

LE COURRIER DES MAIRES

et des élus locaux



Intelligence artificielle, innovation et collectivités locales

DE 1 À 9

L'IA: définition, application et risques

Intelligence artificielle
généraliste, applications,
Albert, risque sur la vie
privée, droits d'auteur... p. 3

DE 10 À 24

Le cadre juridique de l'IA

Régulation, application
aux personnes publiques,
conformité, sécurité,
propriété intellectuelle,
gouvernance, RGPD... p. 5

DE 25 À 28

IA et transparence

Transparence des données,
obligation de transparence
algorithmique, information
des utilisateurs, normes
s'imposant à l'IA... p. 9

DE 29 À 38

IA et sécurisation de l'espace public

Caméras augmentées et
biométriques, surveillance
algorithmique, droits des
personnes filmées... p. 10

DE 39 À 50

L'IA, vecteur d'innovation au sein des collectivités?

Outils, commande publique,
partenariat d'innovation,
achat ou développement
en interne... p. 13



Principal actionnaire: Info Services Holding.
Société éditrice: Groupe Moniteur SAS au capital de 333900 euros.
Siège social: Antony Parc 2 - 10, place du Général de Gaulle - La Croix de Berny - BP 20156 - 92186 Antony Cedex.
RCS: Nanterre 403 080 823.
Numéro de commission paritaire: 0425 T 86402.
ISSN: 1252-1574.
Président-directeur de la publication: Julien Elmaleh.

RÉFÉRENCES

- Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle, dit «Règlement IA».
- Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724.
- Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public et ordonnance n° 2005-650 du 6 juin 2005 relative à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques.
- Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public.
- Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique.
- Loi n° 2023-380 du 19 mai 2023 relative aux Jeux olympiques de 2024 et portant diverses autres dispositions.
- Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.
- Décret n° 2018-1225 du 24 décembre 2018 portant diverses mesures relatives aux contrats de la commande publique.
- Arrêté du 17 décembre 2020 fixant la définition des dépenses de fourniture de prestations de solutions relevant de l'informatique en nuage mentionnées à l'article L.1615-1 du CGCT, éligibles à l'attribution du FCTVA pour les dépenses payées à compter du 1^{er} janvier 2021.

RESSOURCES

- « **IA: notre ambition pour la France** », rapport de la commission de l'Intelligence artificielle présidée par Philippe Aghion et Anne Bouverot, éd. Odile Jacob, mai 2024, 288 p., 19,90 €.
- « **S'engager dans l'intelligence artificielle pour un meilleur service public** », étude du Conseil d'Etat du 30 août 2022.
- « **Bac à sable** » intelligence artificielle et services publics: la Cnil accompagne 8 projets innovants, novembre 2023. artificialintelligenceact.eu/fr/high-level-summary/
- **L'adoption par les eurodéputés d'une législation sur l'IA**, tinyurl.com/4bsuusme
- **Le cadre juridique européen de l'IA** tinyurl.com/bdz7u4xw
- **Cybersécurité et IA générative**, cyber.gouv.fr/publications/recommandations-de-securite-pour-un-systeme-dia-generative
- **Panorama des laboratoires d'innovation publique**, tinyurl.com/32h6njxm
- **La cybersécurité des collectivités locales**, 50 questions-réponses du «Courrier des maires», courrierdesmaires.fr/article.55637
- **Tous les articles sur l'intelligence artificielle** du «Courrier des maires», courrierdesmaires.fr/intelligence-artificielle

LEXIQUE

CRPA

Code des relations entre le public et l'administration.

CSPLA

Conseil supérieur de la propriété littéraire et artistique.

Damun

Directive (UE) 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE.

DSA

Digital services act ou Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques).

Système d'IA

Système d'intelligence artificielle.

Règlement IA

Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle.

Loi «SREN»

Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique.

Intelligence artificielle, innovation et collectivités locales

Quels sont les enjeux juridiques et opérationnels liés à l'intelligence artificielle ? Si l'IA n'est pas nouvelle dans nos systèmes d'information, la déferlante de l'IA générative, ChatGPT en tête, a révélé au public l'existence de systèmes permettant de générer du contenu indépendamment de toute intervention humaine.

Formidable outil de travail permettant de gagner du temps et de supprimer les tâches répétitives pour certains, l'IA suscite aussi de nombreuses inquiétudes : disparition de certains métiers, atteinte à la vie privée notamment en matière de vidéoprotection,

menace pour la véracité de l'information et pour le droit de la propriété intellectuelle, etc. La récente adoption du règlement européen IA, qui pose les principes tendant à encadrer le développement et la fourniture de systèmes d'IA « sûrs, transparents, traçables, non discriminatoires et respectueux de l'environnement » a pour objectif de répondre à ces inquiétudes en garantissant une sécurité juridique. L'objectif affiché par ce nouveau texte est aussi d'encourager les investissements et l'innovation au sein de l'UE. Les collectivités locales sont en première ligne vis-à-vis de ces préoccupations, en tant qu'utilisatrices de ces systèmes, mais

aussi lorsqu'elles les développent pour leurs propres besoins ou pour les besoins de leurs usagers dans le cadre de projets de plus en plus innovants. 50 questions-réponses sur l'intelligence artificielle au service des collectivités locales.

Par **Gabrielle Lambert, Lucile Martin, Sara Ben Abdeladhim, Audrey Lefèvre, Inès Marcenat, David Conerardy, Alexandra Aderno, Philippe Guellier**, avocats à la cour, et **Eliott Fassenet** (étudiant en master de droit public des affaires à l'université Lyon III), cabinet Seban avocats

1

Qu'est-ce que l'IA ?

L'intelligence artificielle, communément dénommée « IA », est définie par le Parlement européen comme « la possibilité pour une machine de reproduire des comportements liés aux humains, tels que le raisonnement, la planification et la créativité ». Ce n'est pas une technologie en tant que telle mais plutôt un processus par lequel un algorithme évalue et améliore ses performances sans intervention humaine.

Un **système d'IA** **VOIR LEXIQUE** repose donc sur un algorithme et des données, dans un volume très important, traitées par cet algorithme. Ses capacités lui permettent ensuite d'extraire de ces données certaines caractéristiques et de les traiter aux fins d'un résultat.

Les cas d'usage de l'IA sont donc très variés, allant de la recommandation personnalisée d'achats en ligne, au moteur de recherche, en passant par les assistants virtuels, aux objets connectés.

En ce sens l'IA n'est pas nouvelle dans nos vies et dans le quotidien des collectivités.

2

Qu'est-ce que l'IA générative ?

C'est l'émergence soudaine de l'IA générative, avec ChatGPT, en 2022, et sa diffusion rapide auprès du public, qui a déclenché les irettes des titulaires de droits d'auteur et des défenseurs de la vie privée et, conséquemment, l'accélération de l'adoption d'une réglementation au niveau européen.

L'IA générative (IAg ou GenAI) est une catégorie d'IA capable, à l'aide de modèles avancés d'apprentissage automatique, de générer du contenu (données, images, textes ou sons) de manière autonome, en réponse à des requêtes renseignées par l'humain appelées invites (« prompts » en anglais) consistant en un court texte descriptif.

