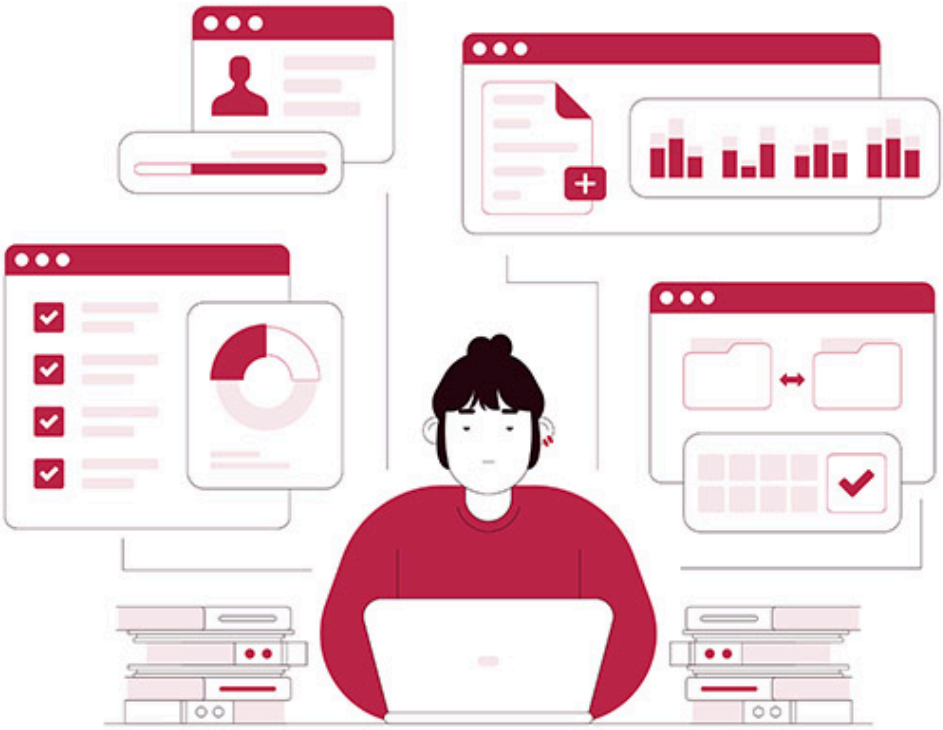
DOSSIER : IA, et si on se posait les bonnes questions juridiques ?
Dossier publié à l'adresse https://www.lagazettedescommunes.com/997639/dans-les-collectivites-locales-comment-cartographier-ses-systemes-dia/

DÉCRYPTAGE

Dans les collectivités locales, comment cartographier ses systèmes d'IA

Auteur associé | Actu juridique | actus experts technique | Analyses juridiques | France | Publié le 27/08/2025

Dans cette analyse, Marie Goutal, avocate, et Théo Simon, juriste au sein du cabinet Goutal, Alibert et associés, expliquent comment sont classés les systèmes d'IA, ce qui permet de connaître et appliquer ensuite les contraintes réglementaires prévues par le règlement sur l'intelligence artificielle.



[1]

Le règlement sur l'intelligence artificielle (RIA – UE 2024/1689) du 13 juin 2024 [2] est venu harmoniser le cadre juridique applicable à l'intelligence artificielle (IA) au sein de l'Union européenne. Ce dispositif, premier du genre à l'échelle mondiale, a vocation à s'appliquer tant au secteur privé que public.

Alors que l'IA tend à s'immiscer progressivement dans tous les rouages de l'action publique, les collectivités territoriales se trouvent confrontées à l'impérieux besoin de maîtriser ces nouvelles règles, qui seront – en grande majorité – applicables à compter du 2 août 2026 (1) [3].

Précisons d'emblée qu'un système d'IA (ci-après SIA) peut être décrit, schématiquement, comme un système automatisé conçu pour générer des contenus variés, comme des textes ou des images, des recommandations ou des décisions, sur la base des données qu'il reçoit, le tout en pouvant faire preuve d'autonomie et même d'adaptation après son déploiement (2) [4].

L'approche retenue par le RIA pour réglementer la matière et créer des obligations graduées repose sur une double classification fondée, d'une part, sur le niveau de risque des SIA et, d'autre part, sur la place occupée par l'opérateur considéré.

Typologie des risques

Cette approche « par le risque » permet d'adapter les contraintes réglementaires à chaque cas d'usage, selon quatre niveaux identifiés. Au sommet de cette pyramide se trouvent les « pratiques interdites » (3) [5] en matière d'IA. Bien que l'entrée en vigueur du RIA soit échelonnée dans le temps, leur mise sur le marché ou en service est d'ores et déjà interdite depuis le 2 février 2025 (4) [6].

