

UNIVERSITÉ DE REIMS CHAMPAGNE-ARDENNE



« RGPD ET COMMANDE PUBLIQUE »

Mémoire présenté et soutenu par

Théo SIMON

Sous la direction de

M. Denis JOUVE

Professeur de droit public à l'Université de Reims Champagne-Ardenne

Directeur du Master Droit public des affaires (DPA)

En vue de l'obtention du

Diplôme de Master 2 Droit public des affaires

Année universitaire 2024-2025

Remerciements

Que serait ce mémoire sans quelques mots de remerciements, devenus à la fois évidence et nécessité. En effet, si ce travail porte ma signature, il est avant tout le fruit d'un parcours jalonné de rencontres inspirantes et de soutiens indéfectibles. Chaque page porte en elle l'empreinte de celles et ceux qui ont cru en moi, m'ont guidé et accompagné tout au long de mon parcours universitaire.

A ce titre, ma reconnaissance va d'abord à Monsieur le Professeur Denis JOUVE, directeur du Master Droit public des affaires. Son encadrement rigoureux, sa bienveillance et la qualité de ses conseils ont été déterminants à la réussite de ce mémoire. Qu'il trouve ici l'expression de mes remerciements les plus sincères, pour son investissement et la confiance dont il m'a honoré.

Je tiens également à exprimer mon éternelle gratitude à Maître Yvon GOUTAL. Outre l'idée de ce sujet – née de nos nombreuses réflexions communes – je lui dois un mentorat précieux. Sa générosité, ses conseils éclairés et sa confiance m'accompagneront, je l'espère, encore longtemps.

Évidemment, mes pensées se tournent également vers mes parents, à qui je dois tout. Sans leurs sacrifices et leur confiance inébranlable, je n'aurais jamais pu entreprendre des études de droit et nourrir l'espoir d'un avenir si prometteur. Ce mémoire leur est dédié, en reconnaissance de leur dévouement sans faille.

J'adresse une pensée toute particulière à Maurane, la femme qui illumine ma vie depuis bientôt huit années. Son soutien indéfectible dans les instants de doute, la minutie de ses relectures et la constance de ses encouragements ont été des sources précieuses de motivation dans la rédaction de ce mémoire. Sa présence à mes côtés rend chaque défi plus léger, chaque réussite plus belle.

Enfin, je n'oublie pas mes fidèles camarades de promotion (autoproclamés *Singe DPA*) : Axel, Alexis, Joshua et Karim. Ils m'ont offert les deux plus belles années universitaires imaginables. Merci pour cette amitié, ces « fous rires », et pour tous ces souvenirs, gravés à jamais dans ma mémoire.

Si ce travail de recherche marque l'aboutissement d'un cycle universitaire, il est avant tout le reflet de la richesse des liens qui l'ont rendu possible.

À tous, merci infiniment.

Sommaire

Partie I – L’application perfectible du RGPD aux contrats de la commande publique.....	11
Chapitre I – L’encadrement complexe du traitement de données à caractère personnel.....	12
Section I – L’omniprésence du traitement de données à caractère personnel dans les contrats de la commande publique	12
Section II – L’application casuistique des qualifications du RGPD aux acteurs de la commande publique	19
Chapitre II - La prise en compte partielle des exigences relatives à la protection des données personnelles par le droit de la commande publique	26
Section I – L’intégration de la protection des données au stade la passation du contrat..	27
Section II - L’intégration de la protection des données au stade de l’exécution du contrat	34
Partie II - L'articulation inachevée du droit de la commande publique et du RGPD.....	43
Chapitre I – L’existence de tensions inhérentes à l’application des garanties de protection des données personnelles aux contrats de la commande publique.....	43
Section I – La difficile conciliation entre logique de marché et protection des données personnelles	44
Section II - L’enjeu complexe et négligé du sort des données personnelles au terme du contrat.....	54
Chapitre II - L'essor de l'IA dans la commande publique ou le renouvellement des problématiques liées à la protection des données personnelles.....	67
Section I – L’intégration inéluctable de l'IA dans l'écosystème de la commande publique	68
Section II - La gouvernance des données personnelles à l’ère de la commande publique <i>augmentée</i>	80

Introduction

« *Safari ou la chasse aux Français* » : c'est par ce titre évocateur que Philippe Boucher révélait, dans un article publié dans *Le Monde* en mars 1974, l'existence d'un projet de fichage généralisé, entrepris secrètement par le ministère de l'Intérieur. Baptisé « SAFARI »¹, le projet avait pour objectif d'informatiser et d'interconnecter la plupart des fichiers administratifs français en utilisant le numéro de sécurité sociale comme identifiant unique.

Le scandale fût immédiat et huit jours seulement après cette révélation, le Premier ministre Pierre Messmer annonça l'abandon du projet et institua une commission « *Informatique et libertés* », chargée de proposer des mesures tenant à garantir un développement de l'informatique « *dans le respect de la vie privée, des libertés individuelles et des libertés publiques* »². Son rapport, remis l'année suivante, servira de fondement à la « *vénérable* »³ loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après Loi informatique et libertés ou LIL) et donnera naissance à la Commission nationale de l'informatique et des libertés (CNIL), première autorité administrative indépendante (AAI).

Évidemment, la crainte d'une dérive totalitaire *orwellienne*⁴ n'était pas une exception française et dès les années 1970, plusieurs États membres de l'Union européenne (UE) ont pris conscience des enjeux liés à l'informatisation des sociétés modernes en adoptant des règles visant à encadrer la collecte et le traitement des données personnelles.

A l'échelle européenne, la « *protection des données à caractère personnel* » occupe une place de choix. En droit primaire, elle est un droit fondamental reconnu à la fois par l'article 8 de la Charte des droits fondamentaux de l'Union européenne (CDFUE) et par l'article 16§1 du Traité sur le fonctionnement de l'Union européenne (TFUE). Il est également étroitement lié au droit au respect de la vie privée et familiale, consacré par l'article 7 de la même Charte.

En droit dérivé, dans un souci d'harmonisation et pour éviter une fragmentation territoriale, le législateur européen est venu adopter la directive 95/46/CE⁵ relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Directement inspirée de la Loi Informatique et libertés de 1978,

¹ Acronyme de « système automatisé pour les fichiers administratifs et le répertoire des individus ».

² Décret n° 74.938 du 8 novembre 1974

³ Fabien J. Matthios, « Données à caractère personnel : la CNIL découvre un trou dans la raquette », JCP A, n° 24, 14 juin 2021, 2181

⁴ 1984, George Orwell

⁵ Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO 1995, L 281, p. 31).

elle sera, pendant de nombreuses années, le principal instrument juridique applicable en la matière.

En 2013, les révélations d'Edward Snowden sur les activités de surveillance massive des services de renseignement américains provoquent un débat international sur les conséquences irréversibles de telles pratiques sur la vie privée. Elles joueront un rôle de catalyseur dans le débat européen sur la protection des données et sortiront de « l'ornière »⁶ le Règlement (UE) 2016/679⁷ sur la protection des données à caractère personnel (ci-après RGPD), longtemps débattu.

Entré en application le 25 mai 2018, le RGPD s'articule autour de six principes fondamentaux qui structurent l'ensemble du dispositif européen de protection des données personnelles : 1° licéité, loyauté et transparence ; 2° limitation des finalités ; 3° minimisation des données ; 4° exactitude ; 5° limitation de la conservation ; 6° intégrité et confidentialité.

Ces principes, énoncés à l'article 5 du Règlement, constituent le socle sur lequel repose la logique de responsabilisation (aussi appelée *accountability*) qui caractérise le nouveau paradigme européen de protection des données. Cette logique d'*accountability* constitue une rupture conceptuelle majeure par rapport au système antérieur d'autorisation préalable mis en place par la LIL et impose au responsable du traitement et à ses sous-traitants d'être en capacité de démontrer – à tout moment – leur conformité aux principes susmentionnés.

L'*accountability* se traduit par diverses obligations documentaires et organisationnelles. Sans prétendre à l'exhaustivité, à ce stade, doivent notamment être assurées : la tenue d'un registre des traitements, la réalisation d'analyses d'impact (AIPD) pour les traitements présentant des risques élevés, la désignation d'un délégué à la protection des données (DPD/DPO⁸) dans certaines circonstances (et notamment lorsque le traitement est réalisé par une autorité publique), la mise en place des mesures de protection dès la conception du traitement (*privacy by design*) et par défaut (*privacy by default*).

Parallèlement à ces évolutions en matière de protection des données, le droit de la commande publique a lui-même subi une refonte complète et constitue aujourd'hui l'une des branches les plus structurées du droit public. L'entrée en vigueur du Code de la commande publique le 1^{er}

⁶ M. Untersinger, « Ce que les « révélations Snowden » ont changé depuis 2013 », Le Monde, 13 sept. 2019

⁷ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

⁸ En anglais, « *Data Protection Officer* ».

avril 2019⁹ fait suite à trois directives européennes du 26 février 2014¹⁰. Cette codification, aboutissement d'un projet maintes fois envisagé, marque l'achèvement d'un processus d'harmonisation et de modernisation engagé depuis plusieurs décennies sous l'impulsion du droit de l'Union européenne.

Pour schématiser, la « commande publique » rassemble aujourd'hui l'ensemble des contrats par lesquels les personnes publiques répondent à leurs besoins en matière de travaux, fournitures et services moyennant une contrepartie onéreuse ; elle se divise traditionnellement en marchés publics et concessions.

Historiquement envisagé comme « *un droit des finances publiques et de police économique* »¹¹ construit autour de préoccupations axées sur la concurrence, la transparence et la bonne utilisation des deniers publics, le droit de la commande publique constitue aujourd'hui un terrain d'expression privilégié pour le numérique.

La commande publique doit ainsi être appréhendée dans le contexte plus large de la numérisation de l'action publique. En la matière, quelques précisions sémantiques s'imposent. Si la plupart des langues voisines¹² – ainsi qu'une grande partie de la doctrine¹³ – s'accordent sur l'usage du terme « *digitalisation* » pour qualifier le phénomène de transformation numérique de la commande publique, il convient de rappeler que ce terme est un anglicisme, que nous nous efforcerons d'éviter dans le cadre de cette étude.

Nous privilégierons donc les expressions « *dématérialisation* » ou « *numérisation* », selon le contexte, en marquant une préférence pour le second terme qui, à notre sens, permet d'embrasser plus largement toutes les facettes du phénomène.

Bien qu'elle ait été initiée par le Code des marchés publics de 2001, la dématérialisation de la commande publique n'était, à l'origine, que partielle. Elle sera généralisée par les directives européennes 2014/24/UE pour les marchés publics et 2014/23/UE pour les concessions,

⁹ Ord. n° 2018-1074, 26 nov. 2018, pour la partie législative du Code de la commande publique : JO 5 déc. 2018, texte n° 20. - D. n° 2018-1075, 3 déc. 2018 : JO 5 déc. 2018, texte n° 21. - D. n° 2018-1225, 24 déc. 2018, portant diverses mesures relatives aux contrats de la commande publique : JO 26 déc. 2018, texte n° 32.

¹⁰ PE et Cons. UE, dir. 2014/24/UE, sur la passation des marchés publics dite directive " secteurs classiques " : JOUE n° L 94, 28 mars 2014. - PE et Cons. UE, dir. 2014/25/UE, relative à la passation de marchés passés par des entités opérant dans les secteurs de l'eau, de l'énergie, des transports et des services postaux dite directive " secteurs spéciaux " : JOUE n° L 94, 28 mars 2014. - PE et Cons. UE, dir. 2014/23/UE, sur l'attribution de contrats de concession : JOUE n° L 94, 28 mars 2014)

¹¹ F. Rolin, Le rôle de la pratique dans la construction du droit des contrats administratifs, in A propos des contrats des personnes publiques, Mélanges en l'honneur du Professeur Laurent Richer, LGDJ, 2013, p. 9

¹² V. par exemple : « *Digitalization* » en anglais, « *Digitalisierung* » en allemand, « *digitalizacion* » en espagnol.

¹³ V. par exemple : F. Lichère, « Digitalisation de la commande publique : état des lieux et perspectives d'évolution », Contrats et Marchés publics n° 6, Juin 2024, étude 5

transposées par la suite, respectivement, par ordonnances le 23 juillet 2015 et le 29 janvier 2016.

L'article L2132-2 du Code de la commande publique dispose désormais que : « *Les communications et les échanges d'informations effectués dans le cadre de la procédure de passation d'un marché sont réalisés par voie électronique, selon des modalités et sous réserve des exceptions prévues par voie réglementaire* ». Il en ressort que depuis le 1^{er} avril 2019, la procédure de passation est obligatoirement dématérialisée pour les marchés publics dont la valeur est égale ou supérieure à 40 000 euros HT¹⁴.

En pratique, cette obligation de dématérialisation transforme radicalement les modalités d'interaction entre acheteurs publics et opérateurs économiques en créant de nouveaux espaces d'échanges numériques qui génèrent mécaniquement des traitements de données personnelles.

En réalité, la numérisation s'est imposée comme une évidence tous les pans de l'action administrative¹⁵. Ce constat n'est pas propre au cas français et peut être transposé à la plupart des pays développés¹⁶, engendrant pour certains auteurs l'émergence d'un « *État digital* »¹⁷ (*e-gouvernement*). En effet, dès les années 1990, les technologies de l'information et de la communication (TIC) sont apparues comme essentielles pour simplifier les procédures administratives et générer des économies d'échelle, notamment à travers l'abandon progressif des circuits papiers.

Initialement motivée par une volonté de simplification administrative et de rationalisation budgétaire, cette évolution s'inscrit aujourd'hui dans un cadre plus ambitieux, celui d'un « *État plateforme* »¹⁸, dont l'objectif vise la dématérialisation complète et native des documents administratifs et la facilitation de leur interconnexion par API¹⁹. Aujourd'hui, la quasi-totalité des procédures administratives sont dématérialisées nativement, bien qu'il reste parfois des voies d'accès papier, notamment pour des considérations propres à la limitation de la fracture numérique²⁰.

¹⁴ Jusqu'en 2020, le seuil était de 25 000 euros HT (R. 2132-2 du CPP).

¹⁵ AFDA, *Le droit administratif au défi du numérique*, Dalloz, 2019

¹⁶ En ce sens, pour le cas des États-Unis, voir par exemple : J. Lubbers, *Electronic Administration in the United States*, in J.-B. Auby [dir.], *Droit comparé de la procédure administrative/ Comparative Law of Administrative Procedure* : Bruylant, 2016, p. 821-831

¹⁷ L. BELLI et G. J. GUGLIELMI (dir.), *L'Etat digital*, Boulogne-Billancourt, Berger Levrault, 2022, 367 p.

¹⁸ V. L. Cluzel-Métayer et C. Prébissy-Schnall, *JurisClasseur Administratif*, Fasc. 109-32.

¹⁹ *Ibid*

²⁰ *Ibid*

De fait, la numérisation a conduit à une prolifération sans précédent des traitements de données personnelles au sein du secteur public. Pourtant, la convergence de ces deux évolutions – numérisation et renforcement de la protection des données – génère des interactions complexes, encore largement inexplorées en matière de commande publique. La complexité de cette articulation est renforcée par la diversité des configurations contractuelles auxquelles sont confrontés les acheteurs publics. Pour ne citer que les plus évidentes, les marchés publics informatiques (IT), l’externalisation des traitements de données, le recours à des dispositifs d’aide à la décision (voir à des dispositifs pouvant aller jusqu’à des décisions entièrement automatisées) et plus récemment l’émergence de l’intelligence artificielle (IA) sont autant de cas dans lesquels la maîtrise des données personnelles devient une question à la fois juridique, technique et stratégique.

Pourtant, force est de constater que l’articulation entre ces deux corpus juridiques demeure largement embryonnaire. Les références croisées entre le RGPD et le droit de la commande publique sont rares, pour ne pas dire inexistantes. De son côté, le RGPD ne mentionne les « *marchés publics* » qu’une seule fois, dans son considérant 78, tandis que pour leur part, les directives européennes de 2014 ne contenaient que quelques occurrences aux « *exigences européennes en matière de protection des données* ».

A vrai dire, le droit interne se révèle encore plus silencieux sur les liens entre protection des données et commande publique. Ce n’est qu’à partir de 2021, au travers de la réforme des cahiers des clauses administratives générales (CCAG), qu’un lien explicite entre ces deux corpus juridiques a été opéré. Ce retard d’adaptation soulève légitimement des interrogations quant à l’effectivité de la protection des données dans le cadre des contrats de la commande publique.

Si l’on observe une tendance à l’intégration progressive des exigences du RGPD dans le processus contractuel, celle-ci n’en demeure pas moins incomplète. En effet, plusieurs incertitudes persistent, tant en ce qui concerne la qualification des acteurs au regard du RGPD que la nature et l’étendue exacte de leurs obligations respectives. La jurisprudence administrative reste lacunaire sur le sujet tant les contentieux spécifiquement liés à la commande publique sont rares. Cette situation contraste avec le développement d’une activité contentieuse systématique dans d’autres domaines liés à la protection des données personnelles comme la vidéoprotection algorithmique.

Dans le contexte de numérisation croissante de l'action publique, ces deux corpus juridiques sont pourtant amenés à se rencontrer fréquemment. Ainsi, chaque étape du processus contractuel implique désormais la manipulation de quantités considérables de données personnelles : identité des candidats, données des usagers des services publics, contenus des bases de données constituées par les prestataires, etc. Cette problématique revêt d'ailleurs une acuité particulière dans les projets de « *villes intelligentes* » (*smart cities*) où le déploiement de l'intelligence artificielle génère de nouveaux points de friction.

Ainsi, l'étude des interactions entre le droit de la commande publique et le droit de la protection des données à caractère personnel présente un intérêt scientifique majeur, tant sur le plan théorique que pratique.

Sur le plan théorique, cette recherche s'inscrit dans le prolongement des réflexions menées par la doctrine²¹ sur les transformations du droit public induites par la transition numérique. Sur le plan pratique, ce mémoire répond également à une préoccupation croissante des acteurs de la commande publique à l'ère de l'IA. Les acheteurs publics, confrontés quotidiennement à ces questions, expriment un besoin d'orientation juridique pour naviguer dans cet environnement normatif complexe – qui ne tend d'ailleurs pas à se simplifier, comme en témoigne la récente adoption du Règlement sur l'intelligence artificielle²² (ci-après RIA) du 13 juin 2024.

Les enjeux pratiques sont considérables : sécurité juridique des procédures, effectivité de la protection des données, efficacité de l'action publique, etc. L'absence de cadre juridique clair génère des incertitudes qui peuvent compromettre la réalisation des objectifs poursuivis par chacun de ces droits.

La situation est d'autant plus complexe que les acheteurs publics doivent concilier leurs obligations de transparence et d'ouverture des données publiques (*Open data*) avec le respect des principes de minimisation des données, de limitation des finalités et de protection des droits des personnes concernées. Dans le même sens, les opérateurs économiques doivent adapter leurs offres aux exigences croisées de la commande publique et de la protection des données.

²¹ Pour un exemple récent, voir par exemple : « *Intelligence artificielle et droit administratif* », RFDA 2025

²² RÈGLEMENT (UE) 2024/1689 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) no 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828.

Cette double intégration ne se limite pas à une simple transposition technique et implique une véritable réflexion sur leurs finalités respectives. En effet, d'un point de vue plus conceptuel, la dualité des logiques en présence engendre des tensions juridiques que le droit positif peine encore à résoudre pleinement.

Cette imbrication s'avère d'autant plus complexe que le droit de la commande publique et le droit de la protection des données personnelles reposent sur des logiques distinctes — entre logique contractuelle et logique de « *compliance* » — et parfois antagonistes. D'un côté, la protection des données personnelles suppose une maîtrise continue sur les traitements, tandis que la logique contractuelle s'accommode d'une certaine autonomie du cocontractant. Cette tension fondamentale entre « contrôle » et « autonomie » traverse l'ensemble des problématiques soulevées par l'intersection de ces deux domaines.

Pourtant, la question de l'articulation entre la commande publique et la protection des données personnelles n'a, à notre connaissance, fait l'objet que de peu d'études spécifiques²³ justifiant d'autant plus l'intérêt d'une recherche approfondie.

Cette démarche vise à contribuer à l'élaboration d'un cadre juridique plus cohérent et plus efficace, capable de concilier les impératifs de protection des données personnelles avec les exigences de modernisation de l'action publique. Elle s'inscrit dans une perspective résolument constructive, cherchant à dépasser les oppositions apparentes pour identifier les synergies possibles entre protection des données et efficacité de la commande publique.

L'ambition de cette recherche est de fournir aux praticiens, comme aux « théoriciens », des clés de compréhension pour appréhender cette problématique complexe. Elle vise également à alimenter le débat public sur les enjeux de la numérisation de l'action publique et sur les moyens de concilier innovation technologique et protection des droits fondamentaux.

Pour toutes ces raisons, le questionnement portera, à titre principal, sur l'articulation entre ces deux corpus juridiques : si le droit de la commande publique tend, de manière croissante, à intégrer les exigences issues du Règlement général sur la protection des données (RGPD), cette intégration demeure partielle et soulève encore bon nombre d'incertitudes. La commande publique constitue-t-elle, dans ce contexte, un cadre adapté à l'application du RGPD, ou bien les tensions persistantes entre logique

²³ Sur ce point, voir I. Hasquenoph, « *Commande publique et protection des données personnelles* », AJDA, 2021, p. 2339

contractuelle et impératifs de protection des données traduisent-elles l'existence de limites structurelles à cette conciliation normative ?

En répondant à ces questions, ce mémoire cherchera à déterminer si nous assistons à une simple juxtaposition de deux régimes juridiques distincts, à une intégration harmonieuse des exigences du RGPD dans le droit de la commande publique, ou à une perturbation mutuelle nécessitant l'élaboration d'un cadre juridique plus cohérent.