Alors que l'IA avait eu jusqu'alors pour objectif principal d'automatiser ou d'améliorer l'exécution de tâches nécessitant des personnes humaines, l'IA générative génère de nouveaux contenus, de manière autonome. Elle nécessite des quantités de données encore plus importantes pour produire des résultats ayant une apparence similaire aux données avec lesquelles le système a été entraîné. Illustration la plus connue : ChatGPT, cet agent conversationnel (chatbot) qui s'appuie sur les grands modèles de langage, suivie de Midjourney (IAg d'images).

3

Quelles sont les applications possibles dans le secteur public ?

Dans le secteur public, l'IA est de plus en plus utilisée pour automatiser ou améliorer l'exécution de tâches répétitives nécessitant en principe des personnes humaines, dans l'objectif de libérer du temps pour d'autres missions. On retrouve l'IA dans la relation avec les usagers au travers de chatbots mis en place sur les sites internet des collectivités pour répondre aux questions les plus fréquemment posées, dans les objets connectés utilisés dans la gestion des services et de la consommation (signalisation lumineuse, gaz, maîtrise de l'énergie, production et distribution de chaleur, réseaux et services locaux de communications électroniques, dispositifs de vidéoprotection...), dans la détection de fraudes notamment aux aides sociales. Cette automatisation fait craindre la suppression d'emplois et l'accélération de l'obsolescence de certaines compétences. Craintes tempérées par la commission «Aghion - Bouverot» réunie par le gouvernement en septembre 2023. Sans nier une part d'incertitude, elle considère que l'IA pourra générer des emplois dans de nouveaux métiers, en partie inconnus à ce jour, ainsi que dans des métiers existants.

4

A quoi sert Albert, l'IA générative développée par l'Etat ?

«Albert» est une IA développée par l'équipe DataLab de la Direction interministérielle du numérique (Dinum) et chargée notamment d'aider les agents de l'administration à mieux répondre aux demandes des Français. C'est un projet d'IA souveraine développée pour accélérer les formalités administratives pour les usagers du service public et faciliter le travail des agents (recherche d'informations, rédaction de synthèses, etc.). Depuis janvier 2024, Albert a été expérimenté par une soixantaine d'agents répartis dans une trentaine de guichets. Des systèmes d'IA sont utilisés par les agents de l'administration fiscale pour préparer des projets de réponses aux 16 millions de demandes faites en ligne chaque année, par les agents des Dreal afin de rédiger des synthèses servant à la pré-instruction des 4000 projets environnementaux (etc.). Le site du gouvernement évoque également des systèmes de sous-titrage automatique de cours magistraux, de retranscription d'audiences judiciaires, de rédaction de dépôts de plainte ou de comptes rendus médicaux.

5

Le déploiement de l'IA au sein des collectivités et administrations est-il poussé par les pouvoirs publics ?

On estime aujourd'hui entre 200 et 300 le nombre de tests d'utilisation d'IA en cours par les collectivités. Ces initiatives s'inscrivent dans le sillon de l'étude du Conseil d'Etat du 30 août 2022 «S'engager dans l'intelligence artificielle pour un meilleur service public», pour la mise en œuvre d'une politique de déploiement de l'IA volontariste.

Les métropoles apparaissent les plus avancées dans ce processus car elles sont souvent déjà intégrées dans un réseau numérique développé et important. C'est, par exemple, le cas de Toulouse métropole qui dispose d'un pôle dédié à l'IA («Aniti») lancé en 2019. La ville et la métropole de Montpellier ont, pour leur part, lancé une convention citoyenne afin de mettre en place une utilisation de l'IA éthique. Nantes métropole porte, elle, le projet Ekonom IA centré sur la consommation d'eau des habitants. A ce titre, elle a bénéficié du dispositif de la Cnil «bac à sable» d'accompagnement de projets utilisant l'IA au bénéfice des services publics.

6

En quoi l'IA présente-t-elle une menace pour l'information et la vie privée ?

Le risque réside dans l'influence que des contenus générés par IA peuvent avoir sur l'opinion et in fine une potentielle déstabilisation démocratique puisque l'IA peut permettre la création et la diffusion de fausses informations et d'images hyper-réalistes de personnes représentant des faits qui n'ont jamais existé («deepfakes» ou hypertrucages). En mars 2024, dans le cadre de la campagne présidentielle, des images du candidat Trump entouré d'afro-américains circulent ainsi sur le net. L'IA peut participer à l'amplification de la désinformation par les algorithmes avec un risque du ciblage d'informations personnalisées (ou recommandations), renforçant le phénomène des bulles de filtre (lorsque l'IA ne propose que des contenus similaires entre eux). Plus généralement, l'IA présente un risque en matière d'éthique et de vie privée car elle permet de surveiller et d'analyser un grand nombre de données rapidement (vidéoprotection par exemple). Ces risques sont accrus par le fait que son système «opaque» ne permet pas, pour l'instant, de mettre en place des modalités de contrôle efficaces de son fonctionnement ou des données qu'elle utilise.

7

Qu'est-ce que le concept de la «boîte noire» des IA ?

Le concept de la «boîte noire» des IA se réfère à l'opacité des algorithmes d'apprentissage automatique, dans lesquels les processus internes et les décisions prises par l'algorithme ne sont pas transparents ou compréhensibles pour les utilisateurs, et même pour les développeurs. En effet, certains systèmes d'IA réussissent à développer des compétences inattendues, pour lesquelles ils n'étaient pas formés. Cela concerne les IA conçues comme des systèmes imitant les «réseaux neuronaux» de l'intelligence humaine, leur permettant de s'autocorriger, contrairement à un algorithme fait de lignes de codes identifiables. Cette problématique soulève de nombreuses questions, par exemple sur le manque d'auditabilité des IA. Plus généralement, cette opacité entraîne une perte de confiance envers l'IAg, d'autant plus problématique dans le cadre de la relation administration/usager. Pour contrer ce phénomène, certains experts en IA proposent un nouveau modèle de «boîte blanche» plus transparent, qui s'inscrit dans l'esprit du nouveau **Règlement IA** [VOIR LEXIQUE](#) (questions 10 et s.).

8

L'IA représente-t-elle une menace pour le droit d'auteur ?

Oui, car les IA génératives ont besoin d'un grand nombre de données pour s'entraîner et pour générer des contenus nouveaux qui, in fine, tendent à ressembler le plus possible à des œuvres originales, créées par des humains.

De nombreux contentieux ont été récemment engagés, notamment aux Etats-Unis avec l'affaire Andersen dans laquelle il a été reproché à Stability AI, Deviant Art et Midjourney d'avoir entraîné leurs programmes informatiques avec des œuvres d'artistes permettant à la machine de générer un contenu «dans le style de». Les juges californiens n'ont pour l'instant pas donné raison aux artistes sur le fondement de leur copyright, faute de preuve, ce qui s'explique aussi par le manque de transparence des systèmes d'IA actuels. Plus récemment, le New York Times a poursuivi OpenAI, créateur de ChatGPT, pour violation des droits d'auteur attachés aux articles publiés par ses journalistes.

Ces affaires posent la question de l'accès licite aux données utilisées, surtout quand celles-ci sont protégées au titre du droit d'auteur.

9

Les créations générées par l'IA sont-elles protégées par le droit d'auteur ?