Cette catégorie rassemble les cas d'usage les plus « orwelliens » : entre autres (5) [7], les systèmes qui recourent à l'évaluation ou la classification des personnes sur la base d'une note sociale ; qui visent à évaluer ou prédire le risque qu'une personne physique commette une infraction pénale ; la création ou le développement de base de données de reconnaissance faciale par le moissonnage non ciblé d'images provenant d'internet ou d'images de vidéosurveillance ; les cas les plus « poussés » de reconnaissance faciale, ou encore la catégorisation biométrique et l'identification biométrique à distance en temps réel, à des fins répressives dans des espaces accessibles au public.

En dessous de ces pratiques interdites se trouvent les systèmes dits « à haut risque » (6) [8]. Le RIA en distingue deux types : en premier lieu, les SIA utilisés comme composant de sécurité d'un produit couvert par la législation d'harmonisation de l'Union (7) [9] et devant faire l'objet d'une évaluation de conformité par un tiers en vue de sa mise sur le marché ou en service.

Cette première catégorie n'est pas d'une grande clarté. Des « lignes directrices » de mise en œuvre énoncées par les autorités seront les bienvenues pour interpréter cette disposition, qui n'entrera en vigueur qu'au 2 août 2027 (8) [10].

En second lieu, relèvent des SIA à « haut risque » les systèmes listés à l'annexe III du RIA [11]. Sans prétendre à l'exhaustivité, ces SIA sont notamment ceux qui permettent l'identification biométrique (dans les rares hypothèses où elle est autorisée) ; qui servent de composants de sécurité dans la gestion et l'exploitation d'infrastructures critiques (numérique, trafic routier, fourniture d'eau, de gaz, de chauffage ou d'électricité…) ; qui déterminent l'accès, l'admission ou l'affectation de personnes physiques à des établissements d'enseignement ; qui sont utilisés dans le recrutement ; ou qui, pour finir, sont utilisés pour évaluer l'éligibilité aux prestations et services d'aide sociale essentiels (également pour octroyer, diminuer ou révoquer ces prestations).

La liste est vaste et, à notre sens, nombreux sont les cas d'usage des personnes publiques susceptibles de relever de cette catégorie. Une analyse minutieuse des annexes I et III du RIA sera nécessaire afin de bien cerner tous les SIA « à haut risque », notamment lorsqu'une demande pratique émanera des services ou des directions des services informatiques (DSI).

Mais soyons clairs (et rassurants), peu de SIA au total présentent un « haut risque ». Bon nombre relèveront de la troisième catégorie, qui regroupe les SIA ne présentant en effet qu'un risque limité et ne seront, pour cette raison, soumis qu'à des obligations de transparence (cf. infra). Il s'agit, pour l'essentiel, des SIA destinés à interagir directement avec des personnes physiques (typiquement, les robots conversationnels dits « chatbots »).

Une dernière catégorie est enfin constituée des SIA présentant un risque minimal. Elle rassemble tous les SIA qui n'appartiennent à aucune des trois catégories précédemment évoquées.

Positionnement dans la chaine de valeur

Dans la pratique, une fois le niveau de risque identifié, il est crucial de déterminer son positionnement dans la « chaîne de valeur ». L'opérateur, qu'il intervienne en tant que fournisseur, déployeur, mandataire, importateur ou distributeur, se voit systématiquement assujetti à un ensemble d'obligations spécifiques. Il serait d'ailleurs réducteur, voire dangereux, de considérer qu'elles ne s'appliquent qu'aux fournisseurs.

Il convient d'emblée de préciser que le RIA prévoit explicitement la possibilité pour une « autorité publique » d'assumer la qualité de fournisseur ou de déployeur. En revanche, cette faculté n'est pas expressément prévue pour les mandataires, importateurs et distributeurs – des catégories qui, en tout état de cause, apparaissent moins compatibles avec la nature des missions des personnes publiques.

Le fournisseur est donc « une personne physique ou morale, une autorité publique, une agence ou tout autre organisme qui développe ou fait développer un système d'IA ou un modèle d'IA à usage général et le met sur le marché ou met le système d'IA en service sous son propre nom ou sa propre marque, à titre onéreux ou gratuit » (RIA, art. 3, 3 [12]). Ce faisant, il est parfaitement envisageable qu'une collectivité qui développe en interne ou fait développer pour elle un SIA soit qualifiée de fournisseur au sens du RIA. Par exemple, en connectant une base de connaissance qui lui est propre à un modèle « standard » (RAG – Retrieval Augmented Generation) ou encore en l'affinant avec ses propres données (« fine-tuning »).