L'hypothèse qui sous-tend cette recherche est que les interactions entre commande publique et protection des données personnelles, bien que complexes, ne sont ni impossibles ni contre-productives. Elles supposent toutefois un dépassement des approches purement techniques, pour intégrer une réflexion sur les finalités respectives de ces deux droits et sur leur contribution commune à l'intérêt général. Cette articulation peut même constituer un facteur d'amélioration de l'efficacité de l'action publique, à condition d'opérer certains ajustements conceptuels et pratiques.

Pour répondre à ces interrogations, cette étude s'articulera autour de deux axes complémentaires. Dans un premier temps, nous analyserons l'application du RGPD aux contrats de la commande publique, en examinant l'encadrement du traitement de données personnelles et la prise en compte progressive des exigences de protection par le droit de la commande publique (Partie I). Cette analyse révélera les mécanismes d'intégration déjà à l'œuvre et leurs limites actuelles.

Dans un second temps, nous étudierons l'articulation complexe entre ces deux corpus juridiques, en nous penchant sur les tensions structurelles qui subsistent et sur les défis nouveaux que soulève l'essor de l'IA dans la commande publique (Partie II). Cette approche permettra d'identifier les pistes d'évolution nécessaires pour une meilleure harmonisation des exigences respectives. Cette seconde partie adoptera une vision prospective, en s'interrogeant sur les adaptations nécessaires pour répondre aux défis futurs.

Partie I – L'application perfectible du RGPD aux contrats de la commande publique

Cette première partie vise à analyser les limites actuelles de l'application du RGPD dans le champ de la commande publique. Elle montrera, d'une part, que l'encadrement des traitements de données à caractère personnel se heurte à la complexité des définitions retenues et à la difficulté de qualifier précisément les acteurs impliqués (Chapitre I) ; et, d'autre part, que si le droit de la commande publique commence à intégrer les exigences liées à la protection des données, il ne le fait encore que de façon partielle et inaboutie (Chapitre II).

Il s'agira ainsi de démontrer que, si le RGPD irrigue déjà l'ensemble des contrats de la commande publique, sa mise en œuvre demeure incertaine et rend nécessaire une adaptation continue des contrats et des pratiques des acheteurs publics.

Chapitre I – L'encadrement complexe du traitement de données à caractère personnel

L'encadrement du traitement de données à caractère personnel dans les contrats de la commande publique révèle une complexité particulière, née de la rencontre entre deux corpus juridiques aux logiques distinctes. Cette complexité peut être appréhendée selon une double approche.

D'un point de vue matériel, l'architecture conceptuelle du RGPD, fondée sur des définitions résolument extensives de la « *donnée à caractère personnel* » et du « *traitement* », étend largement son emprise sur l'ensemble des contrats de la commande publique.

D'un point de vue organique, l'application des qualifications prévues par le RGPD – responsable du traitement, responsables conjoints, sous-traitant – aux acteurs de la commande publique est source de nombreuses confusions.

L'articulation de ces deux dimensions permet d'affirmer l'omniprésence du traitement de données à caractère personnel dans les contrats de la commande publique (Section I) et l'application délicate des qualifications du RGPD aux parties de ces contrats (Section II).

Section I – L'omniprésence du traitement de données à caractère personnel dans les contrats de la commande publique

L'omniprésence des traitements de données personnelles dans la commande publique résulte directement de l'architecture conceptuelle du RGPD, qui repose sur des définitions résolument extensives (I). Cette approche englobante se traduit mécaniquement par une très vaste typologie de données traitées dans le cadre des contrats de la commande publique (II).

I – L'approche extensive du traitement de données à caractère personnel retenue par le RGPD

Le RGPD s'appuie sur une approche résolument maximaliste, caractérisée par deux piliers conceptuels aux contours volontairement larges. Cette approche extensive repose sur les définitions englobantes de la « *donnée à caractère personnel* » (A) et du « *traitement* » de données (B).

A – La conception englobante de la « donnée à caractère personnel »

L'appréhension juridique des données à caractère personnel nécessite d'abord une compréhension technique de la notion de « donnée » elle-même. Ainsi, d'un point de vue technique, les données peuvent être définies comme « *toute information mise en forme pour être traitée informatiquement*²⁴ » ou, plus largement encore, « *comme toute information mise en forme, quel qu'en soit le support ou le mode de traitement* »²⁵. Cette conception « *extensive* »²⁶ révèle d'emblée le caractère potentiellement « *tentaculaire* »²⁷ de la notion.

Pour leur part, les données à caractère personnel sont entendues largement à l'article 4§1 du RGPD comme « *toute information se rapportant à une personne physique identifiée ou identifiable* ». Le même alinéa précisant qu'est réputée être une personne physique identifiable « *une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* ». Cette définition s'inscrit dans la lignée de celle issue de la directive 95/46/CE.

En pratique, il suffit qu'une personne soit « *singularisable* »²⁸ – sans pour autant qu'il soit nécessaire de pouvoir connaître son identité précise – pour qu'une donnée soit considéré comme ayant un caractère personnel²⁹.

La qualification de donnée personnelle ne se limite pas aux informations directement identifiantes : sont également concernées les données qui peuvent permettre l'identification d'une personne par suite d'une opération intellectuelle de déduction ou de recoupement. En ce sens, la CNIL a pu souligner que « *plus que sa qualité intrinsèque, c'est bien l'usage fait de la donnée initiale qui lui confère son caractère personnel* »³⁰.

²⁴ M. Boul, Réflexions sur la notion de donnée publique : RFAP, 2018/3, p. 473

²⁵ JCl. Administratif, fasc. 109-20 : Données publiques et administration numérique, par J.-B. Auby, 2023, § 31.

²⁶ JCP A, J-F Lafaix, « La maîtrise et la protection des données liées aux contrats de la commande publique : approche théorique », n° 51-52, 26 décembre 2023, 2396.

²⁷ *Ibid*

²⁸ Code de la protection des données personnelles, p. 55

²⁹ Groupe 29, avis n° 4/ 2007 du 20 juin 2007 sur le concept de données à caractère personnel.

³⁰ CNIL, délib. n° 2022-032 du 24 mars 2022

La Cour de justice de l'Union européenne (CJUE) a également pu préciser que la qualification de donnée à caractère personnel ne requiert pas que toutes les informations permettant l'identification se trouvent entre les mains d'une seule personne³¹.

Ajoutons à cela que la présence massive de données non personnelles n'empêche par l'application du RGPD si ces dernières font partie d'un ensemble « *inextricablement* »³² lié à des données personnelles.

Précisons néanmoins que le champ d'application de la notion de donnée à caractère personnel connaît une limitation importante – qui trouve toute sa pertinence en matière de commande publique. En effet, seules les informations se rapportant à des personnes physiques sont concernées. Cette restriction exclut donc, par principe, les données relatives aux personnes morales (classiquement, les sociétés). Néanmoins, cette frontière n'est pas hermétique et certaines informations relatives aux personnes morales peuvent revêtir un caractère personnel dès lors qu'elles se rapportent, directement ou indirectement, à une personne identifiée ou identifiable – nous y reviendront.

Aussi, le caractère anonyme d'une donnée conduit naturellement à exclure l'application des garanties du RGPD. Celui-ci peut découler, soit d'un processus d'anonymisation ou relever de la nature même de la donnée. Reste que la question l'anonymisation soulève des défis particuliers. Outre le fait qu'elle soit difficile techniquement pour les collectivités qui l'envisagent, les progrès technologiques – notamment l'IA – remettent en perspective l'anonymat d'aujourd'hui et impliquent que celui-ci soit « *reconsidéré régulièrement au vu des développements techniques et des possibilités de croisement des données* »³³.

Cette conception extensive de la donnée personnelle trouve naturellement son pendant dans la définition – tout aussi large – du traitement de données.

B – L'acception étendue du « traitement » de données

La définition du « *traitement* » constitue le second pilier de l'architecture extensive du RGPD. Elle aussi héritée de la directive 95/46/CE, elle bénéficie également d'une acception

³¹ CJUE, 19 octobre 2016, arrêt Breyer, C-582/14, EU :C :2016 :779, pt 43 ; CJUE, 20 décembre 2017, arrêt Novak, C-434/16, pt 31.

³² Article 2§2 du RÈGLEMENT (UE) 2018/1807 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne.

³³ Le Règlement général sur la protection des données (RGPD / GDPR), Analyse approfondie, Cécile de Terwangne, Karen Rosier, Larcier, 2018, p.

délibérément large qui reflète la volonté du législateur européen d'embrasser l'ensemble des opérations susceptibles d'affecter des données personnelles.

L'article 4§2 du RGPD en consacre une définition particulièrement large, l'entendant comme « *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel* ».

Cette définition s'accompagne d'une longue énumération – non exhaustive et n'ayant d'autre objectif que « *de souligner la polysémie du terme* »³⁴ – comprenant « *la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction* ».

En d'autres termes, la notion de « traitement » renvoi à toute opération portant sur des données personnelles³⁵. Ce positionnement révèle plusieurs caractéristiques notables. D'abord, le RGPD adopte une conception volontairement extensive de la notion de traitement, rompant avec une approche restrictive qui aurait pu limiter son champ d'application. Il opte pour une approche fonctionnelle plutôt que technique, se concentrant sur l'opération réalisée plutôt que sur les moyens utilisés. Sur ce point, le RGPD fait donc l'objet d'une grande neutralité technologique³⁶. Cette neutralité lui permettant de garantir son adaptabilité et sa longévité face au progrès technique (donc, au déploiement de l'intelligence artificielle – v. *infra*). Dans le même sens, le texte précise explicitement que l'opération peut être réalisée à l'aide « *ou non* » de procédés automatisés. Ainsi, il n'est pas nécessaire que le fichier soit informatisé ; un fichier papier doit être « *protégé dans les mêmes conditions* »³⁷.

Ensuite, il n'est pas indispensable que la donnée ait fait l'objet d'un quelconque « *traitement de valorisation* »³⁸ pour que les garanties du RGPD soient applicables. Elles le sont dès la simple « *collecte* ».

Cette définition extensive implique une approche préventive de la protection des données personnelles. Ainsi, les acheteurs publics ne peuvent plus se contenter d'une approche

³⁴ Droit des données personnelles, Dalloz décryptage, 2020, p. 35 ; Groupe 29, Opinion n°05/2014 du 10 avril 2014 sur les techniques d'anonymisation.

³⁵ G. Haas, Guide juridique du RGPD, éd. ENI, 2^e éd., 2020

³⁶ RGPD, cons. 15

³⁷ Site de la CNIL, rubrique « Définition ».

³⁸ Code de la protection des données personnelles 2025, annoté et commenté, p. 55

réactive, consistant à traiter les problèmes de protection des données au fur et à mesure qu'ils se présentent. Ils doivent anticiper l'ensemble des traitements susceptibles d'intervenir dans le cadre de leurs contrats et mettre en place des mesures de protection appropriées dès la conception des procédures (*privacy by design*) et par défaut (*privacy by default*).

Cette double extension conceptuelle – données personnelles et traitements – détermine un champ d'application particulièrement vaste du RGPD qui trouve une illustration concrète dans la diversité des situations contractuelles rencontrées en matière de commande publique.

II – La large typologie de données traitées dans les contrats de la commande publique

La diversité des configurations contractuelles révèle un panorama complexe où les données personnelles s'immiscent selon des modalités variées. Si les données traitées dans le cadre des contrats de la commande publique recourent une large typologie, cette réalité multiforme peut toutefois être appréhendée à travers une grille de lecture fonctionnelle, distinguant les situations où les traitements de données constituent l'objet même du contrat (A) de celles où ils interviennent de manière accessoire dans sa passation ou son exécution (B).

A – Le traitement de données, objet du contrat

L'émergence de nouveaux besoins public – notamment dans le cadre de la numérisation de l'action publique – a donné naissance à de nouveaux contrats où la donnée (qu'elle soit personnelle ou non) occupe une place centrale dans le contrat.

L'illustration la plus parlante de ce « traitement, objet du contrat » correspond précisément au cas des villes intelligentes (*smart cities*), que la CNIL définit exhaustivement comme « *un nouveau concept de développement urbain* » ayant pour objectif « *d'améliorer la qualité de vie des citoyens en rendant la ville plus adaptative et efficace, à l'aide de nouvelles technologies qui s'appuient sur un écosystème d'objets et de services* »³⁹.

Dans ce contexte, de nouveaux types de contrats émergent, ayant pour objet direct la collecte et l'analyse de données personnelles à des fins d'optimisation de la gestion urbaine. Ces derniers illustrent l'apparition d'une véritable économie de la donnée publique où l'information personnelle devient un élément central de la prestation contractuelle, et un facteur de performance des politiques publiques.

³⁹ Site internet de la CNIL, Section définition : « Smart city »

Concrètement, la ville intelligente englobe un périmètre très large : infrastructures publiques (bâtiments, mobiliers urbains, domotique, etc.), réseaux (eau, électricité, gaz, télécoms, etc.) transports (publics, routes et voitures intelligentes, covoiturage, mobilités douces à vélo), e-services et e-administrations⁴⁰.

Ainsi, la ville intelligente repose sur l'agrégation massive de données à travers différentes opérations (création, collecte, assemblage, interconnexion, analyse prédictive, etc.), de sorte qu'elles en constituent le « carburant »⁴¹. Les innovations technologiques déployées dans ce cadre sont innombrables et touchent tous les aspects de la vie urbaine. Pour n'en citer que quelques exemples : un dispositif de lecture automatisée des plaques d'immatriculation (LAPI), un dispositif de comptage des flux de piétons ou encore un réseau de vidéoprotection « augmenté ».

Ces technologies, porteuses d'opportunités considérables pour l'amélioration des services publics et l'optimisation des ressources urbaines, soulèvent simultanément des questions inédites en matière de protection des données personnelles. Elles nécessitent, en conséquence, une réflexion approfondie sur l'équilibre entre les bénéfices collectifs attendus et les risques individuels pour la protection de la vie privée.

Reste qu'en pratique, outre l'hypothèse des *smart cities*, de nombreux contrats ayant pour objet principal un traitement de données personnelles fleurissent dans le paysage de la commande publique. Pour ne citer que les plus évidents, ces contrats peuvent viser l'hébergement de données ; le développement de systèmes d'information (SI) ; ou encore la création et la maintenance de bases de données.

Ces contrats s'inscrivent dans le phénomène plus large d'externalisation des services publics vers des opérateurs économiques privés. Cette externalisation s'accompagne mécaniquement d'une délégation des traitements de données, où les collectivités confient à des prestataires spécialisés des missions impliquant la collecte, le stockage, l'analyse et l'exploitation de données, parmi lesquelles figurent nécessairement des données à caractère personnel.

Si cette évolution s'inscrit dans une logique – souvent trompeuse – d'efficacité et de rationalisation budgétaire, elle n'est pas sans risques et expose les acheteurs publics à de nouvelles problématiques. Cette configuration impose une vigilance particulière dans la

⁴⁰ *Ibid*

⁴¹ J-B Auby, Contrats publics et « smart cities », Contrats et Marchés publics n° 10, Octobre 2017, étude 11

définition des finalités du traitement, la détermination des moyens techniques et organisationnels de protection, et l'encadrement des droits des personnes concernées.

Cependant, cette configuration où la donnée constitue l'objet même du contrat ne représente qu'une facette du phénomène, la réalité contractuelle révélant une présence bien plus diffuse des données personnelles.

B – Le traitement de données, accessoire au contrat

Paradoxalement, c'est dans sa dimension accessoire que le traitement de données personnelles révèle sa profondeur. Cette omniprésence silencieuse se caractérise par une multitude de situations contractuelles où les données, sans constituer l'objet principal de la prestation, s'avèrent indispensables à sa passation ou son exécution.

Ce caractère accessoire ne doit pas pour autant en occulter l'immensité, ni minimiser les enjeux juridiques qui en découlent.

En premier lieu, la passation du contrat implique très souvent un traitement de données à caractère personnel. Ces dernières peuvent être présentes dans les candidatures et/ou offres présentées par les opérateurs économiques. Lorsque la candidature est celle d'une personne physique, l'ensemble des informations qui la concernent constituent des données personnelles : nom, prénom, adresse, références professionnelles etc. Évidemment, bien que les candidats soient – en grande majorité – des personnes morales, de nombreuses données à caractère personnel peuvent être en jeu. Il en est ainsi des « *nom, numéro de carte d'identité, extraits de casier judiciaire, curriculum vitae* »⁴² ; ces exemples ne sont pas limitatifs, chaque marché pouvant présenter des enjeux particuliers.

Ces données sont nécessaires à l'évaluation des candidatures et à la vérification des capacités techniques des candidats. Elles illustrent la dimension transversale de la problématique des données personnelles : la multiplicité des données personnelles impliquées dans la procédure de passation révèle l'ampleur des obligations pesant sur les acheteurs publics qui doivent respecter l'intégralité des dispositions du RGPD dès lors que des données personnelles sont concernées.

⁴² I. Hasquenoph, « *Commande publique et protection des données personnelles* », AJDA, 2021, p. 2339 ; R. Bickerstaff, *Public Procurement and the New data protection regime*, EMEA Conference, avr. 2017.

En outre, de nombreuses données pourront être transmises par l'Administration à son cocontractant pour permettre l'exécution du contrat. Il est ainsi possible de délimiter le champ de ces données « accessoires » selon qu'elles concernent les administrés ou les agents publics.

Les exemples pratiques abondent. Il en est ainsi, par exemple, dans le cadre d'un marché public de restauration scolaire. L'autorité contractante « *tient une liste nominative de personnes identifiables, indiquant les éventuelles allergies alimentaires : il s'agit de données personnelles, qui seront communiquées au prestataire* »⁴³. Il en est de même dans le cadre de concessions relatives à la gestion de l'eau qui donnent « *accès à des données personnelles telles que la localisation du foyer ou les habitudes de consommation* »⁴⁴. Ces exemples, loin d'être exhaustifs, révèlent que même les contrats publics apparemment les plus éloignés du numérique impliquent nécessairement des traitements de données personnelles.

L'identification précise des données concernées par le RGPD dans le contexte de la commande publique ne constitue qu'une première étape de l'analyse. Elle doit être complétée par une qualification rigoureuse des acteurs impliqués dans ces traitements. Reste que dans les faits, l'application des qualifications du RGPD aux acteurs de la commande publique s'avère délicate.

Section II – L'application casuistique des qualifications du RGPD aux acteurs de la commande publique

En réalité, l'application des qualifications du RGPD « *est sans doute la question la plus délicate à traiter en matière de protection des données personnelles* »⁴⁵. Sauf disposition législative expresse contraire, l'identification du responsable du traitement (I), comme celle du sous-traitant (II) exige une analyse casuistique.

I – L'identification délicate du responsable du traitement

L'identification du responsable du traitement dans le cadre de la commande publique ne peut s'opérer de manière automatique. Contrairement à une approche contractuelle classique qui tendrait à faire de l'acheteur public le donneur d'ordre systématique, le RGPD impose une analyse concrète et factuelle des circonstances de chaque espèce.

⁴³ I. Hasquenoph, « *Commande publique et protection des données personnelles* », AJDA, 2021, p. 2339

⁴⁴ *Ibid.*

⁴⁵ J-P Souyris, achatpublic.info, « La DAJ et la CNIL parlent-elles le même langage ? »

Cette approche casuistique conduit à distinguer les situations où le traitement relève de la responsabilité exclusive de l'Administration ou de son cocontractant (A), de celles impliquant une responsabilité conjointe de ces deux acteurs (B).

A – Le cas de la responsabilité « exclusive » du traitement appliqué au contrat public

Alors que l'article 4§7 du RGPD vient définir le responsable du traitement comme « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement* », le droit « commun » de la commande publique reste silencieux sur la question des responsabilités en matière de protection des données.

Évidemment, il convient de préciser que certaines dispositions sectorielles comportent un caractère prescriptif. Pour n'en citer qu'une, en matière d'eau et d'assainissement, le concessionnaire est responsable de la tenue, dans les conditions qu'il définit, du fichier des abonnés mis en œuvre pour la facturation⁴⁶.

À première vue, le contrat ayant pour objet de répondre à un besoin de l'acheteur public, il pourrait sembler logique de considérer que l'opérateur économique mettant en œuvre un traitement précisément pour répondre à ce besoin, soit qualifié de « sous-traitant », tandis que l'acheteur endosserait automatiquement la responsabilité du traitement.

Cette interprétation – réductrice – parfois encouragée par la Direction des affaires juridiques (DAJ) de Bercy⁴⁷ s'avère, en pratique, dépourvue de la nuance requise et mérite d'être écartée. En effet, le seul fait que le traitement soit réalisé pour le compte de l'acheteur ne suffit pas.

Dans les faits, la lecture des lignes directrices du Comité européen de la protection des données (ci-après CEPD) permet une compréhension plus claire et nuancée de ces concepts. Ainsi, l'identification du responsable du traitement doit sauf disposition législative contraire, « *découler d'une analyse des éléments ou circonstances factuels de l'espèce* ⁴⁸ ».

En ce sens, la CNIL précise expressément que l'Administration ne pourra être considérée comme responsable du traitement que « *si elle s'est spécifiquement intéressée à ses objectifs* ».

⁴⁶ Article R.2224-18 du Code général des collectivités territoriales.

⁴⁷ DAJ Bercy, Fiche « *L'IMPACT DU RGPD SUR LE DROIT DE LA COMMANDE PUBLIQUE* », octobre 2018.

⁴⁸ CEPD, Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD.

et conditions de mise en œuvre»⁴⁹. Elle recense ainsi trois situations dans lesquelles l'Administration pourra endosser la responsabilité du traitement : 1° lorsque l'objet même du contrat est la mise en œuvre d'un traitement de données et que ses caractéristiques y sont encadrées ; 2° lorsque l'administration a initialement exigée, dans le cadre du contrat, le déploiement du traitement, « *en le visant dans le cahier des charges définissant la nature et l'étendue des besoins à satisfaire* » ; 3° lorsque « *l'administration a porté une attention particulière aux objectifs et conditions de traitement des données personnelles, en validant celles proposées par l'opérateur économique* »⁵⁰.