Non (enfin, pas pour l'instant). Aux Etats-Unis, plusieurs procédures ont été engagées par Stephen Thaler, détenteur d'un système IA (dénommé «Creativity Machine»). La justice américaine a considéré, pour le cas d'une image générée par une IA en toute autonomie, que celle-ci ne pouvait être protégée par le droit d'auteur à défaut d'intervention humaine. A contrario, aux Etats-Unis toujours, il a été retenu qu'une bande dessinée ayant été créée avec l'assistance de l'IA était protégeable par l'IA car l'intervention humaine était suffisamment établie (affaire «Zaria of the Dawn»).

En Europe, une juridiction de République tchèque a récemment jugé qu'une image générée par IA n'était pas une œuvre de l'esprit susceptible d'être protégée par le droit d'auteur. La décision s'est appuyée notamment sur le contenu du prompt qui ne démontrait pas l'empreinte de la personnalité de son auteur. Si la question n'est pas encore totalement tranchée, l'intervention humaine demeure un critère déterminant et la question reste ouverte lorsque l'IA reste un outil créatif pour l'humain.

10

Comment est régulée l'IA aujourd'hui ?

L'Union européenne s'est saisie des enjeux de l'IA dès 2018 avec le plan stratégique «IA for Europe» et le livre blanc de la Commission européenne publié en 2020, à l'origine du règlement européen sur l'IA du 21 mai 2024.

Si ce texte est la première réglementation mondiale spécifique sur l'IA, d'autres initiatives visent à l'encadrer. Le Partenariat mondial pour l'IA (PMIA), initié en 2020 et hébergé par l'OCDE, vise à guider le développement et l'utilisation responsable de l'IA. Le projet «Hiroshima Process», lancé lors du sommet du G7 en 2023 au Japon, a lui pour objectif de définir les grands principes régissant l'IA générative et les modèles d'IA avancés.

Le 17 mai 2024, le Conseil de l'Europe a adopté la convention cadre sur l'IA, les droits de l'homme, la démocratie et l'État de droit. Ce traité international, juridiquement contraignant, a été adopté par les ministres des Affaires étrangères des 46 pays membres. Il est compatible avec le règlement IA et inclut des pays comme les Etats-Unis, le Japon et le Canada, acteurs incontournables de cette nouvelle technologie.

11

Quel est l'objectif du Règlement IA approuvé le 21 mai 2024 ?

Il vise à établir un modèle de systèmes d'IA « sûrs, transparents, traçables, non discriminatoires et respectueux de l'environnement » dans l'objectif de garantir une sécurité juridique et encourager de ce fait les investissements et l'innovation au sein de l'UE.

Pour ce faire, il met en place une classification selon l'usage qui est fait de l'IA et non selon le système d'IA en lui-même, à l'exception des IA génératives, et leur niveau de risque. Il distingue ainsi les IA à risque inacceptable qui sont interdites (Cf. question 12), les IA à haut risque soumises à un régime d'autorisation avec des obligations renforcées (Cf. question 13), et les IA à risque limité ou faible soumises au respect d'obligations relatives à la transparence (par exemple, certains chatbots). Il impose de nombreuses obligations relatives à la transparence visant à informer l'utilisateur qu'il est en présence d'une IA. Il a été conçu pour s'intégrer dans l'arsenal législatif européen et assurer une cohérence avec les autres textes en vigueur, dont la Charte des droits et libertés fondamentaux et le Règlement général sur la protection des données (RGPD).

12

Le Règlement IA s'applique-t-il aux personnes publiques ?

Oui. Le Règlement IA est applicable tant aux opérateurs de systèmes d'IA conçus au sein de l'UE, qu'à ceux ayant un impact sur le territoire de l'Union, incluant ainsi des acteurs non européens. Il s'applique à une chaîne d'acteurs : le fournisseur (qui développe ou fait développer un système d'IA et le met sur le marché ou en service, à titre onéreux ou gratuit), le déployeur (qui utilise un système d'IA sous son autorité), l'importateur (qui importe un système d'IA au sein de l'UE), et le distributeur (l'intermédiaire entre le fournisseur et le déployeur). Le Règlement IA précise que le fournisseur et le déployeur peuvent être une autorité publique de sorte qu'une collectivité pourra avoir un rôle de fournisseur si elle développe un système d'IA en interne ou de déployeur si elle utilise un système d'IA pour répondre à ses besoins, dans le cadre professionnel.

Le texte ne régit pas les domaines qui sont hors des compétences de l'UE, comme les systèmes d'IA utilisés pour la sécurité nationale ou à des fins militaires. Il exclut les IA utilisées exclusivement à des fins de recherche et d'innovation.

13

Quels sont les systèmes à risque inacceptable interdits par ce texte ?

Sont interdits les systèmes qui manipulent le comportement humain par des techniques subliminales ou qui exploitent les personnes vulnérables (selon leur âge ou leur handicap), ou qui permettent d'établir un score social, notamment en fonction du comportement, du statut socio-économique ou encore des caractéristiques personnelles, ou l'évaluation du risque qu'une personne commette des infractions pénales sur la seule base d'un profilage. Le Règlement proscrie également les IA permettant la reconnaissance des émotions sur le lieu de travail et les établissements d'enseignement. Enfin, il interdit les systèmes qui extraient des images non ciblées à partir de vidéo-protection et sur internet afin de créer des bases de données aux fins de reconnaissance faciale. L'identification biométrique à distance en temps réel dans les espaces publics pour les forces de l'ordre est prohibée sauf dans trois situations : la recherche de personnes disparues, victimes d'enlèvements ou de traite des êtres humains ; la prévention d'une menace grave et imminente pour la vie ou d'un attentat terroriste prévisible ; et l'identification de suspects de crimes graves.

14

Quels sont les systèmes d'IA à haut risque acceptés par le Règlement ?

Il s'agit des systèmes d'IA utilisés comme un composant de sécurité ou comme un produit couvert par les normes de l'UE (dont les textes sont listés en annexe I du Règlement). Ils doivent faire l'objet d'une évaluation de conformité par un tiers. Sont également concernés des systèmes d'IA relatifs au traitement des données biométriques légalement autorisées, aux infrastructures critiques (par exemple la fourniture d'eau et d'électricité), à l'éducation et à la formation professionnelle ou encore ceux relatifs à la gestion de l'emploi. Sont également classés comme à haut risque les systèmes d'IA qui touchent à l'accès à des services privés et publics qualifiés d'essentiels (par exemple ceux permettant d'évaluer l'éligibilité aux aides sociales) mais aussi aux services répressifs, à la gestion des migrations, de l'asile et des contrôles aux frontières ainsi que dans le cadre de la justice et de processus démocratiques. Cela comprend les systèmes d'IA utilisés pour influencer le résultat d'une élection ou d'un référendum, ou le vote de personnes physiques (excepté les outils pour structurer les campagnes politiques sur un plan purement administratif ou logistique).

15

Que prévoit le Règlement sur la conformité des IA à haut risque ?

Les fournisseurs devront mettre en place un système de gestion des risques, assurer une gouvernance des données (notamment veiller à la qualité des données sur lesquelles l'IA s'entraîne), établir une documentation permettant aux autorités de procéder à l'évaluation de cette conformité, concevoir le système d'IA de telle sorte qu'il enregistre automatiquement les événements pertinents au cours de sa vie (problème majeur, modifications substantielles, etc.) ou encore fournir des instructions d'utilisation aux utilisateurs. La particularité de cette procédure repose sur l'enregistrement du système dans une base de données européenne et l'obtention d'une certification (marquage CE). Enfin, les fournisseurs devront mettre en place une surveillance humaine et un système de gestion de la qualité du système.