Il est raisonnable de considérer qu'une personne publique qui développe un SIA et le met en service doit être considérée comme fournisseur et comme déployeur et s'acquitter en conséquence, à la fois, des obligations du « fournisseur » et de celles propres au « déployeur ».

Ces hypothèses resteront cependant marginales en pratique : dans la grande majorité des cas, l'administration se positionnera généralement comme un déployeur (9) [13], se contentant d'utiliser un SIA qu'elle n'a ni développé, ni fait développer.

Obligations

Côté obligations, l'approche mise en place par le RIA s'inscrit dans la continuité du RGPD et impose une mise en conformité préventive et documentée en amont de la mise en place des systèmes.

La première obligation, commune aux fournisseurs et aux déployeurs de SIA – quel que soit le niveau de risque – est de prendre « des mesures pour garantir, dans toute la mesure du possible, un niveau suffisant de maîtrise de l'IA pour leur personnel » (10) [14]. En bref, les agents devront être formés et sensibilisés aux risques induits par l'utilisation de l'intelligence artificielle.

S'agissant de la mise en œuvre de cette obligation, la « FAQ » de la commission publiée le 13 mai dernier, consacrée aux contours de l'obligation de formation imposée par l'article 4 du RIA [15], est une référence obligatoire.

Les fournisseurs de SIA à haut risque seront, quant à eux, soumis à des obligations complémentaires bien plus lourdes. Celles-ci sont précisées aux articles 16 et suivants du RIA [16] : les fournisseurs sont notamment garants du respect des exigences énoncées par la section 2 du RIA (11) [17] et doivent en démontrer le respect, à la demande de l'autorité nationale compétente.

Quant aux déployeurs de SIA à haut risque, bien qu'ils ne soient pas soumis aux obligations les plus poussées, ils devront toutefois prendre de nombreuses mesures pour assurer la conformité de ces SIA aux articles 26 et suivants du RIA [18]. Pour n'en citer que quelques-unes, ils devront prendre les mesures techniques et organisationnelles appropriées afin de garantir que le SIA soit utilisé conformément à la notice d'utilisation transmise par le fournisseur ; confier le contrôle humain à des personnes physiques qui disposent des compétences nécessaires (cf. art. 4 [15]), ce qui renforce la nécessité de créer une forme de « référent » ; surveiller le fonctionnement du SIA et informer le fournisseur en cas de risque ou d'incident grave ; assurer la tenue des journaux générés automatiquement et les conserver pendant une période d'au moins six mois ; lorsqu'ils sont des autorités publiques, respecter les obligations d'enregistrement prévues à l'article 49 [19] ;

réaliser une analyse d'impact relative à la protection des données ; informer les personnes physiques qu'un SIA à haut risque (12) [20] prend ou facilite la prise de décision les concernant.

Sur ce dernier point, le RIA vient réaffirmer une obligation – méconnue ou, la plupart du temps, oubliée – imposée par le CRPA (13) [21] depuis 2016 : informer par une « mention explicite » le destinataire d'une décision individuelle que celle-ci est prise sur le fondement d'un traitement algorithmique.

Enfin, le RIA prévoit l'obligation, pour les « organismes de droit public », d'effectuer une analyse de l'impact que l'utilisation de SIA à haut risque pourrait avoir sur les droits fondamentaux des personnes concernées.

Prévue et décrite à l'article 27 du RIA [22], cette analyse devra comprendre une description des processus dans lesquels l'IA sera utilisée, de la période et de la fréquence à laquelle elle le sera ; les catégories de personnes concernées ; les risques spécifiques de préjudice ; la description de la mise en œuvre des mesures de contrôle humain ; les mesures à prendre en cas de matérialisation des risques. S'agissant des SIA présentant un risque limité, les fournisseurs et développeurs sont assujettis à des obligations de transparence. Très concrètement, les personnes concernées devront être informées qu'elles interagissent avec un SIA « sauf si cela ressort clairement du point de vue d'une personne physique normalement informée et raisonnablement attentive et avisée, compte tenu des circonstances et du contexte d'utilisation » (RIA, art. 50 [23]).

Pour finir, bien que les SIA à risque minimal ne soient, a priori, soumis à aucune règle spécifique, les autres dispositifs en vigueur conservent leur pleine applicabilité. On pense alors évidemment aux garanties issues du RGPD et de la loi « informatique et libertés ».

POUR ALLER PLUS LOIN

- Comment mener le recensement des traitements algorithmiques
- Faut-il désigner un référent IA dans les collectivités ?
- Décryptage du règlement sur l'intelligence artificielle