En dehors de ces cas, l'opérateur économique – titulaire du contrat – endosse la responsabilité exclusive du traitement. Cette lecture est assez logique puisque dans de telles situations, le cocontractant a pu définir les objectifs et conditions de mise en œuvre du traitement « *de manière libre et indépendante* »⁵¹.

Sur ce point, la CNIL identifie deux situations dans lesquelles l'opérateur économique conserve la responsabilité de responsable du traitement. Il en sera ainsi, dans le premier cas, lorsque le contrat n'a pas pour objet principal le traitement de données. De fait, dans le cadre des marchés / concessions de travaux, des marchés de fournitures ou des « petits » marchés de service, le contrat n'a pas vocation à régir ce traitement et « *pourra se limiter à prévoir la transmission par l'administration des données utiles, sans imposer de modalités particulières pour leur traitement* »⁵².

Il en sera également ainsi, dans le second cas, des délégations de service public. En effet, ce type de contrat se confère à son titulaire une certaine liberté dans l'exécution du contrat – moyennant un transfert du risque d'exploitation. Dans ce cadre, « *les prescriptions et contrôles de l'administration compétente vont pouvoir se limiter à la définition d'une politique générale (offre de services, tarification, etc.), à la vérification de l'équilibre financier du contrat, de la qualité du service rendu (indicateurs de performance, remontées de données d'activité anonymisées, etc.), ainsi que du respect des principes gouvernant tout service public (accessibilité, égalité, continuité, etc.)* »⁵³.

⁴⁹ CNIL, Guide « *La responsabilité des acteurs dans le cadre de la commande publique* », p. 5

⁵⁰ *Ibid*, p. 8

⁵¹ *Ibid*, p. 9

⁵² *Ibid*

⁵³ *Ibid*

Pour autant, cette liberté n'est pas totale et l'Administration pourra toujours « *s'intéresser spécifiquement aux conditions de gestion des données relatives aux administrés* »⁵⁴. Dans cette hypothèse, la perspective d'une responsabilité conjointe pourra être envisagée.

B – L'hypothèse réaliste d'une responsabilité « conjointe » du traitement

Celle-ci fait l'objet d'une définition à l'article 26§1 du RGPD qui précise que « *lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement [...]* ».

Cette disposition consacre une qualification intermédiaire qui s'applique lorsque les finalités et moyens essentiels du traitement ont fait l'objet d'une « *co-construction / co-décision entre l'administration et l'opérateur économique* »⁵⁵. Cette participation conjointe peut revêtir plusieurs formes et peut notamment découler « *d'une décision commune* »⁵⁶ ou de « *décisions convergentes* »⁵⁷ prises par les deux entités.

En matière de commande publique, cette responsabilité concernera fréquemment les traitements de données intervenant dans le cadre de l'exécution des contrats liés à la gestion de missions de service public (et concernera très souvent les données des usagers).

Une nouvelle fois, le regard de la CNIL est particulièrement éclairant. D'une part, la responsabilité conjointe trouvera toute sa pertinence lorsque l'administration a « *antérieurement géré le service en régie* »⁵⁸. Dans pareille hypothèse, l'Administration se sera nécessairement intéressée – à un moment ou à un autre – aux modalités dans lesquelles sont traitées les données. Elle conserve ainsi une expertise technique, susceptible d'influencer les choix opérationnels de son cocontractant.

D'autre part, la responsabilité conjointe s'avérera particulièrement adaptée lorsque les conditions d'exploitation des données collectées « *revêtent pour [l'administration] des enjeux stratégiques majeurs d'ordre économique, politique ou juridique, notamment en raison de la finalité de leur traitement (ex. : lutte contre la fraude, sécurisation d'espaces publics) ou de la nature des informations en cause* »⁵⁹. En matière de commande publique, il s'agit

⁵⁴ *Ibid*, p. 10

⁵⁵ *Ibid*

⁵⁶ CEPD, Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, p. 3

⁵⁷ *Ibid*

⁵⁸ CNIL, Guide « La responsabilité des acteurs dans le cadre de la commande publique », p. 9

⁵⁹ *Ibid*

typiquement les données indispensables à l'exécution du service – nous auront l'occasion d'y revenir lors de développements futurs (v. *infra*).

Pour autant, il convient de souligner que la responsabilité « conjointe » n'implique pas nécessairement une responsabilité « équivalente ». En pratique, celle-ci devra être évaluée « *en tenant compte de l'ensemble des circonstances pertinentes : compétence, degré d'implication de chacun des acteurs, etc.* »⁶⁰.

Si l'identification du responsable du traitement pose des difficultés pratiques, celle du sous-traitant soulève des enjeux complémentaires, particulièrement prégnant dans le cadre de la commande publique.

II – Les défis de la qualification du sous-traitant

La qualification de sous-traitant au sens du RGPD présente également des enjeux particuliers. Pour appréhender cette notion, il est primordial d'en cerner d'abord les critères d'identification (A), avant de les mettre en perspective au regard de la source de confusion potentielle que représente le droit de la commande publique (B).

A – L'identification *in concreto* du sous-traitant RGPD

Si « *de prime abord, les terminologies employées par le droit des données personnelles paraissent fort bien se traduire en droit de la commande publique* »⁶¹ : l'acheteur public serait le responsable du traitement tandis que l'opérateur économique titulaire du contrat en serait le sous-traitant. En pratique, cette lecture manque de nuance et ces notions « *autonomes et ne coïncident pas nécessairement* »⁶².

L'article 4§8 du RGPD définit le « sous-traitant » comme « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement* ». Une nouvelle fois, la notion de sous-traitant renvoie à un « *large éventail d'acteurs* »⁶³ et à une « *très grande variété de prestataires de services* »⁶⁴.

⁶⁰ CNIL, Guide « *La responsabilité des acteurs dans le cadre de la commande publique* », p. 11

⁶¹ AJDA, « *Commande publique et protection des données personnelles* », Isabelle Hasquenoph, 2021, p. 2339

⁶² AJDA, « *Commande publique et protection des données personnelles* », Isabelle Hasquenoph, 2021, p. 2339

⁶³ CEPD, Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, p. 29

⁶⁴ CNIL, Guide du sous-traitant, sept. 2017, p. 2

In fine, les personnes susceptibles d'endosser la responsabilité de sous-traitant sont les mêmes que celles pouvant être considérées comme responsable du traitement. Pour autant, la qualité de sous-traitant suppose la réunion d'une double condition. La première est organique et le sous-traitant doit être « *une entité distincte du responsable de traitement* »⁶⁵. La seconde est fonctionnelle : le sous-traitant doit agir pour le compte du responsable du traitement. Si la première semble n'être, en pratique, qu'une formalité, la seconde s'avère plus délicate à caractériser et nécessite – elle aussi – un examen « *in concreto* »⁶⁶.

Comme pour le responsable du traitement, la qualification du sous-traitant nécessite d'examiner les « *activités concrètes [du supposé sous-traitant] dans un contexte précis* »⁶⁷. Pour ce faire, il est possible de classer les moyens du traitement en deux catégories distinctes selon qu'ils soient essentiels ou non-essentiels. Les premiers sont liés à la finalité du traitement et sont, pour cette raison, « *intrinsèquement* » réservés au responsable du traitement. Relèvent ainsi de cette catégorie⁶⁸ : le type de données traitées, la durée du traitement, la catégorie de personnes concernées. Les seconds, plus « *pratiques* », peuvent être laissés « *à la discrétion du sous-traitant* »⁶⁹. En la matière, ce dernier dispose d'une « *certaine latitude* », lui permettant de choisir « *au mieux des intérêts du responsable du traitement [...] les moyens techniques et organisationnels les plus appropriés* »⁷⁰.

Le champ d'intervention du sous-traitant étant « *déterminé par le mandat donné par le responsable du traitement* »⁷¹, dans l'hypothèse où le sous-traitant l'outrepasserait, les deux opérateurs s'exposeraient à une requalification en responsables-conjoints. Le supposé sous-traitant pourrait même se voir requalifier en responsable « unique » selon son degré d'influence dans la définition des finalités et moyens du traitement.

Si la qualité de sous-traitant (au sens du RGPD) s'avère déjà en elle-même difficile à appréhender, ces difficultés sont entretenues par la dualité des régimes de sous-traitance.

⁶⁵ CEPD, Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, p. 29

⁶⁶ CNIL, form. restr., délib. n° SAN-2018-001, 8 janv. 2018

⁶⁷ *Ibid*

⁶⁸ CEPD, Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, p. 17.

⁶⁹ *Ibid*

⁷⁰ CEPD, Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, p. 30

⁷¹ Groupe de travail « Article 29 » sur la protection des données, Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », 16 fév. 2010, p. 27

B – La dualité des régimes de sous-traitance, source de confusion pratique

En effet, rappelons que le régime de la sous-traitance au sens du droit de la commande publique, est organisé par la loi n° 75-1334 du 31 décembre 1975 et par les articles L. 2193-1 et suivants du Code de la commande publique. L'article L. 2193-2 de ce Code vient la définir comme « *l'opération par laquelle un opérateur économique confie par un sous-traité, et sous sa responsabilité, à une autre personne appelée sous-traitant, l'exécution d'une partie des prestations du marché conclu avec l'acheteur* ».

De fait, cette notion occupe une place centrale dans le droit de la commande publique – comme dans le RGPD – mais selon des logiques et des finalités distinctes. L'une des difficultés majeures de l'application du RGPD aux contrats de la commande publique réside dans la coexistence entre deux notions de « sous-traitant » qui, bien que portant la même dénomination, recouvrent pourtant des réalités juridiques distinctes et autonomes. Cette dualité conceptuelle génère des difficultés d'interprétation importantes, d'autant que les deux qualifications peuvent se cumuler ou s'exclure selon les circonstances. Il en résulte une « *confusion sémantique et terminologique* »⁷² entre ces deux qualifications.

La maîtrise de cette distinction s'avère pourtant essentielle pour déterminer les obligations applicables et organiser efficacement la répartition des responsabilités entre les parties au contrat. Il est donc important de distinguer la notion de sous-traitant au sens du RGPD de celle relevant du droit de la commande publique, nonobstant leur occasionnelle convergence pratique.

Rappelons qu'en matière de marchés publics, la sous-traitance totale est interdite⁷³ et que le titulaire du marché ne peut sous-traiter l'exécution que « *d'une partie des prestations de son marché* » ; l'acheteur pouvant d'ailleurs exiger « *que certaines tâches essentielles du marché soient effectuées directement par le titulaire* »⁷⁴. En conséquence, la nature des prestations sous-traitées doit être clairement identifiée dans le « formulaire DC4 ». Pour faire simple, ce document est un modèle de déclaration de sous-traitance pouvant être utilisé par le soumissionnaire ou le titulaire d'un marché pour présenter un sous-traitant. Il est fourni à l'acheteur soit au moment du dépôt de l'offre, soit en cours d'exécution du marché.

⁷² F. Lichère, « *Digitalisation de la commande publique : état des lieux et perspectives d'évolution* », Contrats et Marchés publics n° 6, Juin 2024, étude 5

⁷³ V. CJUE, 14 juill. 2016, aff. C. 406-14, Wrocław-Miasto Na Prawach Powiatu

⁷⁴ Article L. 2193-3 du code de la Commande publique

Dans la pratique, la confusion entre les deux régimes de sous-traitance est entretenue par le formulaire qui sert « *simultanément* »⁷⁵ de support à la déclaration de sous-traitance de prestations et de celle de sous-traitance des données à caractère personnel. En effet, la rubrique⁷⁶ du formulaire détaillant la nature des prestations ciblées consacre un volet spécifique à la sous-traitance de données à caractère personnel.

Il en résulte qu'un souhait de clarification de ces deux termes et dudit formulaire est régulièrement émis par les praticiens de la commande publique⁷⁷. Il est vrai que la CNIL⁷⁸ et la DAJ de Bercy⁷⁹ ont toutes deux produites des fiches techniques / guides à destination des acheteurs publics pour clarifier ces qualifications. Pour autant, ces diverses sources documentaires semblent parfois contradictoires au point où certains auteurs vont jusqu'à se demander si « *la DAJ et la CNIL [parlent] le même langage ?* »⁸⁰.

Du reste, il nous faut préciser que ni la CNIL, ni les juges ne sont tenus par les qualifications des parties – que ce soit responsable / coresponsables / sous-traitant – qui pourront faire l'objet d'une éventuelle requalification⁸¹ aux lourdes conséquences. Il est donc primordial que l'identification des obligations et le partage des responsabilités soit effectués en amont de la conclusion du contrat⁸².

Ces difficultés de qualification sont néanmoins à relativiser compte tenu de la prise en compte partielle des exigences relatives à la protection des données personnelles par le droit de la commande publique.

Chapitre II - La prise en compte partielle des exigences relatives à la protection des données personnelles par le droit de la commande publique

L'omniprésence des données personnelles dans la commande publique s'avérant difficilement contestable (Chapitre I), il devient impératif d'adapter les règles de passation et d'exécution des contrats de la commande publique. Fort heureusement, l'étude révèle une prise en compte partielle des exigences du RGPD par le droit de la commande publique.

⁷⁵ F. Lichère, « Digitalisation de la commande publique : état des lieux et perspectives d'évolution », Contrats et Marchés publics n° 6, Juin 2024, étude 5

⁷⁶ Rubrique « F »

⁷⁷ *Ibid*

⁷⁸ CNIL, Guide « *La responsabilité des acteurs dans le cadre de la commande publique* ».

⁷⁹ Fiche technique, « *L'impact du RGPD sur le droit de la commande publique* », octobre 2018.

⁸⁰ J-P Souyris, achatpublic.info, « *La DAJ et la CNIL parlent-elles le même langage ?* »

⁸¹ G. Desgens-Pasanau, La protection des données personnelles, Le RGPD et la nouvelle loi française : LexisNexis, 3e éd., 2018, p. 22, n° 48)

⁸² CNIL, Guide « *La responsabilité des acteurs dans le cadre de la commande publique* ».

En effet, au stade précontractuel, les mécanismes de passation des contrats se révèlent particulièrement réceptifs aux enjeux de protection des données (Section I), tandis que la phase d'exécution du contrat révèle une « aggravation » des obligations des parties et un renforcement corrélatif de leurs responsabilités (Section II).

Section I – L'intégration de la protection des données au stade la passation du contrat

Le stade de la passation se révèle propice à l'intégration des exigences de protection des données personnelles. Cette réceptivité s'explique par la convergence entre les objectifs du RGPD et les mécanismes propres au droit de la commande publique.

Le RGPD impose, en effet, au responsable du traitement de recourir uniquement à des sous-traitants présentant des *garanties suffisantes* en matière de protection des données. Cette exigence trouve un relais naturel dans les procédures de sélection des candidatures et d'attribution des contrats, qui permettent d'écarter les opérateurs défaillants et d'encourager des pratiques plus protectrices des données.

Cette intégration procédurale s'articule autour de deux leviers complémentaires : une conformité au RGPD érigée en prérequis à l'attribution du contrat (I) et par un encadrement contractuel de la sous-traitance du traitement de données (II).

I – La conformité RGPD, prérequis à l'attribution du contrat

Par certains aspects, la conformité RGPD peut s'avérer être un prérequis à l'attribution du contrat. Se faisant, le droit de la commande publique « *se fait se fait adjuvant de la protection des données personnelles* »⁸³. Il permet notamment d'exclure les opérateurs défaillants en matière de protection des données (A) et de faire du respect des données personnelles un critère de sélection des offres (B).

A – L'exclusion possible des opérateurs défaillants en matière de protection des données

Rappelons que l'article 28§1 du RGPD impose, lorsqu'un traitement doit être effectué pour le compte d'un responsable du traitement, que celui-ci fasse « *uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées* ».

⁸³ I. Hasquenoph, « *Commande publique et protection des données personnelles* », AJDA, 2021, p. 2339

A ce titre, au moment de la sélection du sous-traitant, le responsable du traitement devra s'assurer que ce premier présente des « *connaissances spécialisées* »⁸⁴, qu'il pourra notamment démontrer par l'adhésion à un code de conduite ou à un mécanisme de certification approuvé⁸⁵, voire par sa « *réputation* »⁸⁶ selon les cas.

Une nouvelle fois, les lignes directrices du CEPD s'avère d'une grande limpidité en précisant que cet examen de capacité supposera souvent « *un échange de documents pertinents* »⁸⁷. Par exemple : la politique en matière de respect de la vie privée, les conditions de service, l'enregistrement des activités de traitement, la politique en matière de gestion des documents, la politique de sécurité de l'information, les rapports des audits externes en matière de protection des données, les certifications reconnues (ex : ISO 27000) – la liste n'étant évidemment pas limitative et dépendant très largement des circonstances de chaque espèce.

Sous certains aspects, le droit de la commande publique paraît « *à même de renforcer l'effectivité du droit des données personnelles* »⁸⁸. En effet, le respect de cette exigence est facilité par les dispositions du Code de la commande publique qui permettent à l'acheteur d'exclure de la procédure de passation d'un marché / d'une concession, « *les personnes qui ont dû verser des dommages et intérêts, ont été sanctionnées par une résiliation ou ont fait l'objet d'une sanction comparable du fait d'un manquement grave ou persistant à leurs obligations contractuelles lors de l'exécution d'un contrat de la commande publique antérieur* »⁸⁹.

Plusieurs remarques s'imposent. Cette disposition s'entend comme une interdiction de soumissionner facultative laissée à l'appréciation de l'acheteur – à distinguer des interdictions de soumissionner de plein droit⁹⁰. Cette distinction revêt une importance pratique considérable dans la mesure où elle confère à l'acheteur une marge d'appréciation dans l'évaluation de la gravité des manquements et de leur impact sur la capacité du candidat à exécuter le futur contrat.

⁸⁴ Considérant 81 du RGPD

⁸⁵ Article 28§7 du RGPD

⁸⁶ CEPD, Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, p. 36

⁸⁷ *Ibid*

⁸⁸ I. Hasquenoph, « *Commande publique et protection des données personnelles* », AJDA, 2021, p. 2339

⁸⁹ Article L. 2141-7 du Code de la commande publique pour les marchés publics ; Article L. 3123-7 du même code pour les concessions.

⁹⁰ Articles L. 2141-1 à L.2141-6 du Code de la commande publique.

Par ailleurs, l'activation de cette faculté d'exclusion requiert, le respect d'une procédure contradictoire impliquant, notamment, que l'opérateur soit mis à même « *de fournir des preuves [qu'il] a pris des mesures de nature à démontrer sa fiabilité [...]* »⁹¹. Cette approche procédurale s'inscrit parfaitement dans la logique du RGPD qui privilégie les démarches correctives et préventives plutôt que purement punitives. Elle permet ainsi de concilier les impératifs de protection des données personnelles avec le principe de liberté d'accès à la commande publique.

Au-delà de l'exclusion pure et simple, le droit de la commande publique offre la possibilité de promouvoir la protection des données personnelles par l'intégration de critères spécifiques dans la sélection des offres.

B - Le respect des données personnelles comme critère de sélection des offres

En la matière, les critères de sélection doivent permettre d'identifier l'offre économiquement la plus avantageuse. Pour ce faire, le pouvoir adjudicateur peut se fonder soit sur un critère unique (le prix / le coût), soit sur une « *pluralité de critères non discriminatoires et liés à l'objet du marché ou à ses conditions d'exécution, parmi lesquels figure le critère du prix ou du coût et un ou plusieurs autres critères comprenant des aspects qualitatifs, environnementaux ou sociaux* »⁹².

Ceux-ci devront être rendus publics, en amont de la procédure de passation, dans les documents de la consultation et être pondérés (à défaut, hiérarchisés lorsqu'une telle pondération est impossible).

Pour définir ces critères, les acheteurs pourront recourir au *sourçage (sourcing)* en effectuant des consultations, en réalisant des études de marché, en sollicitant des avis ou en informant les opérateurs économiques de leurs projets et de leurs exigences⁹³ – à condition de ne pas fausser la concurrence ou de méconnaître les principes fondamentaux de la commande publique.

En pratique, les critères de sélection relatifs à la protection des données personnelles pourront revêtir une pluralité de formes. Pour apprécier les performances des opérateurs économiques en la matière, « *il pourra être exigé, au stade de la remise des offres, de faire figurer, dans un chapitre dédié du cadre de réponse technique, une description précise des méthodes de*

⁹¹ Article L. 2141-11 du Code de la commande publique.

⁹² Article R. 2152-7 du Code de la commande publique.

⁹³ Article R. 2111-1 du Code de la commande publique.

gestion de la protection des données personnelles au sein de l'entreprise »⁹⁴. Sur ce point, des documents justificatifs devraient être sollicités et notamment, selon la sensibilité du traitement envisagé : « *le registre des activités de traitement, la politique de sécurité des données personnelles, des certifications, rapports d'audits externes, etc.* »⁹⁵.

Si la prestation porte sur la collecte de données, les critères de sélection seront relatifs à la « *manière dont l'opérateur entend collecter uniquement les données nécessaires au vu des finalités définies par l'acheteur, aux garanties qu'il apporte aux personnes concernées en termes d'information, de droit d'accès ou de rectification* »⁹⁶. A l'inverse, s'il s'agit de traiter des données déjà collectées, les critères pourront être relatifs au chiffrement des données, aux garanties offertes en termes de limitation de l'accès, à leur durée de conservation ou encore à leur suppression⁹⁷.

Cette approche présente un double avantage. Du côté de l'acheteur, ces critères d'attribution permettront de « *valoriser les offres proposant les meilleures garanties en la matière* »⁹⁸. Du côté des opérateurs économiques, l'intégration de ces principes permet d'obtenir un « *avantage concurrentiel* »⁹⁹. La convergence entre ces deux objectifs pourrait « *constituer un levier pour la promotion de la protection des données personnelles* » à condition que « *les autorités contractantes développent une véritable culture de la donnée* »¹⁰⁰.