Les déployeurs devront s'assurer de la mise en place dudit contrôle humain et mener une analyse d'impact sur les droits fondamentaux. En cas de dysfonctionnement, ils devront le notifier aux autorités compétentes (qui ne sont pas encore désignées en France).

16

Comment assurer la sécurité des systèmes d'IA générative ?

Les fournisseurs des systèmes d'IA générative devront procéder à des évaluations desdits modèles, à des tests contradictoires, et assurer un suivi des IA en signalant les incidents graves et mettre en place une politique de protection de la cybersécurité suffisante. L'Anssi a récemment publié un guide de recommandations de sécurité pour ces systèmes afin de sensibiliser les administrations et les entreprises aux risques liés à leur usage.

Ses recommandations sont divisées selon la phase dans laquelle le système d'IA se trouve. Lors de la phase d'entraînement, l'Anssi préconise d'utiliser des données légitimement accessibles pour entraîner le système et protéger leur intégrité. Lors de la phase de déploiement, elle préconise la réalisation d'audits de sécurité et de tests approfondis du système d'IA. Enfin, en phase de production, elle recommande de journaliser l'ensemble des traitements réalisés au sein du système et de mettre en place des mécanismes pour détecter et bloquer les requêtes malveillantes.

17

Quelles mesures prendre pour garantir la sécurité d'un dispositif d'IA ?

Ainsi que le conseille la Cnil, pour déployer un système d'IA, il convient de combiner une analyse de sécurité « classique », portant notamment sur la sécurité de l'environnement et la sécurité du développement logiciel et de sa maintenance, avec une analyse des risques spécifiques aux systèmes d'IA et aux bases de données d'entraînement de grande taille. A cet égard, un système d'IA reposant principalement sur les données utilisées pour son entraînement, leur qualité et leur fiabilité sont primordiales. La mise en œuvre d'un plan d'action pour la sécurité est vivement recommandée et elle permettra de réduire les risques tout au long du développement du système. Il en va de même de la mise en place d'un dispositif de gestion des habilitations et de journalisation des accès.

La sécurité du dispositif d'IA doit se réfléchir à chaque étape de sa conception.

18

Que prévoit le Règlement IA en droit de la propriété intellectuelle ?

Il impose aux fournisseurs de se conformer aux lois européennes sur le droit d'auteur, notamment à la directive **Damun** **VOIR LEXIQUE** qui prévoit le mécanisme de l'« opt out » (possibilité pour les détenteurs de droits d'auteur de refuser l'utilisation de leur contenu dans le cadre de l'exception de fouille de données ou « datamining »).

Les fournisseurs devront livrer publiquement un résumé suffisamment détaillé du contenu utilisé pour l'entraînement de leurs algorithmes. Le contenu exact de ce résumé reste encore à définir afin de rendre cette disposition effective. A ce sujet, le **CSPLA** **VOIR LEXIQUE** s'est vu confier, en avril 2024, la mission d'établir la liste des informations qui devront nécessairement être rendues publiques par les fournisseurs d'IA.

En France, plusieurs organismes ont déjà actionné l'opt out (l'ADAGP, la Sacem et la Scam). Certains médias ont opté pour la voie contractuelle. Le Monde a ainsi conclu un accord avec OpenAI, créatrice de ChatGPT, permettant à son IA de se nourrir des données du journal pour son entraînement, moyennant rémunération.

19

Quelle est la gouvernance mise en place par le Règlement IA ?

Au niveau européen, le Bureau de l'IA est l'office compétent. Il dispose d'une personnalité juridique propre et d'une indépendance institutionnelle pour émettre des avis, recommandations, contributions écrites et codes de conduite sur la réglementation de l'IA. La Commission européenne a un pouvoir de régulation élargi lui permettant de retirer des systèmes d'IA du marché qu'elle juge trop risqués et de modifier la liste des IA à haut risque.

Au niveau national, des autorités de contrôle vont être désignées pour superviser la conformité des systèmes d'IA. En France, la Cnil pourrait être nommée pour cette tâche. Ces autorités devront accompagner les industries dans les évolutions dues à l'IA, notifieront les organismes d'évaluation de conformité sur les systèmes risqués qui pourraient ne pas entrer dans les normes du Règlement IA, et pourront prononcer des sanctions. En parallèle, des autorités «notifiantes» certifieront indépendamment les systèmes d'IA à haut risque et appliqueront les procédures nécessaires à la conformité des IA au niveau national.

20

Quelles sont les sanctions prévues en cas de non-respect du Règlement IA ?

Des sanctions sévères sont prévues pour dissuader les acteurs de l'IA de mettre sur le marché ou de développer des systèmes d'IA non conformes au règlement. Ces sanctions seront prononcées par l'autorité nationale de contrôle compétente. Les amendes pourront atteindre jusqu'à 35 millions d'euros ou 7% du chiffre d'affaires annuel mondial de l'entreprise pour les violations impliquant des systèmes d'IA interdits. En cas de violation d'autres obligations prévues par le Règlement IA, le montant est porté à 15 millions d'euros ou 3% du CA. Enfin, en cas de fourniture d'informations inexactes sur le système d'IA, l'amende est portée à 7,5 millions d'euros ou 1% du CA. Ces sanctions pécuniaires ne sont pas exclusives et pourront être accompagnées, par exemple, d'injonctions ou d'avertissements.

Enfin, le texte permet à toute personne physique ou morale de déposer directement une plainte auprès de l'autorité compétente, suggérant la mise en place d'une procédure spéciale pour traiter les violations de manière efficace et équitable.

21

Quand le Règlement IA entrera-t-il en vigueur ?

Pour rappel, Commission européenne a proposé le premier projet de règlement en avril 2021. Le 8 décembre 2023, le Parlement européen et le Conseil de l'Union européenne ont trouvé un accord sur ce texte, qui sera la première loi sur l'intelligence artificielle au monde. Le 13 mars 2024, les députés européens ont approuvé ce texte (par 523 voix pour, 46 contre et 49 abstentions) et le projet de Règlement IA a été officiellement adopté par le Conseil le 21 mai 2024.

L'entrée en vigueur du Règlement IA est prévue pour 2026, 20 jours après sa publication au Journal officiel, et il sera pleinement applicable 24 mois après son entrée en vigueur, à l'exception de l'interdiction des pratiques à risque inacceptable qui s'appliquera 6 mois après la date d'entrée en vigueur, des codes de pratique (lignes directrices pour l'utilisation de l'IA) qui s'appliqueront 9 mois après, des règles concernant l'IA à usage général, notamment la gouvernance, qui s'appliqueront 12 mois après, et des obligations pour les systèmes d'IA à haut risque qui, elles, s'appliqueront 36 mois après l'entrée en vigueur.

22

Comment se mettre en conformité avec le nouveau Règlement IA ?

Le Règlement IA reposant sur une classification des systèmes d'IA en fonction de leur risque à l'utilisation, il conviendra, en premier lieu, d'identifier dans quelle catégorie le système concerné doit être classé pour en déduire son régime et les obligations qui en découlent. Il faudra, également, clarifier le statut de l'acteur en cause : par exemple, une collectivité pourra être fournisseur si elle développe elle-même son système d'IA, ou bien déployeur si elle utilise le système d'IA dans le cadre professionnel (que ce soit à l'égard des usagers, ou pour une utilisation en interne). En fonction de son statut, elle n'aura pas les mêmes obligations.