Force est de constater qu'il reste encore un chemin considérable à parcourir pour atteindre cet objectif. L'émergence progressive des systèmes d'intelligence artificielle (SIA) permettra, sans doute, d'éveiller davantage les consciences.

Si la phase de candidature permet d'intégrer ces exigences au travers de critères de sélection des offres, la phase d'attribution du contrat doit impérativement permettre de transposer ces critères en clauses contractuelles adaptées.

II – L'encadrement contractuel de la sous-traitance du traitement de données

La conformité au RGPD ne saurait se limiter à une démarche purement déclarative. Si l'identification des garanties suffisantes constitue un préalable nécessaire à la sélection d'un

⁹⁴ CNIL, Guide « *La responsabilité des acteurs dans le cadre de la commande publique* », p. 11.

⁹⁵ *Ibid*

⁹⁶ I. Hasquenoph, « *Commande publique et protection des données personnelles* », AJDA, 2021, p. 2339

⁹⁷ *Ibid*

⁹⁸ CNIL, Guide « *La responsabilité des acteurs dans le cadre de la commande publique* », p. 11.

⁹⁹ M. Griguer et J. Schwartz, Privacy by Design/Privacy by Default. Une obligation de conformité et un avantage concurrentiel, CDE 2017, n° 3

¹⁰⁰ I. Hasquenoph, « *Commande publique et protection des données personnelles* », AJDA, 2021, p. 2339

sous-traitant, leur effectivité repose fondamentalement sur leur traduction contractuelle. Sans cette articulation, les garanties exigées en matière de protection des données personnelles risqueraient de demeurer de simples déclarations d'intention (A). En la matière, la réforme des CCAG de 2021 marque une véritable rupture dans l'intégration des exigences de protection des données personnelles et révèle, par là même, les potentialités d'une convergence normative fructueuse entre les deux corpus juridiques (B).

A – L'intégration des clauses contractuelles, garantie de l'applicabilité du RGPD

Nous avons vu, à titre liminaire, que l'encadrement contractuel du traitement de données supposait que les parties au contrat qualifient juridiquement leurs rôles respectifs au regard du RGPD (v. *supra*). Cette étape préalable doit permettre d'établir un contrat listant exhaustivement toutes les obligations du sous-traitant pour garantir le respect des exigences imposées par le RGPD.

A ce titre, l'article 28§3 du RGPD impose que le traitement par un sous-traitant soit « *régi par un contrat (...)* » liant le sous-traitant au responsable du traitement (ou un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre). Il est donc tout à fait envisageable qu'un contrat de la commande publique soit en mesure de garantir l'applicabilité du RGPD.

Devront ainsi être définis par le responsable du traitement, l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement.

En pratique, ce « contrat » est souvent présenté comme une « *clause au contrat de prestation* »¹⁰¹ (*Data Protection Agreement*) et doit comporter des obligations spécifiques¹⁰². Difficile ici de ne pas céder à la tentation d'un inventaire exhaustif : le fait que le sous-traitant ne traite les données que sur « *instruction documentée* » du responsable du traitement ; veiller à ce que les personnes autorisées à traiter les données s'engagent à respecter la confidentialité ; respecter les conditions pour recruter un autre sous-traitant ; aider le responsable du traitement « *par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes* » des personnes concernées ; aider le responsable du traitement à garantir le respect de ses obligations ; supprimer toutes les données ou les renvoyer au responsable au terme de la prestation, et détruire les « *copies existantes* » ; mettre à la disposition du responsable du

¹⁰¹ Code de la protection des données personnelles, p. 135.

¹⁰² Listées non-exhaustivement à l'article 28 du RGPD.

traitement « *toutes les informations nécessaires pour démontrer le respect des obligations (...) et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté* ».

Sur ces différents points, le contrat ne doit pas se contenter de reproduire les dispositions du RGPD et doit, en pratique, « *inclure des informations plus spécifiques et concrètes sur la manière dont les conditions seront remplies et sur le niveau de sécurité requis pour le traitement de données à caractère personnel qui fait l'objet dudit accord* »¹⁰³.

Le contrat pourra s'appuyer, en toute ou partie, sur clauses contractuelles types (CTT) établies par la CNIL¹⁰⁴ et/ou par la Commission européenne¹⁰⁵. Elles peuvent faire partie d'une « *certification délivrée au responsable du traitement ou au sous-traitant* »¹⁰⁶. Ces clauses types, bien qu'elles n'aient pas de valeur impérative, permettent aux parties d'avoir un modèle sur lequel s'appuyer dans la rédaction de leurs contrats.

Outre ces clauses types, la complexité apparente de cette démarche contractuelle est atténuée par l'existence des cahiers des clauses administratives générales (CCAG). Cette standardisation présente un double intérêt pratique : garantir une cohérence dans le traitement des enjeux de protection des données et simplifier significativement la tâche des acheteurs publics dans l'élaboration de leurs contrats.

B – Une prise en compte des exigences de protection des données facilitée par les CCAG

Rappelons que les CCAG sont des documents généraux, approuvés par arrêté ministériel, auxquels les acheteurs peuvent se référer pour définir les clauses de leurs marchés. Ils « *fixent les stipulations de nature administrative applicables à une catégorie de marchés* »¹⁰⁷ et déterminent les droits et obligations des parties sur toute la vie du contrat : délais d'exécution, règles de sous-traitance, garanties et assurances, dispositions relatives aux prix et aux modalités de paiement, pénalités, etc.

Bien qu'ils soient facultatifs, ils sont, en pratique, « *massivement utilisés par les acheteurs publics* »¹⁰⁸. Leur contenu est donc susceptible d'avoir un impact « *significatif sur la vie des*

¹⁰³ CEPD, Lignes directrices 07/2020 du 7 juill. 2021 sur les concepts de responsable du traitement et de sous-traitant dans le RGPD

¹⁰⁴ CNIL, « *Sous-traitance : exemple de clauses* », 04 octobre 2017

¹⁰⁵ Décision d'exécution (UE) 2021/915 de la Commission du 4 juin 2021 relative aux clauses contractuelles types entre les responsables du traitement et les sous-traitants.

¹⁰⁶ Article 42 et 43 du RGPD.

¹⁰⁷ Article R. 2112-2 du CCP.

¹⁰⁸ DAJ Bercy, « *Réforme des cahiers des clauses administratives générales (CCAG) 2021* », avril 2021, p. 5.

*entreprises participant à la commande publique et peut favoriser les conduites vertueuses dans le cadre de l'achat public »*¹⁰⁹.

Les cinq premiers CCAG furent approuvés par arrêtés entre janvier et octobre 2009 : CCAG Travaux, CCAG Fournitures courantes et services (CCAG-FCS), CCAG-Prestations intellectuelles (CCAG-PI), CCAG Marchés industriels (CCAG-MI), et CCAG Techniques de l'information et de la communication (CCAG-TIC). Ces derniers contenaient un article 5.2 relatif à la protection des données à caractère personnel. Pour l'essentiel, celui-ci se bornait à rappeler aux parties qu'elles étaient tenue de respecter la législation applicable aux données personnelles, précisait la nécessité de conclure des avenants en cas d'évolution de celles-ci (ce qui s'est traduit par des vagues d'avenants lors de l'entrée en vigueur du RGPD), et rappelait l'obligation d'effectuer les déclarations en vue d'obtenir les autorisations administratives nécessaires à l'exécution des prestations (« *les fameuses déclarations CNIL* »¹¹⁰).

Trois ans après l'entrée en application du RGPD (et plus de 10 ans après l'entrée en vigueur des CCAG de 2009), un vaste chantier s'est lancé pour actualiser leurs dispositions : les 5 CCAG actualisés et le nouveau CCAG Maîtrise d'œuvre (CCAG-MOE) sont entrés en vigueur de façon simultanée, le 1^{er} avril 2021.

Si le numéro d'article (5.2) demeure inchangé, le contenu des dispositions s'est largement étoffé pour – enfin – « *pleinement intégrer le RGPD* »¹¹¹. Ainsi, sur le fond, l'article 5.2.1 rappelle l'application des règles européennes et françaises dès lors que l'exécution du contrat comporte des traitements de données à caractère personnel.

La révision de l'article 5.2.2 maintient la nécessité de signer un avenant en cas d'évolution de la réglementation pour se conformer aux règles nouvelles mais ajoute la possibilité pour l'acheteur de procéder à une « *modification unilatérale* » en l'absence d'accord entre les parties.

Enfin, l'article 5.2.3 vient préciser – toujours de manière non exhaustive – les informations devant figurer dans les « *documents particuliers du marché* » : « *la finalité, la description et la durée du traitement dans le strict respect des instructions documentées de l'acheteur* » ; « *les obligations de l'acheteur et celles du titulaire vis-à-vis de ce dernier, en particulier l'obligation de l'informer de toute difficulté dans l'application de la réglementation, de tout*

¹⁰⁹ *Ibid.*

¹¹⁰ Emeline Vandeven, « *La protection des données personnelles pleinement intégrée dans les CCAG* », achatpublic.info, 3 juin 2021.

¹¹¹ *Ibid.*

projet de recours à un tiers pour la mise en œuvre du traitement, ou encore de toute demande de communication de données qui lui serait adressée, ainsi que, lorsque celle-ci serait contraire à la réglementation française et européenne, des mesures adoptées pour s'y opposer » ; « les modalités de prise en compte du droit à l'information et des autres droits des personnes concernées, dont l'exercice doit être garanti » ; « les mesures de sécurité mises en œuvre pour garantir l'intégrité, la confidentialité et la disponibilité des données, ainsi que les conditions de notification des violations de données à caractère personnel » ; « la durée et les modalités de conservation des données et le sort de celles-ci au terme de l'exécution du marché ».

Toutefois, si les dispositions des CCAG rénovés constituent indéniablement une avancée significative dans l'intégration des exigences du RGPD au stade de la formation du contrat, elles n'épuisent pas pour autant la problématique de la protection des données personnelles dans la commande publique. En effet, l'effectivité de cette protection ne peut se limiter aux stipulations contractuelles initiales, aussi complètes soient-elles. Elle suppose une vigilance constante tout au long de la vie contractuelle, de la notification du marché à son terme.

C'est précisément cette exigence d'adaptabilité qui justifie un examen spécifique des modalités d'intégration de la protection des données au stade de l'exécution du contrat, phase durant laquelle les obligations se muent en contraintes opérationnelles.

Section II - L'intégration de la protection des données au stade de l'exécution du contrat

La phase d'exécution du contrat a pour objet l'accomplissement de la prestation par le titulaire du marché. Elle s'ouvre généralement par la signature du contrat et est rythmée par la mobilisation des pouvoirs exorbitants de l'acheteur public qui doit s'assurer que son cocontractant respecte les stipulations contractuelles. Sur ce point, l'analyse démontre que le RGPD est, à la fois, une source du renforcement des obligations des parties (I) et de leurs responsabilités (II).

I – Le RGPD comme source du renforcement des obligations des parties

Force est de constater que le RGPD est source d'un renforcement des obligations des parties. En ce sens, la protection des données personnelles induit un élargissement du panel des sanctions contractuelles prononçable à l'encontre du cocontractant (A), ce qui provoque mécaniquement une aggravation du « *devoir de contrôle* » de l'Administration (B).

A – L’élargissement du panel des sanctions contractuelles envisageables

En matière de sanctions, le contrat peut prévoir un large panel de mesures destinées à contraindre le titulaire à l’exécution conforme du contrat.

Les premières sont évidemment les pénalités. Elles sont applicables pour toute méconnaissance d’une obligation sur laquelle le titulaire du contrat s’est engagé. Le plus souvent, elles prennent la forme de sanctions pécuniaires forfaitaires¹¹². Dans l’immense majorité des cas, elles visent à sanctionner, soit un retard du cocontractant dans l’exécution d’une prestation, soit à sanctionner une faute commise dans l’exécution du contrat.

A titre d’illustrations, les pénalités de retard peuvent notamment sanctionner le non-respect des délais de transmission des analyses d’impact, la remise tardive de la documentation relative aux mesures techniques et organisationnelles mises en œuvre ou encore la transmission différée des registres de traitement à l’acheteur public.

Les pénalités pour faute couvrent quant à elles un spectre plus large, notamment l’absence de mise en place des mesures de sécurité exigées (chiffrement, etc.) ; la non-information des personnes concernées selon les modalités contractuellement prévues ; la sous-traitance non autorisée de tout ou partie du traitement etc. La gradation de ces pénalités doit refléter la gravité du manquement et ses conséquences potentielles sur les droits des personnes concernées.

Reste que, pour être applicables, les pénalités doivent être prévues dans le contrat. Pour être efficaces, les clauses devront faire l’objet d’une attention particulière¹¹³ lors de leur rédaction. Les documents particuliers du marché devront donc définir les manquements concernés, les modalités de calcul des pénalités¹¹⁴, les seuils d’application, les procédures de constatation des manquements, et les éventuelles possibilités d’exonération. Cette contractualisation préalable constitue la condition *sine qua non* de leur opposabilité au cocontractant (et de leur effectivité).

¹¹² Mais modulable en cas de « *montant manifestement excessif ou dérisoire eu égard au montant du marché* » (CE, 29 déc. 2008, n° 296930, SARL OPHLM de Puteaux).

¹¹³ V. S. Banel, C. Delesalle « Appliquer les pénalités contractuelles au titulaire d’un contrat public », La Gazette des communes, mai 2023.

¹¹⁴ DAJ Bercy, Fiche : « Conseils aux acheteurs et aux autorités concédantes. Les pénalités dans les marchés publics », 1^{er} avril 2019.

Sur ce point, les CCAG¹¹⁵ prévoient des clauses types, auxquelles les parties restent libres de déroger dans les documents particuliers du marché. En matière de protection des données personnelles, les CCAG de 2021 prévoient la possibilité pour d'appliquer des pénalités au titulaire du marché « *en cas de méconnaissance de la réglementation* »¹¹⁶.

Ensuite, le Code de la commande publique est venu codifier d'anciennes solutions jurisprudentielles¹¹⁷ en consacrant la possibilité de résilier le contrat en cas de « *faute d'une gravité suffisante* »¹¹⁸. En cas de manquement à ses obligations légales et/ou contractuelles relatives à la protection des données personnelles, les sanctions infligées au cocontractant peuvent aller jusqu'à la résiliation¹¹⁹ du marché pour faute. Les modalités précises de cette résiliation sont détaillées à l'article 50 des CCAG.

En *sus* de ces pénalités « classiques », bien qu'elles ne soient pas des sanctions contractuelles *stricto sensu*, il convient de (re)mentionner (v. *supra*) les futures sanctions d'exclusion dont pourra faire l'objet le cocontractant en cas de manquement à l'une de ses obligations contractuelles. Cette sanction « *à double détente* »¹²⁰ prolonge et décuple l'effet des sanctions contractuelles traditionnelles.

En effet, rappelons que l'article L. 2141-7 du CPP prévoit la faculté pour l'acheteur d'exclure « *de la procédure de passation d'un marché les personnes qui, au cours des trois années précédentes, ont dû verser des dommages et intérêts, ont été sanctionnées par une résiliation ou ont fait l'objet d'une sanction comparable du fait d'un manquement grave ou persistant à leurs obligations contractuelles lors de l'exécution d'un contrat de la commande publique antérieur* ».

Cet élargissement du panel de fautes contractuelles produit mécaniquement un renforcement du pouvoir de contrôle de l'autorité contractante. A ce titre, la mutation de ce « pouvoir » en un « *devoir de contrôle* » pose d'innombrables questions.

¹¹⁵ CCAG – Travaux, art. 19 ; CCAG – FCS, art. 14 ; CCAG – MI, art. 15 ; CCAG – TIC, art. 14 ; CCAG – PI, art. 14.

¹¹⁶ Article 5.2.3 des CCAG révisés.

¹¹⁷ CE, 30 sept. 1983, SARL Comexp : Lebon, p. 393

¹¹⁸ L. 2195-3 du CPP pour les marchés publics et L. 3136-3-1° du CCP pour les concessions.

¹¹⁹ *Ibid.*

¹²⁰ L. Folliot-Lalliot, JurisClasseur Administratif, Fasc. 775 : « *Obligations contractuelles et pouvoirs de l'Administration* ».

B – L'élargissement du « devoir » de contrôle de l'autorité contractante

La phase d'exécution du marché laisse place à d'importants pouvoirs de l'autorité contractante. Lorsqu'il s'agit de les lister, les appréciations doctrinales divergent¹²¹ et la position de la jurisprudence en la matière n'est guère plus satisfaisante. Reste qu'aujourd'hui, ces principaux pouvoirs sont énumérés à l'article L. 6 du Code de la commande publique : pouvoir de contrôle¹²², pouvoir de modification unilatérale, pouvoir de résiliation unilatérale. S'il n'est pas expressément consacré à l'article L. 6, il convient néanmoins d'y ajouter le pouvoir de direction, qui s'avère un prérequis aux autres pouvoirs.

Sur ce point, les modalités de « contrôle » interrogent aujourd'hui la doctrine : « *plus qu'un droit, l'exercice du contrôle constitue une obligation pour l'administration contractante* »¹²³. En effet, la jurisprudence¹²⁴ a déjà admis une obligation – sous peine de voir sa responsabilité engagée – d'user du pouvoir de contrôle pour vérifier la bonne exécution du contrat. Les usagers du service public peuvent d'ailleurs exercer un recours pour excès de pouvoir contre le refus de l'Administration d'exercer ses pouvoirs à l'égard de son cocontractant¹²⁵.

En pratique, la mise en œuvre de ce pouvoir/devoir de contrôle se trouve renforcée par les « récentes » exigences sociales, environnementales et éthiques imposées dans le cadre de la commande publique. Les règles applicables en matière de protection des données à caractère personnel concourent au renforcement de cette obligation et aggravent ses conséquences en cas de non-respect.

En effet, l'obligation faite au responsable du traitement de s'assurer que le sous-traitant auquel il fait appel présente « *des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées* »¹²⁶ a été interprété par l'autorité espagnole de protection des données (*Agencia Española de Protección de Datos*) comme s'imposant «

¹²¹ Pour ne citer que les plus connus : G. Jèze, *Les contrats administratifs* : t. II, 1932, p. 365 s. - G. Péquignot, *Théorie générale du contrat administratif* : 1945, p. 306 s. ; A. de Laubadère, F. Moderne, P. Delvolvé, *Traité des contrats* : t. II, p. 379, n° 1161 s. ; F.-P. Benoit, *Le droit administratif français* : D. 1968, n° 1161 s.

¹²² Le pouvoir de contrôle est d'origine jurisprudentielle : CE, 22 févr. 1952, *Sté pour exploitation procédés Ingrand*, Lebon

¹²³ H. Hoepffner, *Le pouvoir de direction et de contrôle*, in V. Bouhier et D. Riccardi (Dir.), *L'exécution des contrats administratifs*, *Le Moniteur* 2018, p. 74

¹²⁴ CE, 3 avr. 1925, *Cne de Mascara* : Lebon, p. 382 ; CE, 18 juill. 1930, *Cie des Chemins de fer PLM* : Lebon, p. 753 ; CE, 5 nov. 1937, *Caire* : Lebon, p. 899 et CE, 7 nov. 1958, *Sté Électricité et eaux de Madagascar* : Lebon, p. 530.

¹²⁵ CE, 21 déc. 1906, n° 19167, *Syndicat des propriétaires et contribuables du Quartier Croix-de-Seguey-Tivoli* à Bordeaux, Lebon p. 962

¹²⁶ Voir article 28§1 du RGPD.

durant toute l'exécution du contrat »¹²⁷ – autrement dit, pas exclusivement au moment de la passation. Les éventuelles sanctions¹²⁸ de la CNIL viennent donc s'ajouter aux sanctions traditionnelles prévues et organisées par le droit de la commande publique.

Outre ce renforcement des obligations des parties au contrat, le RGPD vient également renforcer leurs responsabilités respectives.

II – Le RGPD comme source du renforcement de la responsabilité des parties au contrat

Ce renforcement de la responsabilité des parties au contrat passe par l'aggravation du volet pénal de la commande publique (A) et par l'adjonction d'un large éventail de sanctions prononçables par la CNIL (B).

A – L'aggravation du volet pénal de la commande publique

Les risques contentieux liés à la commande publique, que ce soit lors de la passation ou de l'exécution du contrat, sont vastes. Celle-ci « *fait l'objet d'une pénalisation importante* »¹²⁹.

Loin de ne renvoyer qu'au délit d'octroi d'un avantage injustifié (le fameux délit de favoritisme), le droit de la commande publique s'accompagne d'un large éventail de peines visant à sanctionner les atteintes à la probité : délit d'octroi d'un avantage injustifié¹³⁰, prise illégale d'intérêts¹³¹, concussion¹³², la corruption¹³³ et le trafic d'influence¹³⁴ ; le détournement de biens publics¹³⁵.

Chaque infraction renvoi, outre les peines principales s'y afférentes, à des peines complémentaires. Pour n'en citer qu'une : l'interdiction d'exercer une fonction publique. Enfin, s'ajoutent à ces peines – déjà très lourdes – des mesures « *largement décriées* »¹³⁶ d'exclusion automatique pour une durée de cinq ans des procédures de passation des marchés¹³⁷ et des concessions¹³⁸.

¹²⁷ I. Hasquenoph, « *Commande publique et protection des données personnelles* », AJDA, 2021, p. 2339

¹²⁸ En l'espèce, l'AEPD avait infligé une amende de 100 000 € au responsable du traitement au titre du manquement à l'article 28§1 du RGPD.

¹²⁹ S. Corioland, « *Commande publique et risque pénal* », AJ Pénal 2022, p. 563.

¹³⁰ Article 432-14 du Code pénal.

¹³¹ Article 432-12 et 432-13 du Code pénal.

¹³² Article 432-10 du Code pénal.

¹³³ Article 432-11 du Code pénal.

¹³⁴ Article 432-11, al. 2 du Code pénal.

¹³⁵ Article 432-15 et 432-16 du Code pénal.

¹³⁶ S. Corioland, « *Commande publique et risque pénal* », AJ Pénal 2022, p. 563.

¹³⁷ Article L. 2141-1 du Code de la commande publique.

¹³⁸ Article L. 3123-1 du Code de la commande publique.

On oublie trop souvent que les dispositions du RGPD s'accompagnent, en droit interne, d'un arsenal pénal d'une grande sévérité. De nombreuses infractions relatives aux « *atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques* » ont été insérées dans le Code pénal¹³⁹. Pour n'en citer que quelques-unes, on rappellera : le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre¹⁴⁰ ; le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite¹⁴¹ ; le fait de détourner les informations collectées de leur finalité¹⁴².

Toutes ces infractions sont assorties de peines pouvant atteindre 5 ans d'emprisonnement et de 300 000 euros d'amende. Même si, dans la pratique, les sanctions sont rares, le *quantum* des peines témoigne de l'importance accordée par le législateur à ces questions.

Cette dimension pénale, bien que dissuasive, ne constitue qu'un volet de l'arsenal répressif applicable aux manquements en matière de protection des données personnelles. Viennent s'y adjoindre, le large éventail de sanctions prononçables par la CNIL en cas de méconnaissance du RGPD.

B – L'adjonction d'un large éventail de sanctions prévues par la CNIL

Les articles 77 à 79 du RGPD organisent plusieurs voies de recours au profit de la personne concernée lorsque celle-ci considère qu'un traitement de ses données personnelles a été effectué en violation des garanties prévues par la législation relative à la protection des données.

Dans cette hypothèse, la sanction prévue par le RGPD est pécuniaire et consiste en amende administrative dont le régime est détaillé à l'article 83. Pour décider s'il y a lieu d'imposer une amende et pour décider de son montant, il devra être tenu compte, dans chaque cas d'espèce, d'une vaste série d'éléments. Pour ne citer que les principaux : « *a) la nature, la gravité et la durée de la violation, compte tenu de la nature, de la portée ou de la finalité du traitement concerné, ainsi que du nombre de personnes concernées affectées et le niveau de dommage qu'elles ont subi ; b) le fait que la violation a été commise délibérément ou par négligence ; c) toute mesure prise par le responsable du traitement ou le sous-traitant pour atténuer le*

¹³⁹ Section 5 du chapitre VI du titre II du livre II du Code pénal : articles 226-16 à 226-24.

¹⁴⁰ Article 226-16 du Code de la commande publique.

¹⁴¹ Article 226-18 du Code de la commande publique.

¹⁴² Article 226-21 du Code de la commande publique.

dommage subi par les personnes concernées (...) »¹⁴³. Reste que, chaque fois qu'elles sont prononcées, ces amendes devront être « *effectives, proportionnées et dissuasives* »¹⁴⁴.

Outre ces amendes administratives, en cas de violation du RGPD, les États membres ont la liberté de déterminer « *le régime des autres sanctions applicables* »¹⁴⁵. Dans le même esprit, le considérant 155 du RGPD, repris à l'article 83§7, laisse une marge de liberté à chaque État membre pour établir « *les règles déterminant si et dans quelle mesure des amendes administratives peuvent être imposées à des autorités publiques et à des organismes publics établis sur son territoire* ».

Le régime des sanctions auxquelles la CNIL peut recourir nécessite quelques précisions. Tenant compte des libertés octroyés par le RGPD en la matière, la France a fait le choix de détailler le régime des sanctions applicables par la CNIL aux articles 20 et suivants de la LIL. Elle est aujourd'hui dotée d'un large éventail de sanctions, qu'elle peut prononcer à l'encontre du responsable du traitement, comme du sous-traitant.

Sous couvert de respecter une « *procédure contradictoire* »¹⁴⁶, elle peut notamment prononcer une ou plusieurs mesures suivantes : un rappel à l'ordre ; une injonction de mise en conformité (éventuellement sous astreinte) ; une limitation temporaire ou définitive du traitement ; le retrait d'une certification ; et même une « *amende administrative* » dont le montant ne peut excéder 10 millions d'euros (ou 2% du chiffre d'affaire – CA – annuel s'agissant d'une entreprise), portés à 20 millions d'euros (ou 4% du CA annuel) pour les manquements les plus graves.

En pratique, le régime applicable à ces amendes administratives appelle plusieurs précisions majeures. Premièrement, l'État est « *à l'image du principe d'irresponsabilité pénale*¹⁴⁷ » majoritairement exonéré de ses manquements à la protection des données personnelles et aucune sanction pécuniaire ne peut viser les traitements qu'il met en œuvre¹⁴⁸. Pourtant, le texte ne définit pas clairement la notion d'État. Il est certain que les administrations centrales¹⁴⁹ y échappent, mais les établissements publics¹⁵⁰ de l'État, les collectivités

¹⁴³ Article 83§2 du RGPD a) à k)

¹⁴⁴ Article 83§1 du RGPD.

¹⁴⁵ Article 84 du RGPD.

¹⁴⁶ Article 83§8 du RGPD.

¹⁴⁷ R. Perray, « *La sanction complexe des personnes publiques* », Communication Commerce électronique n° 3, Mars 2024, dossier 5

¹⁴⁸ Article 20 de la Loi Informatique et Libertés.

¹⁴⁹ Voir par exemple, le cas du ministère de l'Intérieur : Délibération SAN-2021-003 du 12 janvier 2021 relative à l'usage illicite de drones équipés de caméras pour contrôler le respect des mesures de confinement.

territoriales et leurs groupements, ainsi que les personnes publiques *sui generis* (Banque de France, Caisse des dépôts et consignations, etc.) restent susceptibles d'être concernées par ces sanctions pécuniaires.

Le Sénat estimait qu'en raison « *de la charge financière excessive* »¹⁵¹ que ferait peser le coût de la conformité au RGPD sur les collectivités, elles devraient bénéficier d'une exonération similaire. Finalement non retenue, cette proposition donne malgré tout lieu à une « *pratique (non dite) de la CNIL* »¹⁵² qui consiste à éviter « *soigneusement non pas de sanctionner les personnes publiques, mais de faire en sorte qu'elles ne le soient à titre pécuniaire qu'aussi rarement que possible* »¹⁵³.

En la matière, sa politique répressive se concentre sur « *le panachage entre mises en demeure et rappels à l'ordre rendus publics* »¹⁵⁴. La CNIL semble y voir un « *véritable levier d'efficacité de son pouvoir répressif à l'égard des personnes morales de droit public* »¹⁵⁵, la moindre sanction prononcée faisant « *aussitôt lieu à une diffusion médiatique nationale, surtout lorsqu'il s'agit d'organismes administratifs habituellement assimilés aux déviations de la surveillance étatique de type Big Brother* »¹⁵⁶.

¹⁵⁰ Voir par exemple, le cas de la RATP : Délibération SAN-2021-019 du 29 octobre 2021 (manquements aux principes de minimisation et de sécurité des données – amende de 400 000 euros).

¹⁵¹ R. Perray, « La sanction complexe des personnes publiques », Communication Commerce électronique n° 3, Mars 2024, dossier 5

¹⁵² *Ibid.*

¹⁵³ *Ibid.*

¹⁵⁴ *Ibid.*

¹⁵⁵ *Ibid.*

¹⁵⁶ *Ibid.*

Conclusion de la première partie

Au terme de cette première partie, il apparaît que le droit de la commande publique, confronté à l'exigence croissante de protection des données à caractère personnel, a opéré une adaptation progressive – mais encore imparfaite – à la logique imposée par le RGPD.

Le diagnostic mené a révélé l'omniprésence des traitements de données à caractère personnel au sein des contrats de la commande publique, que ces traitements de données en constituent l'objet même, ou qu'ils interviennent à titre accessoire lors de leur passation et ou de leur exécution. La nature et l'ampleur des données traitées témoignent de la profondeur de la numérisation de l'action publique, laquelle a eu pour effet de placer la question de la maîtrise et de la sécurisation des données personnelles au cœur des préoccupations des acteurs publics.

Sur le plan technique et juridique, l'analyse a mis en évidence que les notions fondamentales du RGPD s'appliquent directement aux acteurs de la commande publique, mais selon une articulation souvent complexe et nécessitant une appréciation au cas par cas. Cette complexité est encore accrue par la coexistence de deux régimes juridiques de la sous-traitance : celui, classique, de la commande publique, et celui, autonome, consacré par le RGPD. Ceux-ci ne se recourent pas nécessairement et impliquent un effort de clarification pour les praticiens.

Les développements ont pu démontrer que le droit de la commande publique s'est saisi des enjeux relatifs à la protection des données, tant au stade de la passation du contrat (par la possible exclusion des opérateurs défaillants en matière de protection des données et par la valorisation des approches respectueuses du RGPD dans les critères d'attribution) qu'au stade de son exécution (par l'élargissement du panel des sanctions contractuelles, le renforcement du volet pénal de la commande publique et par le large éventail des sanctions prononçables par la CNIL etc.).

Les derniers développements, intégrés notamment dans les CCAG depuis 2021, démontrent une volonté accrue d'organiser contractuellement la conformité aux exigences européennes et nationales en matière de protection des données. Toutefois, si ce mouvement traduit une sensibilisation grandissante des acteurs aux enjeux de conformité, il subsiste des limites importantes : incertitudes sur le partage des rôles et des responsabilités, relative rareté des sanctions prononcées à l'encontre de personnes publiques, confusions entre les deux régimes de sous-traitance.

En définitive, la première partie de cette étude a fait ressortir que l'application du RGPD aux contrats de la commande publique reste marquée par une dynamique d'intégration progressive, mais encore inachevée, oscillant entre adaptation des outils contractuels et insuffisance de l'encadrement normatif.

Si l'on observe une amélioration de la prise en compte des exigences de protection des données par le droit de la commande publique, cette intégration demeure partielle et l'effectivité du dispositif dépend encore largement de la vigilance, de la compétence des acteurs impliqués et de la traduction des obligations réglementaires en clauses contractuelles adaptées.

La suite du travail consistera à s'interroger, dans une perspective critique et prospective, sur l'articulation des deux régimes : il s'agira d'identifier les points de friction, les défis nouveaux – notamment à l'ère de l'intelligence artificielle et de la généralisation de la donnée – et de proposer des pistes pour une harmonisation susceptible de garantir un équilibre durable entre innovation et protection des droits fondamentaux.

Partie II - L'articulation inachevée du droit de la commande publique et du RGPD

L'application du RGPD aux contrats de la commande publique, analysée dans la première partie, a mis en lumière une adaptation progressive mais encore inaboutie du cadre contractuel à la protection des données à caractère personnel. Ce constat appelle désormais à s'intéresser aux tensions spécifiques qui résultent de l'imbrication – souvent conflictuelle – des logiques juridiques propres au droit de la commande publique et celles issues du RGPD.

Cette observation conduit à approfondir l'analyse, en inscrivant la réflexion dans une perspective critique et prospective. La seconde partie s'attache ainsi à examiner l'articulation inachevée entre droit de la commande publique et RGPD, en mettant en lumière, d'une part, l'existence de tensions inhérentes à l'application des garanties de protection des données personnelles aux contrats publics (Chapitre I) et, d'autre part, le renouvellement de ces problématiques à l'ère de l'intelligence artificielle (Chapitre II).

Chapitre I – L'existence de tensions inhérentes à l'application des garanties de protection des données personnelles aux contrats de la commande publique

Le présent chapitre entend démontrer l'existence de tensions structurelles et de zones d'incertitude persistantes, qui rendent imparfaite et parfois précaire la protection effective des données personnelles dans le champ de la commande publique.

Deux axes principaux structurent la réflexion : d'une part, la difficile conciliation entre la logique de marché inhérente au droit de la commande publique et l'exigence croissante de protection des droits individuels, portée par le RGPD (Section I); d'autre part, l'enjeu complexe – souvent négligé – du sort réservé aux données personnelles au terme du contrat (Section II).

Section I – La difficile conciliation entre logique de marché et protection des données personnelles

L'articulation entre commande publique et RGPD révèle une confrontation structurelle entre deux philosophies juridiques aux fondements distincts. D'un côté, la commande publique s'appuie historiquement sur une logique de marché privilégiant la transparence, la concurrence et la bonne utilisation des deniers publics ; de l'autre, le RGPD instaure une approche protectrice centrée sur la responsabilisation (*accountability*) des acteurs et la préservation de la vie privée.

Ces divergences se manifestent particulièrement dans la prééminence accordée aux impératifs économiques, laquelle constitue une limite intrinsèque à la protection des données personnelles (I). Cette confrontation s'accroît encore lorsque l'on examine le déséquilibre structurel qui oppose l'objectif de transparence de la commande publique à l'exigence de confidentialité portée par la protection des données personnelles (II).

I – Les fondements économiques de la commande publique comme limite intrinsèque à la protection des données

Si la commande publique constitue, par son ampleur et son importance, un vecteur majeur du dynamisme économique et de l'action publique, elle n'a pas, historiquement, intégré la préoccupation des droits individuels. Son ancrage dans une logique de marché, axée sur la transparence et la concurrence, tend ainsi à reléguer la confidentialité des données au second plan. Pourtant, l'avènement du RGPD a profondément rebattu les cartes, faisant émerger de nouvelles exigences qui entrent en tension, voire en contradiction, avec le socle de la commande publique.

Afin de mieux comprendre la portée de cette confrontation, il convient d'abord d'analyser la prééminence des impératifs économiques propre à la commande publique (A), puis de mettre en lumière la logique de protection des données personnelles qui fonde le RGPD (B).

A – La prééminence des impératifs économiques dans la commande publique

Nous l'évoquons en introduction, le droit de la commande publique n'a « *pas été pensé pour les individus* »¹⁵⁷ et révèle, « *par certains aspects son indifférence à l'égard de la protection des données personnelles* »¹⁵⁸ ; et pour cause, il a été historiquement envisagé comme un « *droit des finances publiques et de police économique* »¹⁵⁹.

Cette logique économique en détermine, encore aujourd'hui, les orientations principales de la commande publique. Cette dimension économique se manifeste d'abord par l'ampleur des enjeux financiers concernés. Avec un volume annuel d'environ 90 milliards d'euros – soit près de 8% du produit intérieur brut (PIB)¹⁶⁰ – les achats publics jouent un rôle structurant dans l'activité économique nationale.

L'application du droit de la concurrence aux contrats de la commande publique « *est aujourd'hui acquise* »¹⁶¹. Les principes fondamentaux de la commande publique que sont les principes d'égalité de traitement des candidats, de liberté d'accès et de transparence des procédures à ont d'abord été consacrés par la jurisprudence de la CJUE¹⁶² ; avant d'être repris par les juridictions nationales. Sans prétendre en retracer l'historique complet, le Conseil d'État est d'abord venu reconnaître les reconnaître comme principes généraux du droit¹⁶³ avant que le Conseil constitutionnel ne leur reconnaisse explicitement valeur constitutionnelle en tant qu'ils découlent des articles 6 et 14 de la Déclaration des droits de l'homme et du citoyen de 1789¹⁶⁴.

Ces principes sont aujourd'hui codifiés à l'article L. 3 du Code de la commande publique. Il en ressort que les acheteurs et les autorités concédantes doivent respecter « *le principe d'égalité de traitement des candidats à l'attribution d'un contrat de la commande publique* » et mettre en œuvre « *les principes de liberté d'accès et de transparence des procédures* ».

Au-delà de cette dimension quantitative, c'est la finalité même de la commande publique qui révèle son caractère intrinsèquement économique. Depuis le Code des marchés publics de 2004, il est expressément précisé que ces principes permettent « *d'assurer l'efficacité de la*

¹⁵⁷ I. Hasquenoph, « *Commande publique et protection des données personnelles* », AJDA, 2021, p. 2339

¹⁵⁸ *Ibid.*

¹⁵⁹ F. Rolin, Le rôle de la pratique dans la construction du droit des contrats administratifs, in A propos des contrats des personnes publiques, Mélanges en l'honneur du Professeur Laurent Richer, LGDJ, 2013, p. 9

¹⁶⁰ Banque des territoires et Intercommunalités de France, « Baromètre de la commande publique », mars 2023.

¹⁶¹ G. Kalfleche, « *Secteur public et concurrence : la convergence des droits* », AJDA 2007 p.2420

¹⁶² CJCE, 7 décembre 2000, aff. C-324/98, Telaustria.

¹⁶³ CE, avis, 29 juill. 2002, n° 246921, Sté Maj Blanchisseries de Pantin.

¹⁶⁴ Conseil constitutionnel, 26 juin 2003, n° 2003-473 DC, Loi habilitant le gouvernement à simplifier le droit.

commande publique et la bonne utilisation des deniers publics », laquelle est d'ailleurs une exigence de valeur constitutionnelle¹⁶⁵. Cette formulation traduit une approche utilitariste qui place l'optimisation de l'utilisation des deniers publics et la recherche de l'efficacité économique au cœur du système normatif. Pour nuancer notre propos, précisons néanmoins que la loi Climat et résilience¹⁶⁶, y ajoute un nouvel objectif, celui de participer « *à l'atteinte des objectifs de développement durable, dans leurs dimensions économique, sociale et environnementale* ».

Pour être complet, nous ajouterons que cette liste n'est pas limitative et que d'autres principes sont susceptibles de s'y adjoindre, de sorte, qu'en pratique, il soit possible de dissocier les principes fondamentaux de la commande publique en deux sous-ensembles : d'une part, les principes « *essentiels* » (égalité de traitement, liberté d'accès, transparence des procédures) et d'autre part, les principes « *sous-jacents* » (impartialité¹⁶⁷, reconnaissance mutuelle¹⁶⁸, proportionnalité¹⁶⁹ et droit à une protection juridictionnelle effective¹⁷⁰). Ces principes posent nécessairement la question de leur conciliation avec celle de la protection des données personnelles, mais plus largement à celle des droits et libertés fondamentaux.

La commande publique cherche à maximiser l'information disponible pour assurer la meilleure allocation des ressources publiques. Cette logique économique pousse les acheteurs publics à collecter massivement des données sur les candidats, leurs sous-traitants, leurs références, leur situation financière et leurs capacités techniques, souvent sans considération pour la proportionnalité ou la minimisation des traitements.

Les choses ne sont pas pour autant manichéennes. Il arrive que la protection des données personnelles prenne le pas sur le libre jeu de la concurrence. Il en est ainsi, notamment, lorsque la détention de données personnelles est susceptible d'avantager le titulaire sortant d'un contrat, candidat lors de son renouvellement¹⁷¹.

L'utilisation des données fait l'objet d'une attention particulière de l'Autorité de la concurrence. A titre d'exemple, elle a déjà pu identifier un abus de position dominante de Gaz

¹⁶⁵ Conseil constitutionnel, 29 déc. 2003, n° 2003-489 DC, Loi de finances pour 2004.

¹⁶⁶ Loi n° 2021-1104, 22 août 2021, portant lutte contre le dérèglement climatique et renforcement de la résilience face à ses effets ; codifié à l'article L. 3-1 du Code de la commande publique.

¹⁶⁷ CE, 12 sept. 2018, n° 420454 et 420512, SIOM de la vallée de Chevreuse : Lebon T. 2018.

¹⁶⁸ Article 34 du Traité sur le fonctionnement de l'Union européenne ; CJCE, 20 févr. 1979, aff. 120/78, Rewe-Zentral AG c/ Bundesmonopolverwaltung für Branntwein (Cassis de Dijon).

¹⁶⁹ Article 5§4 du Traité sur l'Union européenne ; CJCE, 9 juill. 1989, aff. C-265/87, Hermann Schröder.

¹⁷⁰ CJCE, 15 mai 1986, aff. 222/84, Marguerite Johnston c/ Chief Constable of the Royal Ulster Constabulary.

¹⁷¹ Autorité de la concurrence et Bundeskartellamt, « *Étude conjointe sur les données et leurs enjeux pour l'application du droit de la concurrence* », 10 mai 2016.

de France¹⁷² (GDF) résultant des modalités d'utilisation d'une base de données non répliquable par ses concurrentes et qu'il n'avait pu constituer que grâce à sa position d'opérateur historique. L'Autorité lui a ainsi – sans pour autant qualifier les données de « ressources essentielles » – enjoint, sous réserve du consentement des personnes concernées, d'accorder à ses concurrents l'accès à certaines des données figurant dans les fichiers clients. La primauté a ainsi été « *accordée à la protection des données personnelles* »¹⁷³.

La « *logique économique qui sous-tend le droit de la commande publique* »¹⁷⁴ entre en tension structurelle avec les principes fondamentaux du RGPD, révélant une incompatibilité qui dépasse le simple conflit normatif pour toucher aux philosophies mêmes de ces deux corpus juridiques. Sur ce point, la logique de responsabilisation imposée par le RGPD s'avère antagoniste à ces impératifs économiques.

B – L'Accountability du RGPD, une logique antagoniste aux impératifs économiques

À rebours de la logique de marché propre à la commande publique, le RGPD repose sur le principe de responsabilité (*accountability*), inspiré très largement des lignes directrices de l'OCDE¹⁷⁵. Consacré par les articles 5§2 et 24 du RGPD, il marque un changement de paradigme important en matière de protection des données personnelles : les traitements ne font plus l'objet d'un contrôle *ex ante* – au travers des autorisations préalables délivrées par la CNIL – mais *ex post* – au travers des divers contrôles menés par la CNIL.

Sur ce point, la doctrine de l'ère pré-RGPD s'adonnait à une comparaison intéressante et assimilait l'ancien régime d'autorisation préalable organisé par la LIL à un régime de police administrative¹⁷⁶. Reste que ce cadre d'analyse s'avère aujourd'hui désuet compte tenu du changement de logique opéré par le RGPD.