Afin de permettre une meilleure compréhension du texte, l'UE a mis en ligne un site internet (artificialintelligenceact.eu/fr/) qui permet notamment de vérifier si le Règlement IA a une incidence sur l'activité de celui qui remplit un questionnaire. En tout état de cause, la mise en œuvre d'un système d'IA, surtout s'il est à haut risque, nécessitera de prévoir un cadre contractuel pour encadrer la relation entre toutes les parties prenantes.

23

Quels sont les risques d'engagement de la responsabilité en cas d'utilisation de l'IA ?

S'il collecte, exploite et conserve des données personnelles, un système d'IA doit en assurer la protection (art. 32). Cette approche par le risque impose de sécuriser les traitements. La difficulté en la matière repose sur la nécessité d'imputer une faute et donc d'identifier un ou plusieurs responsables. A cet égard, la directive européenne du 12 mars 2024 sur la responsabilité du fait des produits défectueux a intégré des règles plus protectrices des consommateurs concernant notamment les technologies émergentes. La responsabilité des fournisseurs pourrait être engagée sur ce fondement. De la même manière, la Commission européenne a publié le 28 septembre 2022 une proposition de directive relative aux règles de responsabilité civile extracontractuelle applicables aux outils d'IA. Les mécanismes d'engagement de responsabilité civile devraient donc évoluer. Les risques d'engagement de la responsabilité pénale concernant les dispositifs d'IA sont sensiblement identiques à ceux concernant la violation de données personnelles.

24

Comment assurer la conformité de sa structure au RGPD en utilisant l'IA ?

Dès lors que le système d'IA conduit à la collecte et au traitement de données personnelles, il doit nécessairement respecter le RGPD et garantir le droit des personnes concernées. A cet égard, il doit être déployé avec une finalité bien définie, reposé sur une base légale, respecté le principe de minimisation des données (collecte de données adéquate, pertinente, limitée à ce qui est nécessaire) et fixé une durée de conservation des données.

Si le système d'IA doit être conforme au RGPD, cela signifie, de la même manière, qu'il ne peut procéder qu'à une exploitation licite des données collectées. L'exercice des droits des personnes concernées est identique à celui garanti dans le cadre de la collecte de données personnelles. De manière plus spécifique concernant les dispositifs d'IA, une personne peut s'opposer à une prise de décision entièrement automatisée. Des mesures doivent également être prises pour éviter les discriminations par ce type de dispositif.

25

De quelle transparence parle-t-on ?

La transparence des systèmes d'IA est un enjeu majeur dans le cadre de la mise en place d'une IA éthique. Prôné par l'UE lors des débats sur le Règlement IA, ce principe peut se retrouver à différents niveaux.

Tout d'abord, la transparence des données d'entraînement du système d'IA est un enjeu majeur pour savoir si la source de la « connaissance » du système est licite. C'est par exemple le cas pour le respect du droit d'auteur (question n°18) ;

La transparence des systèmes d'IA se retrouve également au niveau de l'utilisation qui en est faite : une personne qui a interféré avec une IA doit en être informée (questions 7 et 11). Enfin, la transparence des IA renvoie nécessairement à la transparence des algorithmes qui, comme nous l'avons vu, est problématique du fait de l'opacité de certains systèmes d'IA complexes qui s'autocorrigent et peuvent donc échapper à la compréhension humaine.

26

Qu'entend-t-on par «transparence algorithmique» ?

La transparence algorithmique désigne la nécessité de rendre les algorithmes compréhensibles et accessibles, notamment dans le secteur public. Les personnes publiques sont soumises à une obligation de transparence sur leurs codes sources, assimilables à des documents administratifs communicables. Ce principe qui est prévu à l'article L.300-2 du **CRPA** [VOIR LEXIQUE](#) fait l'objet de quelques exceptions susceptibles de s'appliquer aux codes sources des algorithmes d'IA. C'est le cas notamment du secret des affaires. La loi du 7 octobre 2016 pour une République numérique a introduit des obligations de transparence pour les administrations qui ont recours à des traitements algorithmiques pour fonder leurs décisions administratives individuelles. Dans ces cas, il doit être explicitement mentionné que la prise de décision est fondée sur un traitement algorithmique et l'administration doit être en mesure de communiquer, à la demande de l'utilisateur, les principales caractéristiques de sa mise en œuvre. Enfin, les administrations de plus de 50 agents ont l'obligation de publier en ligne les principes de fonctionnement des traitements qu'elle utilise.

27

Comment l'IA s'articule-t-elle avec l'obligation de transparence algorithmique ?

La technologie de l'IA reposant sur des algorithmes, les personnes publiques devront, en cas de recours à de tels dispositifs respecter leurs obligations en matière de transparence algorithmique pour leurs systèmes d'IA.

Cette transparence consiste à décrire la façon dont le système d'IA renseigne tout utilisateur sur son but et son fonctionnement, et plus particulièrement comment il procède dans sa prise de décision. Afin de vérifier sa conformité aux normes applicables, notamment celles du droit d'auteur, le système d'IA doit assurer une transparence dans ses paramètres permettant une traçabilité des résultats produits.

Les normes en matière de transparence algorithmes ont été récemment modifiées par le **DSA VOIR LEXIQUE** en ce qui concerne les plateformes en ligne (notamment sur les mécanismes de préférences et de publicité ciblée), bientôt complété par les obligations issues du Règlement IA pour le cas spécifique des systèmes d'IA.

28

Quelles sont les normes en matière de transparence d'information des IA à l'égard des utilisateurs ?

Si ces règles restent encore à préciser dans la documentation qui accompagnera le Règlement IA, les fournisseurs et utilisateurs des systèmes d'IA les plus à risques seront soumis à plusieurs obligations de transparence reposant sur l'objectif d'informer l'utilisateur final de la présence d'une IA.

Les personnes qui mettent en œuvre un système d'IA doivent ainsi informer de manière claire les utilisateurs finaux lorsqu'ils interagissent avec une IA, à moins que cela ne soit évident ou que l'IA soit utilisée à des fins légalement admises, comme pour la détection de la criminalité. Ces dispositions rejoignent la loi « **SREN** » **VOIR LEXIQUE** qui prescrit de mentionner expressément que l'IA est utilisée. Les systèmes d'IA doivent également indiquer que le contenu est généré de manière artificielle. Enfin, il est obligatoire d'informer les personnes concernées en cas d'utilisation d'une IA permettant la reconnaissance faciale ou la détection des émotions (avec la même exception pour l'utilisation à des fins légales).

29

Quel est le régime juridique applicable aux caméras dans l'espace public ?

La loi n°95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité a élaboré le premier cadre juridique régissant la captation d'images de sécurité. A ce titre, les systèmes de vidéoprotection sont visés par les articles L. 251-2 du code de la sécurité intérieure (CSI) et suivants. Un système de vidéoprotection se définit par une ou plusieurs caméras filmant la voie publique et les lieux ouverts au public (espaces d'entrée et de sortie du public, comptoirs, caisses, etc.).

Le code de la sécurité intérieure prévoit que l'installation d'un système de vidéoprotection suppose de demander l'autorisation au préfet territorialement compétent. L'autorisation est valable 5 ans et renouvelable. Sa demande doit être déposée par l'autorité décidant de la mise en œuvre du dispositif, éventuellement accompagnée dans cette procédure par son prestataire technique.