Ainsi, pour le responsable du traitement et son sous-traitant, deux types d'obligations découlent de ce principe cardinal : celle de mettre en œuvre « *proactivement* »¹⁷⁷ les mesures techniques et organisationnelles pour assurer la protection des données, et celle de

¹⁷² Autorité de la concurrence, déc. n° 14-MC-02, 9 sept. 2014 relative à une demande de mesures conservatoires présentée par la société Direct Energie dans les secteurs du gaz et de l'électricité

¹⁷³ I. Hasquenoph, « *Commande publique et protection des données personnelles* », AJDA, 2021, p. 2339

¹⁷⁴ *Ibid.*

¹⁷⁵ Recommandation du Conseil concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, 23 sept. 1980, pt 14.

¹⁷⁶ B. Du Marais, V. « *Compliance* », in Dictionnaire des régulations, LexisNexis, 2016, p. 191.

¹⁷⁷ L. Paillet, « *Le paradoxe de la compliance dans le droit de la protection des données* », Cahiers de droit de l'entreprise n° 1, Janvier-Février 2025, dossier 8

« documenter chacune de ces mesures »¹⁷⁸. L'objectif est simple : faire du responsable du traitement, l'acteur principal de la protection des données, en lui laissant le soin d'évaluer les risques et d'adopter des mesures destinées à les réduire, le tout sous supervision de la CNIL – qui a vu, nous l'avons déjà évoqué, ses pouvoirs de contrôle et de sanction renforcés par l'entrée en application du RGPD.

On retrouve ici la logique de *compliance*¹⁷⁹ venue des États-Unis et pouvant être définie comme « un système de politiques et de contrôles que les organisations adoptent pour prévenir les violations de la loi et pour garantir aux autorités extérieures qu'elles prennent des mesures pour prévenir les violations de la loi »¹⁸⁰.

Elle fait de chaque administration « le gendarme d'elle-même »¹⁸¹. En pratique, elle devra se devra tenir un registre des traitements, intégrer tout en amont du traitement les principes de protection des données dès la conception (*privacy by conception*) et par défaut (*privacy by default*), désigner un délégué à la protection des données personnelles (DPO / DPD), élaborer une analyse d'impact relative à la protection des données (AIPD) chaque fois qu'un traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées.

Ce nouveau paradigme conduit – en partie – à un recul de la « *conception volontariste du contrat* »¹⁸². En effet, il a conduit à un renouvellement du rôle de la CNIL, laquelle s'est muée en un véritable régulateur en la matière, n'hésitant pas à s'immiscer dans « *l'œuvre des parties* »¹⁸³, en les conduisant à réécrire leur contrat pour garantir sa conformité au RGPD.

RGPD et commande publique reposent donc sur des logiques parfois antagonistes. Cette nouvelle logique de responsabilisation – et, partant, de *compliance* – porte en elle un « *paradoxe* » qui en limite intrinsèquement l'efficacité : celui de confier à « *l'auteur d'une ingérence lucrative la charge d'y remédier* »¹⁸⁴.

L'honnêteté intellectuelle nous pousse cependant à nuancer le propos sur un point. Outre la protection des données personnelles, il ne faut pas oublier que le RGPD a également pour

¹⁷⁸ *Ibid.*

¹⁷⁹ Terme anglo-saxon signifiant littéralement « *la conformité* ».

¹⁸⁰ M. Baer, « *Governing Corporate Compliance* », B. C. L. Rev., vol. 50, 2009, pp. 949-1019, not. p. 958

¹⁸¹ J.-J. Daigre, *Compliance entreprise et Europe*, in M.-A Frison-Roche, *Pour une Europe de la compliance*, préc., p. 61

¹⁸² I. Hasquenoph, « *Commande publique et protection des données personnelles* », AJDA, 2021, p. 2339

¹⁸³ *Ibid.*

¹⁸⁴ L. Pailler, « *Le paradoxe de la compliance dans le droit de la protection des données* », Cahiers de droit de l'entreprise n° 1, Janvier-Février 2025, dossier 8

objectif principal d'en permettre la « *libre circulation* ». Il ne s'avère donc pas, totalement, opposé à la logique économique qui irrigue la commande publique.

Reste que ces tensions se trouvent renforcées par le déséquilibre structurel qui oppose transparence de la commande publique et confidentialité des données personnelles du RGPD.

II – Le déséquilibre structurel entre transparence de la commande publique et confidentialité des données personnelles

Le respect du RGPD s'avère être une limite à l'ouverture des données publiques, et au cas particulier, à celle des données essentielles des contrats de la commande publique (A). Cette confrontation trouve sa traduction la plus révélatrice dans l'étude approfondie de la place accordée aux différents secrets par le droit de la commande publique, laquelle révèle l'existence d'une hiérarchie implicite (B).

A – Le respect du RGPD comme limite à l'ouverture des données publiques

Depuis les années 1990, les pouvoirs publics ont entrepris un large mouvement en faveur de l'ouverture des données publiques (*Open data*). Cette politique d'ouverture est aujourd'hui consacrée par les dispositions du livre III du CRPA qui consacre un droit d'accès et de réutilisation des informations publiques¹⁸⁵.

La publication facultative constitue le premier volet de ce dispositif ; l'administration dispose de la faculté de rendre publics les documents administratifs « *qu'elle produit ou reçoit* »¹⁸⁶. Cette publication s'inscrit dans le prolongement du droit d'accès individuel, tout demandeur pouvant solliciter la mise en ligne d'un document communicable¹⁸⁷.

Cette possibilité est complétée par l'obligation pour les administrations employant plus de cinquante agents en équivalent temps plein – à l'exclusion des collectivités de moins de 3 500 habitants – de mettre en ligne¹⁸⁸ : les documents communiqués en application du CRPA et leurs versions actualisées ; les documents figurant dans le répertoire des informations publiques ; les bases de données régulièrement mises à jour qu'elles produisent ou reçoivent ; les données présentant un intérêt économique, social, sanitaire ou environnemental, ainsi que

¹⁸⁵ L. Cluzel-Métayer, La loi pour une République numérique : l'écosystème de la donnée saisi par le droit : AJDA 2017, p. 340

¹⁸⁶ Article L. 312-1 du Code des relations entre le public et l'Administration.

¹⁸⁷ Article L. 311-9 du Code des relations entre le public et l'Administration.

¹⁸⁸ Article L. 312-1-1 du Code des relations entre le public et l'Administration.

les règles définissant les principaux traitements algorithmiques fondant des décisions individuelles¹⁸⁹.

A ce cadre général viennent s'ajouter des dispositions sectorielles diverses et variées. Nous concernant, l'obligation pour les acheteurs¹⁹⁰ et les autorités concédantes¹⁹¹ de publier sur le portail national des données ouvertes, dans un format ouvert et librement réutilisable les « *données essentielles* » des contrats de la commande publique.

Sur ce point, nous l'avons vu, le droit de la commande publique – dispositions combinées du CCP et des CCAG – facilite la satisfaction des obligations liées à *l'Open data*.

A l'origine, l'ancien article 133 du Code des marchés publics (2006) prévoyait que l'acheteur devait publier la liste des marchés conclus l'année précédente. Le dispositif – encore embryonnaire – avait pour objectif d'assurer la transparence dans l'emploi des deniers publics. Lacunaire sur bien des points, il fut renforcé à l'occasion de la transposition¹⁹² des directives européennes.

Cette exigence d'ouverture des données répond aujourd'hui à des objectifs allant au-delà de la simple transparence : « *prévention et la lutte contre la corruption, la bonne gestion des deniers publics, le pilotage des politiques d'achat et le développement économique des entreprises (...)* »¹⁹³. Une nouvelle fois, ce sont bien les fondements économiques sous-jacents au droit de la commande publique qui justifient la « transparence ».

Pour créer un « *écosystème des données de la commande publique* »¹⁹⁴, il est apparu nécessaire de standardiser leurs formats pour faciliter leur exploitabilité et leur réutilisation. Ainsi, le Code précise expressément que les données essentielles portent sur la procédure de passation du contrat, son contenu et son exécution (le cas échéant, sa modification). Dans un souci d'harmonisation, l'arrêté du 22 mars 2019¹⁹⁵, repris à l'annexe 15 du Code de la commande publique, vient énumérer la liste de ces « *données essentielles* » et précise les modalités de leur mise à disposition.

¹⁸⁹ Article L. 312-1-3 du Code des relations entre le public et l'Administration.

¹⁹⁰ Articles L. 2196-2 et R. 2196-2 du Code de la commande publique ; l'obligation de publication est circonscrite aux marchés dont la valeur est supérieure ou égale à 40 000 euros hors taxes.

¹⁹¹ Articles L. 3131-1 et R. 3131-1 du Code de la commande publique.

¹⁹² Décret n° 2022-767 du 2 mai 2022 portant diverses modifications du Code de la commande publique.

¹⁹³ DAJ, La publication des données essentielles de la commande publique, Fiche pratique, juill. 2023, p. 2

¹⁹⁴ DAJ Bercy, « La publication des données essentielles de la commande publique », juin 2024, p.1

¹⁹⁵ Arrêté du 22 mars 2019 relatif aux données essentielles dans la commande publique.

On y retrouve, pêle mêle, une liste de 15 informations différentes (et 7 supplémentaires en cas de modifications) pour les marchés publics ; et de 16 informations différentes (auxquelles s'ajoutent 3 informations devant être publiées tous les ans, et 5 informations en cas de modifications) pour les contrats de concessions.

Pour l'essentiel, leur mise en ligne devra intervenir dans les deux mois¹⁹⁶ suivant la notification du marché ; avant le début de leur exécution pour les concessions. Elles devront être maintenues disponibles pendant une durée minimale de cinq ans après la fin de l'exécution du contrat ; la durée pouvant être réduite à un an si les données sont publiées sur le portail unique interministériel (data.gouv.fr)¹⁹⁷. Le format de la mise à disposition devra respecter les formats (*XLM* ou *JSON*), normes et nomenclatures des référentiels des données de la commande publique¹⁹⁸ ; les acheteurs pouvant faire le choix de mettre à disposition ces données sous une licence de réutilisation qu'ils déterminent dans le respect des dispositions du CRPA¹⁹⁹.

Certaines de ces données peuvent revêtir un caractère personnel. Pour n'en citer que quelques exemples : le nom du titulaire du marché ou du concessionnaire ; son numéro d'inscription au répertoire des entreprises et de leurs établissements, etc. Compte tenu des définitions extensives du RGPD, les acheteurs se doivent de faire preuve d'une vigilance particulière dans l'identification des données à caractère personnel.

En la matière, puisque la diffusion en ligne de documents contenant des données à caractère personnel constitue un « *traitement* » au sens de l'article 4 du RGPD, toutes les obligations qui en découlent sont applicables. Si les noms / prénoms des cocontractants sont communicables²⁰⁰, certaines informations portent atteinte au secret de la vie privée²⁰¹ : l'âge ou l'adresse d'une personne physique, les *curriculum vitae*, les coordonnées ou les attestations bancaires produites dans les dossiers de candidatures²⁰² ; les déclarations de revenus, les salaires respectifs des employés de l'entreprise²⁰³ ; etc.

¹⁹⁶ Article 6, arrêté préc.

¹⁹⁷ Article 7, arrêté préc.

¹⁹⁸ Article 9, arrêté préc.

¹⁹⁹ Article 10, arrêté préc.

²⁰⁰ D'une part, une disposition législative l'autorise (l'impose, même) expressément. D'autre part, la jurisprudence le confirme (CE Sect., 30 mars 1990, Mme Degorge Boëtte, n° 90237)

²⁰¹ V. DAJ Bercy et CADA, « La communication des documents administratifs en matière de commande publique », 1^{er} avril 2019.

²⁰² CADA, avis n° 20033429 du 28 août 2003 et conseil n° 20031928 du 15 mai 2003.

²⁰³ CADA, conseil n° 20004574 du 7 décembre 2000.

En conséquence, le principe est l'anonymisation²⁰⁴ des documents contenant de telles données avant leur publication, sauf exceptions strictement encadrées. L'équilibre peut sembler difficile à trouver pour les personnes publiques qui devront construire une anonymisation, au cas par cas, reposant sur trois critères cumulatifs²⁰⁵ : « *l'individualisation* » (il doit être impossible d'isoler un individu), « *la corrélation* » (impossible de relier des ensembles de données concernant un même individu) et « *l'inférence* » (impossible de déduire des informations sur un individu).

En toute hypothèse, cette publication s'entend naturellement sous réserve de ne pas publier les informations dont la divulgation serait contraire à l'ordre public ou porterait atteinte à un secret protégé par la loi. En pratique, l'étude approfondie de la place accordée à ces différentes limites par le droit de la commande publique révèle l'existence d'une « hiérarchie » des secrets.

B – L'existence implicite d'une hiérarchie des secrets en droit de la commande publique

A y regarder de plus près, le droit de la commande publique « *révèle par certains aspects son indifférence à l'égard de la protection des données personnelles* »²⁰⁶. Le constat est prégnant lorsqu'on examine respectivement la protection accordée aux différents secrets par le droit de la commande publique.

D'une part, le CRPA fait apparaître un premier niveau de hiérarchie en distinguant les secrets absolus, des secrets relatifs. Les deux constituent des limites à la communication des documents administratifs (et par extension, à leur publication dans le respect des obligations applicables à *l'Open data*). Ils n'ont cependant pas la même portée.

Ainsi, les secrets absolus sont opposables à l'égard de tous et découlent, pour la plupart, de la préservation des intérêts publics. Ils sont listés à l'article L. 311-5 du CRPA. On y retrouve ainsi, notamment, le « *secret des délibérations du Gouvernement et des autorités responsables relevant du pouvoir exécutif* », le « *secret de la défense nationale* », de « *la conduite de la politique extérieure de la France* », de « *la sûreté de l'Etat* », des « *autres secrets protégés par la loi* »²⁰⁷. A titre illustratif, en matière de commande publique, il a été retenu que la communication des éléments relatifs à une offre retenue dans le cadre d'un concours de

²⁰⁴ Articles L. 311-5 et L. 311-6 du Code des relations entre le public et l'Administration.

²⁰⁵ CNIL, Guide pratique de la publication en ligne et de la réutilisation des données publiques (« Open data »).

²⁰⁶ I. Hasquenoph, « *Commande publique et protection des données personnelles* », AJDA, 2021, p. 2339

²⁰⁷ Lecture combinée des articles L. 312-1-2 al. 1 ; L. 311-5 et L. 311-6 du Code des relations entre le public et l'Administration.

maîtrise d'œuvre pour la construction d'un hôtel de police porte atteinte à la sécurité publique²⁰⁸.

Quant à eux, les secrets relatifs ne sont opposables qu'aux tiers et sont énumérés à l'article L. 311-6 du même Code. Ne sont ainsi communicables qu'à l'intéressé, les documents « *dont la communication porterait atteinte à la protection de la vie privée, au secret médical et au secret des affaires, lequel comprend le secret des procédés, des informations économiques et financières et des stratégies commerciales ou industrielle (...)* » ; ceux « *portant une appréciation ou un jugement de valeur sur une personne physique, nommément désignée ou facilement identifiable* » ; ceux « *faisant apparaître le comportement d'une personne, dès lors que la divulgation de ce comportement pourrait lui porter préjudice* ».

D'autre part, l'étude détaillée de ces secrets « relatifs » fait apparaître un second niveau de hiérarchie, opéré, cette fois, implicitement par le Code de la commande publique. Celui-ci met à la charge de l'autorité contractante une obligation de confidentialité²⁰⁹ lui interdisant de communiquer les informations confidentielles dont elle a eu connaissance lors de la procédure de passation, « *telles que celles dont la divulgation violerait le secret des affaires, ou celles dont la communication pourrait nuire à une concurrence loyale entre les opérateurs économiques* »²¹⁰. Ici, « *seul le secret des affaires est mentionné ; nulle trace du secret de la vie privée* »²¹¹.

Par souci d'honnêteté, il nous faut toutefois nuancer quelque peu le propos. La mention du secret des affaires en tant qu'information confidentielle est précédé de la formule « *telles que* », de sorte qu'il est possible de considérer la liste d'exemples comme non-exhaustive. Il n'y a cependant, à notre connaissance, aucun exemple contentieux susceptible d'étayer cet argument²¹². En réalité, ce « *déséquilibre s'explique sans doute par les fondements économiques du droit de la commande publique* »²¹³.

Le texte précise expressément que cette obligation de confidentialité s'oppose à la communication du montant total / du prix détaillé des offres (de la valeur globale, pour les

²⁰⁸ CADA, conseil n° 20073859 du 11 octobre 2007.

²⁰⁹ V. Articles L. 2132-1, L. 2332-1 et L. 3122-3 du Code de la commande publique.

²¹⁰ Article L2332-1 du Code de la commande publique.

²¹¹ I. Hasquenoph, « *Commande publique et protection des données personnelles* », AJDA, 2021, p. 2339

²¹² Voir néanmoins : CJUE, 17 nov. 2022, aff. C-54/21, Antea Polska SA : sous certaines conditions, des informations nominatives permettant d'identifier des personnes ainsi que les informations relatives à la conception des projets objet du marché et de la description de ses modalités d'exécution s'ils ont une valeur commerciale.

²¹³ Ibid ; V. également : A. Sanchez-Graells, *Public Procurement and the EU Competition Rules*, Hart Publishing, 2015

concessions), et donc à la communication du bordereau des prix unitaires unitaire (BPU) de l'entreprise attributaire aux concurrents évincés²¹⁴.

Elle justifie également que les exigences de la contradiction soient « *adaptées à celles de la protection du secret des affaires* »²¹⁵. Les répercussions en cas de méconnaissance de cette obligation peuvent être lourdes ; elle constitue un manquement de nature à justifier l'annulation de la procédure de passation du marché par le juge du référé précontractuel²¹⁶.

Rappelons, pour terminer – et parachever notre raisonnement sur la place prééminente des intérêts économiques dans le droit de la commande publique – que la loi du 30 juillet 2018 relative à la protection du secret des affaires a conduit à l'introduction d'un référé secret des affaires permettant au juge, lorsqu'il est saisi aux fins de prévenir une atteinte imminente ou faire cesser une atteinte illicite à un secret des affaires, de prescrire toute mesure provisoire et conservatoire proportionnée, y compris sous astreinte.

Tous ces arguments permettent d'entériner le fait que les fondements économiques du droit de la commande publique constituent, dans leur immense majorité, une limite structurelle à la protection des données à caractère personnel.

Au demeurant, à cette limite vient s'ajouter l'enjeu complexe et négligé du sort des données au terme du contrat.

Section II - L'enjeu complexe et négligé du sort des données personnelles au terme du contrat

A l'ère du *Big Data*, les données numériques représentent « *l'or noir du XXIe siècle* »²¹⁷. Elles sont ce que « *furent l'électricité ou les chemins de fer pour les siècles précédents* », elles « *irriguent l'ensemble des secteurs de la société, sont garants de sa cohésion, sont vitaux pour son industrie, ses services et son administration* »²¹⁸.

Dès lors, le sort des données – qu'elles soient personnelles ou non – bien que souvent négligé par les parties au contrat, revêt un intérêt majeur. Cette problématique met en lumière

²¹⁴ CE 12 juin 2019, n° 427397, ministre des Armées.

²¹⁵ Article L. 611-1 du Code de justice administrative.

²¹⁶ CAA Paris, 20 mars 2012, Caisse nationale d'assurance vieillesse travailleurs salariés (CNAVTS).

²¹⁷ 3. M. Fontaine et S. Juillet, « La donnée numérique : l'or noir du xxi siècle ? », LPA 8 sept. 2017, n° 179-180, p. 90.

²¹⁸ La société et l'économie à l'aune de la révolution numérique - Enjeux et perspectives des prochaines décennies (2015-2025), Rapport de la commission présidée par A. Bravo, Centre d'analyse stratégiques, Doc. fr., 2009, quatrième de couverture.

l'épineuse question de la propriété des données, dont l'absence de reconnaissance juridique claire crée de nombreuses zones d'incertitude (I). Transposée au champ spécifique de la commande publique, cette interrogation révèle un traitement différencié du sort des données selon le type de contrat concerné (II).

I – L'épineuse question de la propriété des données

La question de la propriété des données brutes fait l'objet « *d'après discussions* »²¹⁹. Bien que l'état du droit témoigne de l'absence avérée de droit de propriété sur les données personnelles (A), les bases de données peuvent, sous conditions, être protégées au titre de la propriété intellectuelle (B).

A – L'absence avérée de droit de propriété sur les données personnelles

Depuis de nombreuses années déjà, la question de la propriété des données a fait l'objet de nombreuses controverses. Pour tenter d'apporter une réponse appropriée à cette épineuse question, la doctrine s'est d'abord interrogée – en profondeur – sur les conditions préalables à la reconnaissance d'un tel droit sur des données brutes non personnelles. Pour ne citer que les principaux : la donnée peut-elle être qualifiée de « *chose* »²²⁰ ? De « *chose appropriable* »²²¹ ? De « *chose hors du commerce* »²²² ? Ou encore de « *chose commune* »²²³ ?

Ces vastes travaux doctrinaux tendent à démontrer la complexité de la reconnaissance d'un droit de propriété sur les données. En la matière, plusieurs courants s'opposent : les défenseurs de la théorie des communs s'opposent à l'application de la notion de propriété aux données ; d'autres estiment que la notion de propriété n'est « *techniquement* »²²⁴ pas applicable aux données ; tandis que certains plaident malgré tout pour la reconnaissance d'un tel droit²²⁵.

Bien que les positions divergent, celle du droit français est claire : les données brutes n'ont aucun caractère appropriable ; prises isolément, elles sont « *rétives à toute forme de propriété*,

²¹⁹ J-B Auby, *JurisClasseur Administratif*, Fasc. 109-20, « *Orientations du droit des données publiques* ».

²²⁰ Th. Saint-Aubin, *Les nouveaux enjeux juridiques des données (big data, web sémantique et linked data)*, *Les droits de l'opérateur de données sur son patrimoine numérique informationnel* : RLDI 2014, n° 102.

²²¹ J. Rochfeld, *Contre l'hypothèse de la qualification des données personnelles comme des biens*, in E. Netter et A. Chaigneau, *Les biens numériques* : Paris, PUF, coll. CEPRISCA, 2015, p. 221-236.

²²² A. Basdevant et J.-P. Mignard, *L'empire des données, Essai sur la société, les algorithmes et la loi* : Don Quichotte, 2018, p. 127

²²³ D. Bourcier et P. de Filippi, *Vers un droit collectif sur les données de santé* : RDSS 2018, p. 444

²²⁴ J.-M. Bruguière, *Les données publiques et le droit* : Litec, 2002, p. 55

²²⁵ C. Rees, *Who Owns Our Data ?*, août 2013

fût-ce une propriété intellectuelle »²²⁶, ce dernier ne protégeant pas les « *idées exprimées mais seulement la forme originale sous laquelle elles le sont* »²²⁷.

Aussi, ce débat sur la propriété des données trouve naturellement son pendant au sujet du droit de propriété sur les données personnelles. Il nous faut toutefois préciser que le droit français s'oppose également à cette conception, privilégiant une conception extrapatrimoniale de la donnée dont la protection repose sur le respect des libertés fondamentales²²⁸. Cette vision, « *personnaliste* »²²⁹, reconnaît des droits « *à l'individu mais ne protège pas la donnée personnelle en tant qu'objet économique* »²³⁰.

Quelques rappels s'imposent ; à la différence des droits patrimoniaux attachés à des choses (*in rem*), et des droits personnels (*in personam*) attachés à des individus et n'opposables qu'à eux, le droit à la protection de la vie privée appartient à la catégorie des droits extra-patrimoniaux. Les données sont dépourvues de toute consistance matérielle, elles ne sont pas associées à une chose et sont opposables à tous. Étant inhérents à la personne humaine, elles ne peuvent en être dissociées et sont inaliénables.

Rappelons également que, de son côté, le droit de propriété se forme de trois composantes distinctes : *l'usus*, qui correspond au droit d'utiliser une chose ; *le fructus*, qui est le droit de disposer des fruits d'une chose ; enfin, *l'abusus* correspond au droit de disposer d'une chose, notamment en l'aliénant ou en la détruisant.

En pratique, l'étude des données personnelles révèle qu'elles permettent à la personne concernée de bénéficier d'une sorte d'usufruit. Ils n'en sont cependant pas propriétaires « *car ils ne peuvent en disposer librement* »²³¹. Ce principe d'indisponibilité des données personnelles a d'ailleurs été reconnu par le Conseil d'État qui précise que « *s'il convient de renforcer la dimension de l'individu acteur dans le droit à la protection des données, c'est en envisageant celui-ci comme un droit à l'autodétermination plutôt que comme un droit de*

²²⁶ T. Bassi, « *Les données collectées par le concessionnaire de service public* », AJDA, 2019, p.496

²²⁷ Civ. 1re, 8 nov. 1983, n° 82-13.547, Bull. civ. I, n° 260 ; Civ. 1re, 25 mai 1992, n° 90-19.460, Bull. civ. I, n° 161 ; Civ. 2e, 30 janv. 2014, n° 12-24.145, Bull. civ. II, n° 26

²²⁸ T. Saint-Aubin, Les nouveaux enjeux juridiques des données (big data, web sémantique et linked data), Les droits de l'opérateur de données sur son patrimoine numérique informationnel : RLDI 2014, n° 102, pt I

²²⁹ N. Ochoa, « *Pour en finir avec l'idée d'un droit de propriété sur ses données personnelles : ce que cache véritablement le principe de libre disposition* », RFDA 2015 p.1157.

²³⁰ Belot, Doc. AN, Rapp. n° 3399, au nom de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République sur le projet de loi (n° 3318) pour une République numérique, 15 janv. 2016, p. 456

²³¹ D. Bourcier et P. de Filippi, Vers un droit collectif sur les données de santé : RDSS 2018, p. 444

propriété »²³². Le droit sur la protection des données personnelles « *ne repose pas sur une logique patrimoniale mais sur une logique de droits attachés à la personne* »²³³. Il en ressort que les données ne sont pas une « *ressource dont les individus sont propriétaires, mais uniquement une extension de leur personnalité, dont ils ont le droit de contrôler l'usage et l'exploitation* »²³⁴.

Quoi qu'il en soit, la question réapparaît régulièrement²³⁵ et l'argument phare de ses défenseurs consiste à souligner la valeur économique des données : conférer un droit de propriété à la personne concernée lui permettrait de « *monétiser l'usage* »²³⁶ de ses données personnelles. Une telle approche rendrait les individus attentifs à la gestion faite de leurs données, « *et plus motivés à s'opposer à une utilisation non-autorisée* »²³⁷ ; de la même façon que les titulaires des droits d'auteur se préoccupent des usages qui sont faits de leurs droits de propriété intellectuelle.

Pour autant, cet argument s'expose à plusieurs critiques. La première est que « valeur économique », « bien » et « propriété » sont souvent assimilés sans que le passage de l'un à l'autre soit démontré²³⁸. Dans le même sens, s'il n'est pas contesté que les données ont effectivement une valeur économique, celle-ci découle, en pratique, de leur agrégation, de sorte que « *les données de Mme Martin ou de M. Dupont n'intéressent pas grand monde. En revanche, lorsqu'elles sont corrélées avec des milliers d'autres informations, numérisées, commentées, elles sont susceptibles de présenter une valeur tout autre* »²³⁹.

En réalité, cette proposition – fausse bonne idée²⁴⁰ selon la CNIL – est « *beaucoup moins porté par les juristes que suscité par des lobbyistes afin d'assouplir radicalement les réglementations françaises et européennes en matière de traitement de données*

²³² Les rapports du Conseil d'État (ancienne collection Étude et documents du Conseil d'État), Le numérique et les droits fondamentaux, 2014, p. 263.

²³³ V. Les rapports du Conseil d'État (ancienne collection Étude et documents du Conseil d'État), Le numérique et les droits fondamentaux, 2014, p. 263.

²³⁴ D. Bourcier et P. de Filippi, Vers un droit collectif sur les données de santé : RDSS 2018, p. 444

²³⁵ Voir notamment : Y. Pouillet, La « propriété » des données : balade au « pays des merveilles à l'heure du big data », in Penser le droit de la pensée, Mélanges en l'honneur de Michel Vivant, Dalloz, 2020, p. 338 ; pour une justification économique de l'absence de droit de propriété sur les données personnelles : A. Anciaux et J. Farchy, L'instauration de droits de propriété sur les données personnelles, une légitimité économique contestable, Rev. éco. ind. 2017, n° 158, p. 9

²³⁶ N. Ochoa, « Pour en finir avec l'idée d'un droit de propriété sur ses données personnelles : ce que cache véritablement le principe de libre disposition », RFDA 2015 p.1157.

²³⁷ L. Lessig, Privacy as property, Social Research: An International Quarterly, 69, 2002. P. 257.

²³⁸ *Ibid.*

²³⁹ J-M Bruguière, L'émergence d'un droit des données, 2023, p. 9

²⁴⁰ CNIL, Vie privée à l'horizon 2020. Paroles d'experts, Cahiers IP Innovation et prospective, n° 1.

personnelles »²⁴¹ ; l'analyse révèle en effet qu'un tel droit ne bénéficierait pas tant aux personnes concernées qu'aux « courtiers en données » (appelés *databrokers*) « très investis dans les débats et qui ont, à n'en pas douter, un avantage économique à voir reconnaître un tel droit de propriété »²⁴².

Il est néanmoins possible de revendiquer des droits de propriété intellectuelle lorsque ces données sont présentées sous la forme d'une « base de données ».

B – La reconnaissance d'un droit de propriété des « bases de données »

Si les données « brutes » sont, en elles-mêmes, inappropriables, les bases de données (et les fichiers) constituent des biens meubles immatériels²⁴³ appropriables. L'identification – et l'appréhension – juridique de la base de données est relativement ancienne.

A l'occasion de l'affaire *Microfor*²⁴⁴, la jurisprudence fit le premier pas vers sa protection au titre du droit d'auteur en qualifiant, l'index de la presse écrite française, « *d'œuvre d'information* ». Une protection lui fut ensuite accordée à la suite de plusieurs conventions internationales²⁴⁵, avant que le droit communautaire ne lui confère une assise dans la directive du 11 mars 1996²⁴⁶.

Celle-ci sera transposée en France au sein du Code de la propriété intellectuelle par la loi n° 98-536 du 1^{er} juillet 1998. Elle confirmera la possible application du droit d'auteur à la base de données et reconnaitra un droit *sui generis* au producteur de bases de données. A l'instar du RGPD, la directive opte pour le principe de neutralité technologique²⁴⁷ ; il en ressort que la notion s'applique également bases non électroniques (par exemple, pour un catalogue d'exposition papier).

La base de données fait aujourd'hui l'objet d'une définition à l'article L. 112-3 du Code de la propriété intellectuelle. Elle y est envisagée comme « *un recueil d'œuvres, de données ou*

²⁴¹ N. Ochoa, « Pour en finir avec l'idée d'un droit de propriété sur ses données personnelles : ce que cache véritablement le principe de libre disposition », RFDA 2015 p.1157

²⁴² Margo Bernelin, « La patrimonialisation des données personnelles : entre représentation(s) et réalité(s) juridiques », La Semaine Juridique Edition Générale n° 46, 11 novembre 2019, doct. 1172

²⁴³ F. Tarlet, Les biens publics mobiliers, Dalloz, Nouv. bibl. de thèses, 2017

²⁴⁴ Cass. Ire civ., 9 nov. 1983 : JurisData n° 1983-702217.

²⁴⁵ Accord ADPIC, 15 avr. 1994, art. 10, [sect] 2 ; Traité de l'OMPI, 20 déc. 1996, art. 5, sur le droit d'auteur

²⁴⁶ Directive 96/9/CE du Parlement européen et du Conseil, du 11 mars 1996, concernant la protection juridique des bases de données

²⁴⁷ V. Gautrais, Neutralité technologique : rédaction et interprétation des lois face aux changements technologiques : Thémis, 2012

d'autres éléments indépendants, disposés de manière systématique ou méthodique, et individuellement accessibles par des moyens électroniques ou par tout autre moyen ».

En résumé, elles peuvent être protégées par deux droits de propriété intellectuelle. D'une part, elles peuvent être l'objet d'un droit d'auteur²⁴⁸ lorsque la base de données comporte une originalité révélatrice d'une création intellectuelle propre à l'auteur (que celle-ci soit d'ordre structurel ou méthodique). Cette hypothèse s'avère toutefois relativement rare en matière de base de données « publiques ». Ce droit permet à son auteur d'exercer « *des attributs d'ordre intellectuel et moral* (droit de divulgation, paternité de l'œuvre, droit de retrait et de repentir) *ainsi que des attributs d'ordre patrimonial* (exploitation de l'œuvre par sa représentation ou sa reproduction) »²⁴⁹.

D'autre part, elles peuvent être l'objet du droit *sui generis* reconnu aux producteurs de bases de données²⁵⁰ à la condition d'établir la réalité d'un « *investissement substantiel apprécié de manière quantitative et/ ou qualitative, soit dans l'obtention, soit dans la constitution, soit dans la vérification, soit dans la présentation du contenu de la base* »²⁵¹. Le droit reconnu est alors distinct du droit d'auteur susmentionné. Il permet cependant à son titulaire de s'opposer à « *tout acte non autorisé d'appropriation et de diffusion au public* »²⁵² d'une partie substantielle de la base de données²⁵³ ou d'une partie non substantielle « *lorsque ces opérations excèdent manifestement les conditions d'utilisation normale* »²⁵⁴.

En pratique, en l'absence de décision de justice, le producteur n'est pas garanti d'être titulaire du droit *sui generis* reconnu aux producteurs. Ainsi, la conclusion d'un contrat – de la commande publique, notamment – peut avoir pour objectif de consolider la protection juridique de la base de données ; encore faut-il que la répartition des droits de propriété intellectuelle fasse l'objet de stipulations contractuelles claires.

Reste que l'article 15 de la directive 96/9/CE vient interdire certaines dispositions contractuelles, notamment, celles ayant pour objet de restreindre l'accès à son contenu²⁵⁵ et celles empêchant d'en extraire / d'en réutiliser des parties non substantielles²⁵⁶. Ces

²⁴⁸ Article L. 112-3 du Code de la propriété intellectuelle ; Voir par exemple : Civ. 1re, 20 janv. 2004, n° 00-19.577 et Civ. 1re, 22 sept. 2011, n° 10-23.073.

²⁴⁹ Article L. 111-1 du Code de la propriété intellectuelle.

²⁵⁰ Article L. 341-1 du Code de la propriété intellectuelle.

²⁵¹ Code de la propriété intellectuelle, 2025, p.566

²⁵² CJCE 9 nov. 2004, aff. C-203/02, RTD com. 2005. 90, obs. F. Pollaud-Dulian.

²⁵³ Article L. 342-1 du Code de la propriété intellectuelle.

²⁵⁴ Article L. 342-2 du Code de la propriété intellectuelle.

²⁵⁵ V. art. 6, sect 1.

²⁵⁶ V. art. 8, sect 1.

restrictions à la liberté contractuelle des parties ne sont pas sans difficultés pratiques et contraignent les producteurs à « *apprécier en amont l'existence potentielle d'un droit pour définir les stipulations contractuelles* »²⁵⁷ qu'ils peuvent prévoir.

Pouvant faire l'objet d'un « contrat », le sort des données doit nécessairement être examiné au prisme du droit de la commande publique.

II – Le sort différencié des données au terme de l'exécution du contrat

Comme nous l'avons constaté, les opérateurs économiques et les acheteurs publics sont fréquemment tentés de régir le statut juridique des bases de données – et *in extenso* des données qu'elles contiennent – par le biais des clauses de leurs contrats. Toutefois, cette approche se heurte à une difficulté : les données constituent des biens immatériels non rivaux dont la nature particulière résiste aux catégories traditionnelles du droit administratif des biens. Les concepts classiques que sont l'affectation, l'appropriation ou encore l'utilisation privative lui paraissent difficilement applicables.

Dès lors, le contrat doit organiser la répartition des droits sur les données et bases de données entre les parties, tant pendant l'exécution du contrat que postérieurement à celle-ci. Il convient d'y insérer des clauses spécifiques destinées à assurer la continuité de l'action publique et à favoriser l'ouverture des données publiques (*Open data*) tout en prévenant les risques liés à la diffusion d'informations couvertes par le secret, qu'il soit relatif à la vie privée, ou encore aux affaires (*v. supra*).

L'étude du sort des données au terme de l'exécution du contrat révèle des éléments de réponse différenciés selon le type de contrat envisagé. Alors que les CCAG mettent en place un cadre structuré autour des connaissances « antérieures » et des « résultats » du marché (A), celui mis en œuvre dans le cadre des contrats de concession est fondé sur la théorie des biens de retour et se heurte parfois au principe de continuité du service public (B).

A – Le cadre structuré des CCAG, entre « connaissances antérieures » et « résultats »

Il est traditionnellement admis que les personnes publiques puissent détenir des droits de propriété intellectuelle²⁵⁸ – nous concernant – que ce soit en qualité d'auteur²⁵⁹ ou de producteur d'une base de données. Dans les marchés publics, la question de la répartition des

²⁵⁷ S. Chatry, Fasc. 1650 : DROITS DES PRODUCTEURS DES BASES DE DONNÉES. – (CPI, art. L. 112-3 et L. 341-1 à L. 343-7 et CRPA, art. L. 321-3)

²⁵⁸ CE 23 mars 1960, n° 46221, Société Spiesshofer et Braun, Lebon 215

²⁵⁹ CE 10 juill. 1996, n° 168702, Société Direct Mail Promotion, Lebon 277

droits et obligations relatives aux données et aux bases de données est opérée dans les CCAG²⁶⁰. Ceux-ci organisent la répartition des droits en distinguant les « connaissances antérieures » et les « résultats » du marché.

Ainsi, « les connaissances antérieures désignent tous les éléments, quels qu'en soient la forme, la nature et le support, qui sont incorporés aux résultats et/ou sont fournis pour répondre aux besoins de l'acheteur dans le cadre d'une prestation intellectuelle et qui appartiennent à l'acheteur, au titulaire ou à des tiers, ou qui leurs sont concédés en licence, mais qui ont été réalisés dans un cadre extérieur et indépendamment du marché, tels que notamment (...) les bases de données, (...) les données et les informations, et plus généralement tous les éléments protégés ou non par des droits de propriété intellectuelle ou par tout autre mode de protection (...) »²⁶¹. En pratique, les connaissances antérieures « standards » viennent s'ajouter à cette catégorie. Il s'agit de connaissances antérieures destinées à être fournies à plusieurs opérateurs pour l'exécution d'une même fonction.

A l'inverse, « les résultats désignent tous les éléments, quels qu'en soient la forme, la nature et le support, qui sont réalisés dans le cadre des prestations du marché, tels que, notamment, (...), les bases de données, les données et les informations, et plus généralement tous les éléments protégés ou non par des droits de propriété intellectuelle ou par tout autre mode de protection (...) »²⁶². Les CCAG ajoutent qu'à « défaut d'identification expresse en tant que connaissance antérieure (dans l'offre ou en cours d'exécution), tout élément livré en exécution du marché est réputé être un résultat »²⁶³.

Outre ces définitions, les CCAG fixent le régime applicable à ces deux éléments. Ainsi, la conclusion d'un marché « n'emporte pas transfert des droits de propriété intellectuelle ou des droits de toute autre nature afférents aux connaissances antérieures »²⁶⁴. Il en ressort que les parties restent titulaires de leurs droits respectifs sur les connaissances antérieures ; le marché n'a pas pour objet, ni pour effet, d'opérer un transfert de ces droits.

²⁶⁰ V. J-F Lafaix « La maîtrise et la protection des données liées aux contrats de la commande publique : approche théorique », JCP A, n° 51-52, 26 décembre 2023, 2396.

²⁶¹ Disposition issue du CCAG TIC, art. 43.2 ; Dispositions similaires : CCAG Travaux, art. 45.2. – CCAG PI, art. 32.2. – CCAG FCS, art. 34.2. – CCAG MI, art. 37.2. – CAG MO, art. 22.6.

²⁶² Issue du CCAG Travaux, art. 45.1. ; Dispositions similaires : CCAG TIC, art. 43.1. – CCAG PI, art. 32.1. – CCAG FCS, art. 34.1. – CCAG MI, art. 37.1. – CCAG MO, art. 22.1.

²⁶³ CCAG Travaux, art. 46. ; CCAG PI, art. 33.2 ; CCAG TIC, art. 44.2 ; CCAG FCS ; CCAG MI, art. 38.

²⁶⁴ CCAG Travaux, art. 46. ; CCAG PI, art. 33.1 ; CCAG TIC, art. 44.1 ; CCAG FCS, art. 35. ; CCAG MI, art. 38. ; CCAG MO, art. 23.1.

A l'inverse, il est expressément précisé que « *le titulaire accorde (...) à l'acheteur, les droits nécessaires pour utiliser ou faire utiliser les résultats, en l'état ou modifiés, de façon permanente ou temporaire, en tout ou partie, par tout moyen et sous toutes formes, pour les besoins et finalités d'utilisation exprimés dans les documents particuliers du marché et en toute hypothèse pour les besoins d'utilisation découlant de l'objet des prestations commandées dans le cadre du marché* »²⁶⁵. Lorsque les résultats sont protégés par un droit de propriété intellectuelle (v. *supra*), les CCAG prévoient que le « *titulaire cède à l'acheteur les droits patrimoniaux des droits d'auteur ou des droits voisins des droits d'auteur* »²⁶⁶.

Par principe, cette cession intervient « *à titre non exclusif afin d'accorder au titulaire le droit d'exploiter les résultats* »²⁶⁷. Par exception, elle peut intervenir à titre exclusif²⁶⁸ lorsque les résultats ont pour « *objet de distinguer l'identité propre de l'acheteur et/ou de ses services* », de « *promouvoir l'acheteur, ses produits et services et plus généralement ses missions de service public* » ou lorsque les résultats sont « *qualifiés de confidentiels* ».

Enfin, les CCAG prévoient une clause spécifique relative aux données indispensables à l'exécution d'une mission de service public. Dans une telle hypothèse, « *le titulaire fournit à l'acheteur sous format électronique, dans un standard ouvert librement réutilisable et exploitable par un système de traitement automatisé, et dans le respect du secret des affaires et des droits de propriété intellectuelle détenus par des tiers, les données et les bases de données collectées ou produites à l'occasion de la gestion du service public faisant l'objet du contrat et qui sont indispensables à son exécution* »²⁶⁹. Les documents particuliers du marché devront toutefois définir les données concernées, le calendrier de transmission ainsi que les éventuelles pénalités de retard en cas de non-respect de celui-ci.

Reste que, pour leur part, les données sont soumises à un régime d'exclusivité : qu'elles soient « *intégrées ou générées, [elles] sont confidentielles et appartiennent exclusivement à l'acheteur* »²⁷⁰. D'un point de vue conceptuel, cette disposition tranche avec le caractère

²⁶⁵ CCAG Travaux, art. 48.1. – CCAG PI, art. 35.1.1. – CCAG TIC, art. 46.1.1. – CCAG FCS, art. 37.1.1. – CCAG MI, art. 40.1.1.

²⁶⁶ CCAG travaux, art. 48.2.1. – CCAG PI, art. 35.2.1. – CCAG TIC, art. 46.2.1. – CCAG FCS, art. 37.2.1. – CCAG MI, art. 40.2.1. – CCAG MO, art. 24.1.