Par ailleurs, ces dispositifs constituent des traitements de données personnelles et doivent être respectueux du RGPD.

30

Doit-on parler de caméras augmentées ou biométriques ?

La Cnil fait la distinction entre dispositifs de vidéo « augmentée » et dispositifs de reconnaissance biométriques. Deux critères permettent de les distinguer :

- la nature des données traitées : caractéristique physique, physiologique ou comportementale ;
- l'objectif du dispositif : identifier ou authentifier de manière unique une personne.

Un dispositif de reconnaissance biométrique cumulera toujours ces deux critères tandis qu'une caméra « augmentée » n'en remplira aucun (par exemple une caméra « augmentée » qui filme la rue pour classer les différents usages : voitures, vélos, etc.) ou seulement un des deux (par exemple une caméra « augmentée » qui détecte les bagarres dans une foule). Cette distinction emporte des conséquences juridiques : contrairement aux caméras « augmentées », les dispositifs de reconnaissance biométrique impliquent des traitements de données dites « sensibles » qui sont, par principe et sauf exceptions, interdits par le RGPD et la loi « informatique et libertés ».

31

Quels dispositifs d'IA peuvent être déployés sur des caméras ?

De multiples cas d'usage sont envisageables. Dans le secteur public, les autorités pourraient notamment exercer leurs missions de police administrative et judiciaire, notamment municipales, via la détection automatisée :

- de situations permettant de constater la commission d'infractions (stationnement interdit, dépôt sauvage d'ordures, etc.) ;
- ou encore d'évènements « suspects » ou potentiellement dangereux (attroupements d'individus, présence anormalement longue d'une personne dans des lieux et à certains moments, etc.).

Les collectivités utilisent également ces dispositifs pour la régulation des flux de circulation et l'aménagement de leur territoire, dans une logique à la fois sécuritaire, d'optimisation, écologique et économique. Ils permettent une comptabilisation et une différenciation en temps réel des usages (piétons, camions, vélos...), afin, notamment, d'identifier et de résoudre d'éventuels conflits d'usage (modification de la signalétique, développement sur la chaussée de voies, pistes réservées, etc.), ou encore d'envisager une revitalisation de certains quartiers par des décisions en matière de commerces par exemple.

32

Peut-on déployer un dispositif de caméras intelligentes en dehors de tout cadre légal ?

Non. La Cnil a notamment considéré que le code de la sécurité intérieure, qui fixe le cadre applicable aux dispositifs de vidéoprotection traditionnels, n'était pas adapté à cette nouvelle technologie.

Les dispositifs les plus intrusifs, c'est-à-dire ceux susceptibles de modifier les conditions fondamentales d'exercice des droits et libertés des personnes, ne pourront être déployés que si une loi les autorise et les encadre spécifiquement.

La Cnil estime notamment que les services de police de l'Etat ou les collectivités territoriales ne sont pas autorisés par la loi à brancher sur les caméras de vidéoprotection des dispositifs d'analyse automatique permettant de repérer des comportements contraires à l'ordre public ou des infractions. C'est dans ce cadre que la loi du 19 mai 2023 relative aux Jeux olympiques a été adoptée (voir question 31).

33

Comment s'appliquent les règles du RGPD aux caméras intelligentes ?

Les acteurs souhaitant mettre en œuvre des caméras intelligentes doivent satisfaire aux exigences de protection des données issues des textes européens, c'est-à-dire réaliser une analyse d'impact sur la protection des données, informer les personnes susceptibles d'être filmées par un système de vidéoprotection, limiter la durée de conservation des images à ce qui est nécessaire au regard de la finalité poursuivie, en plus d'assurer la sécurité des données traitées.

De plus, tout acteur qui souhaiterait déployer un dispositif de vidéo intelligente devra se fonder sur une base légale déterminée au cas par cas. La base légale de « l'intérêt légitime » ne doit pas conduire à un déséquilibre manifeste entre les intérêts poursuivis par l'utilisateur d'un dispositif de vidéo intelligente et les attentes raisonnables des personnes. De façon plus générale, il faut faire, au préalable, une démonstration de la proportionnalité du dispositif envisagé au regard des objectifs poursuivis. À ce titre, des mécanismes effectifs de protection des données et de la vie privée dès la conception (privacy by design) doivent être mis en œuvre.

34

Que prévoit l'expérimentation relative à la surveillance algorithmique ?

L'article 10 de la loi « Jeux olympiques » du 19 mai 2023 introduit la possibilité de mettre en œuvre, à titre expérimental, des dispositifs de caméras augmentées dans l'espace public.

Les images collectées grâce à des systèmes de vidéoprotection dans les lieux accueillant certaines manifestations, et à leurs abords, ainsi que dans les véhicules et les transports publics et sur les voies les desservant, peuvent ainsi faire l'objet de traitements algorithmiques.

Ces traitements doivent toutefois avoir pour objet précis de détecter en temps réel et de signaler des événements prédéterminés susceptibles de présenter ou de révéler des risques d'actes de terrorisme ou d'atteintes graves à la sécurité des personnes.

Ces événements ont été fixés par le décret n°2023-828 du 28 août 2023, et renvoient à la présence d'objets abandonnés, la présence ou l'utilisation d'armes, le non-respect par une personne du sens de circulation, des mouvements de foule, des densités trop importantes de personnes, etc.

35

Quels sont les droits des personnes filmées par ce type de caméras ?

Conformément à l'article 15 du RGPD, les personnes filmées par des caméras intelligentes ont le droit d'obtenir de l'organisme responsable de traitement la confirmation que des données personnelles les concernant sont traitées, et, le cas échéant, l'accès aux dites données.

Dans ces situations, la Cnil préconise qu'une copie des enregistrements leur soit livrée. Toutefois, les images issues des caméras de vidéoprotection devant être détruites dans un délai de 30 jours, on peut s'interroger sur la façon de conjuguer cette destruction programmée avec la délivrance des images sur un support permanent pour respecter les droits des personnes.

En outre, lorsque les données personnelles ne sont plus nécessaires au regard des finalités poursuivies par les traitements mis en œuvre, ou lorsqu'elles font l'objet d'un traitement illicite, la personne concernée peut également demander leur suppression (art. 17 RGPD).

Le droit à rectification, permettant à la personne de modifier les données traitées la concernant, comme le droit d'opposition, sont, quant à eux, peu praticables.

36

Une personne peut-elle s'opposer aux traitements mis en œuvre par des dispositifs de caméras intelligentes ?

En théorie oui... En pratique, non. Les dispositifs de caméra intelligente captent automatiquement l'image des personnes et la traitent souvent instantanément pour en tirer une conséquence en temps réel (affichage d'une publicité, calcul d'une donnée, génération d'une alerte etc.).

Dès lors, les personnes filmées n'ont pas de possibilités en pratique de s'opposer aux traitements de leurs données, dès lors que la captation d'une image constitue une donnée personnelle. Exprimer son opposition par un mouvement corporel significatif ou par le port d'une tenue d'une certaine couleur, par exemple, constituerait une contrainte trop lourde et difficilement généralisable.

A cet égard, la Cnil précise que l'existence même d'un droit d'opposition pourrait paraître antinomique avec la finalité poursuivie par le traitement, et de surcroît, compromettre l'efficacité des dispositifs de caméras intelligentes.

37

Installer ces caméras implique-t-il de réaliser une analyse d'impact sur la protection des données ?

Oui. Conformément à l'article 35 du RGPD, une analyse d'impact (aussi nommée AIPD ou PIA) doit obligatoirement être menée dès lors que le traitement est « susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées ». C'est le cas lorsqu'un traitement remplit au moins deux des neuf critères issus des lignes directrices du G29 (ancien organe de l'UE sur la protection des données), parmi lesquels figurent la « collecte de données personnelles à large échelle », un « usage innovant » et la « surveillance systématique ». La mise en œuvre de ces caméras impliquant l'emploi d'une technologie innovante, le traitement de données à grande échelle (nombre élevé de personnes concernées, volume important de données traitées) et, éventuellement, la surveillance systématique, une AIPD doit être réalisée. En outre, selon l'article 90 de la loi « informatique et libertés », l'AIPD doit être soumise à la consultation obligatoire de la Cnil quand ces traitements sont mis en œuvre par des autorités publiques.

38

Les traitements d'images à des fins statistiques bénéficient-ils d'un régime dérogatoire ?

Oui et ce régime dérogatoire permet d'exclure le droit d'opposition des personnes concernées. Pour bénéficier d'un tel régime, diverses conditions doivent être remplies.

En premier lieu, le traitement doit entrer dans le champ des traitements de données mis en œuvre à des fins statistiques, et, partant, avoir une finalité statistique, d'une part, et d'autre part, permettre la production de données agrégées et anonymes.

En second lieu, conformément à l'article 21.6 du RGPD, les traitements doivent être nécessaires à l'exécution d'une mission d'intérêt public.

A défaut, le droit d'opposition peut tout de même être exclu lorsque son exercice empêcherait l'obtention de résultats statistiques fiables, lorsqu'aucune modalité effective d'opposition ne peut en pratique être mise en œuvre ou lorsque les modalités d'opposition techniquement envisageables se révèlent plus intrusives que le traitement de données lui-même.

39

Le secteur public représente-t-il une source de données pour l'IA nécessaire à l'innovation?

Oui. Le rapport «IA : notre ambition pour la France» a rappelé que le secteur public représente une source de données à la fois nombreuses et de qualité. Leur réutilisation pourrait permettre la création de nombreux services nouveaux, pour des activités de nature commerciale comme d'intérêt général. Le principe en vigueur en Europe depuis 2003 est celui de l'ouverture et de la libre réutilisation des données publiques élaborées ou détenues par l'ensemble des organismes publics et appartenant au secteur public. Les modifications du Règlement IA sur la gouvernance des données ont pour objectifs d'étendre le champ de ce principe et d'en faciliter l'application, notamment en prévoyant une plateforme européenne unique destinée à la réutilisation de ces données. En outre, une IA générative ne pourra être utilisable que si elle est véritablement performante, ce qui ne peut être permis que par l'accès à des données fiables et de qualité.

40

De quels outils disposent les collectivités en matière d'innovation?

Les collectivités ne sont pas dépourvues d'outils pour favoriser ou bénéficier d'innovations. Le domaine qui comporte le plus de dispositifs à cet effet est le code de la commande publique, au travers du partenariat d'innovation et d'achat de prestations innovantes (voir questions n° 41 et n° 42). Autre domaine à envisager : l'organisation et le fonctionnement des collectivités, levier d'innovation le plus important avec, parmi les outils récemment et largement développés, les appels à projets (AAP), les plateformes collaboratives ou les hackathons, événements où des volontaires – originellement des développeurs – se réunissent dans un cadre temporel donné pour répondre de façon créative à la problématique posée par le service organisateur». Il existe par ailleurs des structures dédiées au soutien de l'innovation entre ou au sein de collectivités, à l'image des laboratoires d'innovation publique, ou portées par des collectivités des acteurs régionaux à l'image de l'Agence régionale du numérique et de l'intelligence artificielle en région Bourgogne-Franche-Comté qui incube des projets innovants.

41

Commande publique: qu'est-ce que le partenariat d'innovation?

Le partenariat d'innovation (art. L. 2172-3 du code de la commande publique), est un type de marché visant à faciliter la passation de marchés publics ayant pour objet des prestations de recherche et de développement. Il vise à «stimuler l'innovation» et la recherche de solutions nouvelles pour répondre aux besoins spécifiques des acheteurs publics, lorsque ces besoins ne peuvent être satisfaits par l'acquisition de produits, services ou travaux déjà disponibles sur le marché. Ce partenariat permet de coupler dans un même marché la phase de recherche et développement de produits, services ou travaux innovants à celle de leur acquisition ultérieure, sans nouvelle mise en concurrence. L'acheteur peut contracter avec plusieurs entreprises pour réaliser des études de faisabilité, chaque contrat s'exécutant alors indépendamment. Il peut aussi arrêter le contrat individuel à la fin de chaque phase (recherche, développement, acquisition). Le partenariat d'innovation permet donc aux collectivités de commander un service d'IA sur mesure à travers une procédure simplifiée couvrant la phase de recherche, développement et acquisition.

42

Quelles sont les particularités pour l'achat des prestations innovantes?

Le dispositif d'«achats innovants» (art. R. 2122-9-1, CCP) permet aux acheteurs publics de passer des marchés sans publicité ni mise en concurrence préalables pour l'achat de travaux, fournitures ou services innovants dont la valeur estimée est inférieure à 100000 € hors taxes et 80000 € HT pour les lots de fournitures ou services innovants. L'article R.2122-9-1 pose trois conditions pour bénéficier de cette franchise de mise en concurrence: d'abord, «choisir une offre pertinente», ce qui implique une évaluation rigoureuse des propositions. A cet effet, le «guide pratique: achat public innovant» de la Direction des affaires juridiques préconisait, dans sa première édition, de réaliser un «sourcing» ou une étude de marché sommaire. Ensuite, l'acheteur doit faire une bonne utilisation des deniers publics. Enfin, il doit veiller à éviter la monopolisation, il ne doit pas contracter systématiquement avec un même opérateur économique lorsqu'il existe une pluralité d'offres susceptibles de répondre au besoin. Cette technique d'achat encourage l'innovation en réduisant les obstacles à la contractualisation avec les start-up et PME.

43

Commande publique : comment identifier les prestations innovantes ?

L'article R 2124-3, alinéa 2, du code de la commande publique donne une définition – peu précise – d'une prestation innovante. Le CCP la définit positivement par rapport aux solutions existantes et négativement par rapport aux solutions en cours de développement : une prestation innovante est soit totalement nouvelle, soit une amélioration d'une prestation existante. La prestation présente un caractère inédit et n'est pas encore répandue et commercialisée sur le marché. L'innovation se distingue ensuite négativement de la recherche et développement par son caractère opérationnel. La Direction des affaires juridiques préconise de se référer à un faisceau d'indices pour apprécier si une solution peut être qualifiée d'innovante : indices relatifs au procédé, à la solution même, à sa méthode de commercialisation et à l'entreprise la proposant. Enfin, pour y voir plus clair, la loi de finances pour 2024 a identifié les jeunes entreprises innovantes (JEI) comme productrices, de par leur statut, de travaux, fournitures ou services innovants.

44

Comment prendre en compte l'IA dans les marchés et concessions ?

A l'heure actuelle, les améliorations susceptibles d'être apportées par l'IA pour les acheteurs publics paraissent nombreuses et variées. Elles demeurent toutefois qualifiées de « promesse ». Dans l'attente d'y voir plus clair sur ces améliorations et leurs implications, deux démarches semblent d'ores et déjà opportunes. D'une part, intégrer dans les cahiers des charges des marchés et des concessions des clauses traitant de l'utilisation de l'intelligence artificielle. Ces clauses pourraient, par exemple, obliger le cocontractant à prévenir l'acheteur public, dès l'offre, en cas d'exécution de prestations ou de création de résultats avec le concours de l'IA ou interdire au cocontractant de confier des données de l'acheteur public à une plateforme d'IA sans l'accord de l'acheteur public. D'autre part, l'utilisation de l'IA dans le cadre de la commande publique pourrait être intégrée dans une démarche de réflexion plus large sur l'utilisation de l'IA par la collectivité elle-même et ses agents, par exemple sous forme de schéma interne de l'IA à mettre en place et à suivre de manière partagée entre services.

45

Faut-il acheter ou développer en interne un système d'IA ?

Dans son étude « Intelligence artificielle et action publique : construire la confiance, servir la performance », le Conseil d'Etat a considéré en 2022 que « l'arbitrage entre faire et acheter (option au sein de laquelle on pourrait distinguer « faire faire » et « acheter tout fait ») ne peut être fait abstraitement, une fois pour toutes. Il doit résulter d'une analyse projet par projet des besoins induits par sa création, son développement et sa maintenance, notamment en termes de compétences. Il peut ne pas y avoir d'intérêt à recréer un SIA déjà disponible sur le marché et facilement internalisable, tout comme il peut être opportun de développer soi-même un SIA dont on maîtrisera de bout en bout l'apprentissage et l'industrialisation. Il propose trois éléments pour arbitrer ce choix : analyser les « compétences internes dont dispose l'administration pilote », « tenir compte de considérations chronologiques » et « prendre en compte [...] les contraintes liées au droit de la commande publique, très largement commandées par le droit européen et qui ne doivent pas être surestimées ».

46

Qu'est-ce qu'un territoire intelligent et durable ?

Portées par les collectivités, de nombreuses innovations voient le jour dans le cadre de projets de territoires intelligents et durables. Après avoir fait réaliser une étude relative à ce sujet en 2021, l'Etat a lancé un appel à projets au profit des collectivités du 4^e programme d'investissements d'avenir (PIA4) et du plan France Relance. Cet appel à projets a fait l'objet de deux vagues dont les lauréats ont tous été désignés. A ce titre, la Direction générale des entreprises (DGE) définit la notion de territoire intelligent et durable comme « un territoire où la donnée et les infrastructures sont au service de la mise en œuvre des politiques publiques, des services aux usagers et d'un développement territorial durable ». Un autre appel à projets concernait les « démonstrateurs d'IA frugale au service de la transition écologique dans les territoires ». Beaucoup de collectivités lancent ou portent aujourd'hui de tels projets, au-delà des appels de l'Etat.

47

Avec quelles compétences mettre en œuvre un projet de territoire intelligent et durable?

Il n'existe pas, dans le CGCT, de compétence relative à la mise en œuvre de projet de territoire intelligent et durable. Cette absence n'empêche pas les collectivités d'agir, en premier lieu, lorsque le projet vise à ce que l'une d'elles «satisfasse, par ses propres moyens, aux besoins de ses services» (CE, 29 avril 1970, société Unipain, n° 77935). Dans ce cadre, certaines lancent un achat mutualisé, par exemple via un groupement de commandes (art. L. 2113-6 et s., CCP) ou une coopération public-public (art. L. 2511-6). Le droit de la coopération n'est pas dépourvu de solutions tels les syndicats mixtes ouverts pouvant être constitué «en vue d'œuvres ou de services présentant une utilité pour chacune» (art. article L. 5721-2, CGCT) des personnes morales qui le composent ou encore les groupements d'intérêt public. Dans certains cas, les outils peuvent se rattacher à une compétence déjà exercée (par exemple, télérelève par réseau radio des compteurs d'eau potable) ou à leurs moyens généraux (collecte et traitement de données pour les RH ou les finances).

48

Quelles précautions prendre dans la mise en œuvre d'un tel projet?

L'identification de la compétence sur laquelle va être fondé le lancement d'un projet de territoire intelligent et durable est un élément structurant. Elle influe sur le ou les bénéficiaires du projet (la seule structure? ses membres? des tiers?) et peut aussi avoir des implications plus larges. Par exemple, la mise en œuvre d'un réseau d'objets connectés peut, dans certains cas, tomber dans le champ de la compétence relative aux services locaux de communications électroniques (art. L. 1425-1, CGCT). Or, cette compétence fait l'objet de règles de transfert et de mise en œuvre particulières et peut conduire la collectivité à revêtir la qualité d'opérateur au sens du code des postes et communications électroniques. Rappelons aussi que les relations entre collectivités ne sont pas exonérées par principe de mise en concurrence et peuvent constituer un marché public ou une concession dès lors que les critères prévus à l'article L. 2 du CCP sont réunis. Il importe donc de veiller à ce que les flux financiers visant à partager un outil de territoire intelligent, comme une plateforme de stockage de données, s'inscrivent dans le cadre des règles prévues audit code.

49

Quels enjeux budgétaires pour les outils d'un territoire intelligent?

Les projets de territoire intelligent peuvent nécessiter une réflexion préalable d'ordre budgétaire s'agissant des dépenses et des produits qui seront générés. En effet, les outils de ces projets (capteurs divers, caméras basse résolution, datalake, applications, IA...) serviront sans aucun doute dans le futur de manière transverse à toutes les compétences des collectivités. Or, certaines compétences doivent respecter des règles budgétaires comme celle de l'équilibre des dépenses et des recettes prévu à l'article L. 2224-2 du CGCT pour les Spic. Une collectivité qui voudra utiliser de tels outils pour son service de distribution d'eau mais aussi la gestion de ses bâtiments devra donc procéder à une analyse de l'utilisation qui sera faite des outils et à des affectations entre son budget général et son ou ses budgets annexes ou autonomes afin de répartir dépenses et produits de manière cohérente avec cette utilisation. Un autre point impactant concerne l'imputation budgétaire et l'éligibilité au FCTVA des services informatiques en nuage (SaaS, IaaS, PaaS). Les abonnements à de tels services relèvent du fonctionnement et non de l'investissement, ce qui peut freiner les projets.

50

Comment sont protégés les systèmes d'IA développés par les collectivités?

L'IA est composée de différents éléments dont des algorithmes, logiciels et données. Si le logiciel est protégé au titre du droit d'auteur prévu par le code de la propriété intellectuelle, ce n'est pas le cas de l'algorithme qui est assimilé à un principe mathématique appartenant au domaine des idées, de libres parcours, qui ne sont en principe non appropriables. En ce qui concerne les données, les règles diffèrent selon leur nature (œuvre de l'esprit, données personnelles, base de données...). Afin de protéger les différentes composantes d'un système d'IA, il est utile de se référer au droit d'auteur spécifique des logiciels et au droit sui generis des bases de données. En ce qui concerne les algorithmes, ils sont à tout le moins protégeables par la réglementation sur le secret des affaires. Enfin, si un système d'IA pris dans son ensemble constitue une invention nouvelle susceptible d'application industrielle, il pourra peut-être être éligible à la protection par le brevet qui confère un monopole d'exploitation pour une durée de 20 ans.