²⁶⁷ *Ibid.*

²⁶⁸ *Ibid.*

²⁶⁹ CCAG PI, art. 26. – CCAG TIC, art. 28. – CCAG FCS, art. 26.

²⁷⁰ CCAG Travaux, art. 48.2.3. – CCAG PI, art. 35.2.3. – CCAG TIC, art. 46.2.3. – CCAG FCS, art. 37.2.3. – CCAG MI, art. 40.2.3.

inappropriables (voir *sus*) des données, ayant d'ailleurs déjà été appliqué aux données publiques²⁷¹.

Rappelons enfin que le RGPD prévoit la possibilité, pour le responsable du traitement, d'imposer au sous-traitant la suppression de « *toutes les données à caractère personnel ou [leur] renvoie (...) au terme de la prestation de services relatifs au traitement, et [la destruction des] copies existantes* »²⁷². Les CCAG se font le relai de cette possibilité en précisant que « *les documents particuliers du marché précisent notamment : (...) la durée et les modalités de conservation des données et le sort de celles-ci au terme de l'exécution du marché* »²⁷³.

Cette liberté contractuelle appelle plusieurs observations critiques. Le sort des données personnelles relève de la négociation entre les parties, qui doivent impérativement définir ces modalités dans les documents particuliers du marché. Cette approche présente l'avantage de la souplesse mais impose une vigilance particulière dans la rédaction du contrat.

Sans prétendre à l'exhaustivité, pour défendre au mieux les intérêts de la personne publique – et par extension ceux des personnes concernées – les documents contractuels devront préciser : les formats de restitution acceptés (formats ouverts, interopérables) ; le caractère gratuit de la restitution ; les délais d'exécution de la restitution et de destruction des copies ; les modalités de certification de la destruction effective des copies ; les pénalités en cas de non-respect des obligations.

Ces qualifications ne sont pas applicables aux concessions dont le régime des biens est fixé – en grande majorité – par les dispositions du Code de la commande publique.

B – Le régime complexe des concessions, entre « biens de retour » et continuité du service public

La qualification des biens entrant dans le champ de la concession ont fait l'objet de longs débats doctrinaux. Reste qu'aujourd'hui, le Conseil d'État a précisé l'ensemble des principes applicables à ces biens dans une décision d'Assemblée²⁷⁴ (classée en A) ; aujourd'hui codifiée à l'article L. 3132-4 du Code de la commande publique.

²⁷¹ V. CA Paris, 18 mars 1993, Société du journal téléphoné, AJDA 1993. 652 ; circ. NOR : PRMG9400081C du 14 févr. 1994 relative à la diffusion des données publiques : « *les données brutes élémentaires, sans mise en forme originale, ne sont en principe la propriété de personne* ».

²⁷² Article 28§3, g) du RGPD.

²⁷³ CCAG, art. 5.2.3.

²⁷⁴ CE, Ass., 21 déc. 2012, n° 342788, Commune de Douai.

A l'époque, de nombreux auteurs se sont prononcés en faveur de l'application de la théorie des biens de retour aux bases de données²⁷⁵. Il est aujourd'hui établi que cette classification s'applique aux biens immatériels présentant une valeur économique²⁷⁶. Rappelons, à ce titre, que les droits dont sont susceptibles de faire l'objet les bases de données sont susceptibles d'appropriation (v. *supra*). Leur statut et leur sort au terme du contrat doit être déterminé contractuellement en tenant compte de la définition et du régime des biens des concessions.

Pour mémoire, les biens de retour sont ceux « *qui résultent d'investissements du concessionnaire et [qui] sont nécessaires²⁷⁷ au fonctionnement du service public (...) dans le silence du contrat, ils sont et demeurent la propriété de la personne publique dès leur réalisation ou leur acquisition* »²⁷⁸. Ces biens ne sont pas librement déterminé par la volonté des parties ; le respect de cette définition étant un moyen d'ordre public²⁷⁹.

Quant à eux, les biens de reprise sont ceux qui « *ne sont pas remis au concessionnaire par l'autorité concédante de droit public et qui ne sont pas indispensables au fonctionnement du service public (...). Ils sont la propriété du concessionnaire, sauf stipulation contraire prévue par le contrat de concession* »²⁸⁰. Autrement dit, ils sont utiles sans être « *indispensables au fonctionnement du service public* »²⁸¹.

Une troisième et dernière catégorie résiduelle peut être formée en rassemblant les biens qui « *ne sont ni des biens de retour, ni des biens de reprise* ». Pour leur part, « *ils sont et demeurent la propriété du concessionnaire* »²⁸².

En pratique, deux principaux cas de figure peuvent être distingué. Dans le premier, les bases de données du concessionnaire ne sont pas nécessaires au fonctionnement du service public. Le concessionnaire peut donc « *se prévaloir assez largement des droits de propriété intellectuelle* »²⁸³ – tant le droit d'auteur ou le droit *sui generis* reconnu au producteur des bases de données ; si les conditions d'octroi sont réunies.

²⁷⁵ J-D Dreyfus, Fichiers, bases de données : quel droit de propriété ? p. 39 ; T. Bassi, « Les données collectées par le concessionnaire de service public », AJDA, 2019, p.496

²⁷⁶ Voir par exemple, CE, 16 mai 2022, n° 459904, Commune de Nîmes pour les « droits d'administration des pages des réseaux sociaux » lorsque la gestion d'un site est concédée.

²⁷⁷ Sur la « nécessité », voir CE, 9 déc. 1898, Compagnie du Gaz de Castelsarrazin.

²⁷⁸ Article L. 3132-4, 1° du Code de la commande publique.

²⁷⁹ CE, 16 mai 2022, n° 459904, Commune de Nîmes.

²⁸⁰ Article L. 3132-4, 2° du Code de la commande publique.

²⁸¹ CE, Ass., 21 déc. 2012, n° 342788, Commune de Douai, préc.

²⁸² Article L. 3132-4, 3° du Code de la commande publique.

²⁸³ T. Bassi, « Les données collectées par le concessionnaire de service public », AJDA, 2019, p.496

Dans le second, pour des considérations relatives à la continuité du service public, le régime applicable est différent ; la base de données étant nécessaire au fonctionnement du service public.

En pratique, en l'absence de dispositions contractuelles dédiées, la seule théorie des biens de retour s'avérait insuffisante pour obtenir la communication des bases de données constituées au cours de l'exécution du contrat ; et pour cause, de nombreux concessionnaires refusaient de les restituer au terme du contrat. Ces difficultés pouvaient nuire à la préparation du prochain contrat, mettant ainsi en péril la continuité du service public « *qui sous-tend la théorie des biens de retour* »²⁸⁴ ; celle-ci ne pouvant « *assurée si le nouveau délégataire doit entièrement reconstituer la base de données sur les usagers* »²⁸⁵.

La loi pour une République numérique²⁸⁶ est ainsi venue ajouter une nouvelle règle – codifiée²⁸⁷ à l'article L. 3132-2 du CPP – au terme de laquelle, lorsque la gestion d'un service public est concédée, « *le concessionnaire fournit à l'autorité concédante, sous format électronique, dans un standard ouvert librement réutilisable et exploitable par un système de traitement automatisé, les données et les bases de données collectées ou produites à l'occasion de l'exploitation du service public faisant l'objet du contrat et qui sont indispensables à son exécution* »²⁸⁸.

Si, de prime abord, ces deux dispositions – L. 3132-2 et L. 3132-4 du CCP – semblent identiques. L'étude approfondie révèle qu'elles n'ont ni « *le même objet, ni le même champ d'application* »²⁸⁹. D'abord, cette disposition s'inscrit dans le cadre de la politique d'ouverture des données publiques (*Open data*) (v. *supra*). Ensuite, si les termes « indispensables » et « nécessaires » doivent être regardés comme synonymes²⁹⁰, les deux dispositions ne doivent pas pour autant sembler ambiguës. En effet, alors que la première vise à s'assurer que les bases de données, en tant que biens de retour, fassent « leur retour » dans le patrimoine de la personne publique en fin de contrat ; la seconde vient renforcer le pouvoir de

²⁸⁴ I. Hasquenoph, « Commande publique et protection des données personnelles », AJDA, 2021. 2339

²⁸⁵ J.-D. Dreyfus, Fichiers, bases de données : quel droit de propriété ?, CP ACCP 2009, n° 88, p. 39

²⁸⁶ Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

²⁸⁷ L'article L. 3131-2 du Code de la commande publique codifie l'article 53-1 de l'ordonnance n° 2016-65 du 29 janvier 2016 relative aux contrats de concession, ajouté à celle-ci par la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

²⁸⁸ Article L. 3131-2 du Code de la commande publique.

²⁸⁹ Rép. min. n° 13693 : JO Sénat 12 mars 2020, p. 1270 (Q. 9 janv. 2020, M. Claude Raynal).

²⁹⁰ *Ibid.*

contrôle de l'autorité concédante en imposant une transmission à la personne publique concédante « *au cours de l'exécution du contrat* »²⁹¹.

Il en ressort que les bases de données nécessaires au fonctionnement du service public sont réputées appartenir *ab initio* à la personne publique concédante. Ainsi, les bases de données constituées par le concessionnaire seront qualifiées de biens de retour et retourneront dans le patrimoine du concédant au terme du contrat. Il en sera ainsi, notamment, du « *fichier des abonnés, composé de données personnelles pour la facturation de l'eau et de l'assainissement* »²⁹². Il sera remis par le délégataire au délégant au moins 6 mois avant l'échéance du contrat.

En tant que producteur, le concessionnaire pourrait être tenté d'invoquer ses droits de propriété intellectuelle²⁹³ pour éviter cette restitution ; entre alors en conflit le principe de continuité du service public. Il est donc primordial de s'assurer lors de la rédaction du contrat que des clauses *ad hoc* prévoient le sort des données de manière claire. Cette vigilance doit d'autant plus être de mise qu'à l'inverse des CCAG, qui prévoient, nous l'avons vu, les « premières briques » pour imposer la suppression des données personnelles / la destruction des copies existantes, aucun mécanisme similaire n'est prévu dans le régime des concessions.

Ces différences conceptuelles majeures illustrent la difficulté à concilier la logique de marché, qui sous-tend le droit de la commande publique, et la protection des données personnelles – fer de lance du RGPD.

Pour autant, si l'articulation entre le RGPD et commande publique s'avère inachevée compte tenu de l'existence de tensions inhérentes à l'application des garanties de protection des données personnelles aux contrats de la commande publique, l'essor de l'IA dans la commande publique vient renouveler et amplifier toutes ces problématiques.

²⁹¹ B. KOEBEL, « Transmission à l'autorité concédante des données et bases de données », Contrats et Marchés publics n° 6, Juin 2020, comm. 190

²⁹² Article L. 2224-11-4 du Code général des collectivités territoriales.

²⁹³ E. Muller, Propriété intellectuelle et commande publique, AJDA 2017, p. 2056.

Chapitre II - L'essor de l'IA dans la commande publique ou le renouvellement des problématiques liées à la protection des données personnelles

La difficulté technique du sujet appelle inéluctablement quelques précisions terminologiques. Très simplement, un algorithme peut être défini comme la description d'une série d'étapes permettant d'obtenir un résultat déterminé à partir de données fournies en entrée²⁹⁴.

La formule « *traitement algorithmique* » semble pour sa part se référer à l'exécution, par un ordinateur, des instructions contenues dans un algorithme. Trompeuse par sa simplicité, cette définition renferme en réalité une grande variété de processus ; la distinction peut ainsi être faite entre les algorithmes « classiques », dont les règles sont prédéfinies et stables, et les algorithmes auto-apprenants qui peuvent réviser, eux-mêmes, leur structure interne pour s'adapter à l'environnement dans lequel ils se déploient.

Ces derniers semblent aujourd'hui se rassembler sous l'appellation de « *systèmes d'IA* » (ci-après SIA), récemment définis à l'article 3§1 du Règlement européen sur l'intelligence artificielle²⁹⁵ (ci-après RIA) comme « *un système automatisé qui est conçu pour fonctionner à différents niveaux d'autonomie et peut faire preuve d'une capacité d'adaptation après son déploiement, et qui, pour des objectifs explicites ou implicites, déduit, à partir des entrées qu'il reçoit, la manière de générer des sorties telles que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer les environnements physiques ou virtuels* »²⁹⁶.

« *Aucun domaine de l'action publique n'est imperméable* »²⁹⁷ à leur déploiement, qui suscite l'enthousiasme des uns et la crainte des autres. Facilité par des vagues successives de dématérialisation, ce phénomène s'inscrit dans le phénomène plus large de numérisation de l'action publique. En réalité, compte tenu de la taille « *éléphantinesque* »²⁹⁸ que tendent à prendre certains dossiers de commande publique, l'intégration de l'IA dans l'écosystème de la commande publique s'avère inéluctable (Section I), et commande un renouvellement de la gouvernance des données personnelles (Section II).

²⁹⁴ Glossaire de la CNIL.

²⁹⁵ Règlement sur l'intelligence artificielle UE 2024/1689 du 13 juin 2024.

²⁹⁶ Article 3§1 du RIA.

²⁹⁷ Conseil d'État, « *Intelligence artificielle et action publique : construire la confiance, servir la performance* », 31 mars 2022, p. 6.

²⁹⁸ Y. Goutal, « *Intelligence artificielle et droits des administrés* », AJCT 2025 p.142

Section I – L'intégration inéluctable de l'IA dans l'écosystème de la commande publique

Le déploiement de l'IA dans le secteur public, que tout laisse présager comme « *inéluçtable* »²⁹⁹, ne risque pas d'épargner la commande publique, qui s'avère être un terreau fertile à son intégration. La question de l'IA examinée au prisme de la commande publique (I) illustre la nécessité d'un encadrement dédié (II).

I – L'IA examinée au prisme du droit de la commande publique

Quelques précisions liminaires s'imposent. Bien entendu, rien n'impose à l'Administration d'externaliser la conception d'un système d'IA ; celle-ci demeurant libre de réaliser cette tâche « en interne ». Cette tâche suppose néanmoins de rassembler des compétences techniques importantes, qui peuvent parfois manquer. L'Administration peut alors faire le choix – pour des raisons de simplicité ou de calendrier – d'externaliser cette conception à un opérateur économique par le biais d'un contrat de la commande publique. Celle-ci peut ainsi constituer un « *levier* »³⁰⁰ important du développement de l'IA dans le secteur public.

Si l'usage de l'IA par l'Administration a fait l'objet de nombreuses contributions³⁰¹, son utilisation dans le cadre de la commande publique n'a – pour l'heure et à notre connaissance – fait l'objet que de rares études spécifiques³⁰².

Il en ressort néanmoins que commande publique et IA peuvent être analysées sous deux angles ; l'IA pouvant ainsi être l'objet d'un contrat de la commande publique (A) et un outil à son service (B).

A – L'intelligence artificielle, objet du contrat de la commande publique

Rappelons que dès lors qu'ils répondent à un « *besoin* » de l'acheteur et qu'ils sont conclus à titre onéreux, les achats des personnes publiques doivent être formalisés par l'intermédiaire de marchés publics et seront, à ce titre, soumis aux règles de la commande publique dès le premier euro dépensé. Les systèmes d'IA n'y font pas exception et pourront faire l'objet d'un contrat de la commande publique. L'administration devra se soumettre aux procédures de passation prévues par le Code de la commande publique, parfois perçues comme des «

²⁹⁹ V. notamment, CE, *Intelligence artificielle et action publique : construire la confiance, servir la performance*, 30 août 2022, préc.

³⁰⁰ C. Villani, Donner un sens à l'intelligence artificielle, 2018, p. 42.

³⁰¹ V. par exemple, le rapport du Conseil d'État : « *Intelligence artificielle et action publique : construire la confiance, servir la performance* », 31 août 2022 ; Commission européenne, Livre blanc relatif à l'IA, « *Intelligence artificielle : une approche européenne axée sur l'excellence et la confiance* », 19 février 2020

³⁰² I. Hasquenoph, « *L'intelligence artificielle et la commande publique* », AJDA 2024 p.76.

contraintes, imparfaitement adaptées à l'acquisition de systèmes d'IA »³⁰³. Pourtant, cette démarche n'est pas uniquement légaliste, elle est la garantie d'un achat raisonné (et réussi).

Certains dispositifs ayant pour objectif de favoriser les achats innovants pourront, de temps à autre, être utilisés par les acheteurs publics³⁰⁴. Sans prétendre à l'exhaustivité : le dialogue compétitif³⁰⁵ ; le partenariat d'innovation³⁰⁶ ; les marchés de services de recherche et développement³⁰⁷ ; les marchés d'achats innovants³⁰⁸.

Mal conseillés, ceux-ci pourront même, parfois, être tentés de s'exonérer de l'obligation de publicité et de mise en concurrence particulièrement, pour des raisons tenant à l'existence de « *droits d'exclusivité, notamment de propriété intellectuelle* »³⁰⁹. Attention toutefois à ne pas invoquer ces dispositions à tout va ; elles sont d'interprétation strictes et encadrées tant par le juge administratif que par le juge européen. À défaut, la personne publique s'expose à des risques contentieux importants : référé précontractuel (ou contractuel, le cas échéant) ; recours Tarn-et-Garonne ; condamnations pour octroi d'un avantage injustifié (v. *supra*).

En réalité, les risques contentieux ne seront dissipés que par une bonne définition du besoin. Pour autant celle-ci est loin d'être une chose aisée compte tenu de la diversité des acteurs présents sur le marché, du large panel de prestations disponibles et de la technicité du « jargon » technique employé.

Plusieurs écueils pratiques devront ainsi être évités. Pour ne citer que les principales : confondre besoin et offre en se laissant séduire par des promesses commerciales trop souvent exagérées (voir mensongères) ; utiliser des standards techniques d'apparences neutres mais favorisant, en pratique, certaines catégories d'opérateurs au détriment de solutions équivalentes ; la non-identification d'alternatives crédibles répondant au même besoin fonctionnel ; l'acquisition partielle d'une solution d'IA répondant à son besoin, sans anticiper la manière dont cette acquisition s'inscrira dans un ensemble plus vaste ; la retranscription des caractéristiques techniques d'une solution existante en spécifications techniques.

L'immense majorité de ces écueils peuvent être évités par la mise en place d'une phase de *sourcing* approfondie en amont de la passation du marché. Sur ce point, rappelons

³⁰³ I. Hasquenoph, « *L'intelligence artificielle et la commande publique* », AJDA 2024 p.76.

³⁰⁴ V. C. Vilani, « *Donner un sens à l'intelligence artificielle* » : Rapport, 2018, p. 43

³⁰⁵ art. L. 2124-4 du Code de la commande publique.

³⁰⁶ art. L. 2172-3 du Code de la commande publique.

³⁰⁷ art. L. 2512-5, 2°) du Code de la commande publique.

³⁰⁸ art. R. 2122-9-1 du Code de la commande publique.

³⁰⁹ V. Article R2122-3, 3° du Code de la commande publique.

que la nature et l'étendue des besoins à satisfaire doivent être « *déterminées avec précision avant le lancement de la consultation* »³¹⁰ et être définis « *par référence à des spécifications techniques* »³¹¹ ; l'insuffisance dans la définition du besoin pouvant être reprochée à l'acheteur (au stade de la passation³¹², comme au stade de l'exécution³¹³ du marché) par le juge administratif autant que par le juge pénal.

Ces exigences doivent être clairement identifiées, traduites dans les documents de la consultation et formalisées dans des clauses contractuelles appropriées. Cette approche fonctionnelle nécessite un travail préparatoire approfondi pour identifier les véritables besoins métier et les distinguer des habitudes ou des préférences techniques subjectives – les deux pouvant évidemment se recouper.

Lorsque l'Administration envisage de se doter d'un SIA portant sur un secteur sensible (touchant portant sur des activités dites de « souveraineté »), la question de l'exclusion des opérateurs tiers à l'UE – sorte de « *préférence européenne* » en matière d'IA – suscite également de nombreux débats doctrinaux³¹⁴, non encore tranchés.

Une maîtrise juridique et technique des marchés publics d'IA s'avèrera essentielle pour ne pas se priver, aujourd'hui comme demain, de la richesse qu'offre le marché. En retour, l'IA peut s'avérer être un « *outil novateur* »³¹⁵ et contribuer à transformer la passation et l'exécution des contrats.

B – L'intelligence artificielle, outil au service de la commande publique

Rendu possible par la dématérialisation des procédures – de la passation à la facturation (via *Chorus Pro*) – le déploiement de l'IA peut également s'avérer être un outil d'optimisation au service de la commande publique. Sur ce point, il est hautement probable – pour ne pas dire « *inéluçtable* » – que des systèmes d'IA soit, progressivement intégrés dans le processus d'achat.

³¹⁰ Article L2111-1 du Code de la commande publique.

³¹¹ Article L2111-2 du Code de la commande publique.

³¹² Par exemple : CAA Douai 17 janvier 2013, Commune d'Hazebrouck, n° 12DA00780 concernant un marché de vidéosurveillance d'un musée n'imposant ni un nombre de caméras déterminées, ni leur lieu d'implantation.

³¹³ Par exemple : CAA Douai, 10 mai 2007, Commune de Maromme c/ Société X n° 06DA00353 concernant l'imprudence d'une commune ayant signé un marché informatique dont les subtilités des clauses pouvaient être sujettes à interprétation.

³¹⁴ V. P. Terneyre, Sur la faculté d'exclure de la commande publique les offres en provenance d'Etats tiers à l'Union européenne, Rev. CMP 2022, n° 4 et Etude 4 ; E. Muller, La réciprocité dans l'accès à la commande publique européenne : un enjeu de politique industrielle, Rev. CMP 2021, n° 5 et Repère 5

³¹⁵ G. CLAMOUR, « *IA moyen* », Contrats et Marchés publics n° 8-9, Août 2023, repère 8

En la matière, les scénarios d'application n'ont de limite que l'imagination des praticiens. Dans sa forme la plus élémentaire, l'IA peut servir au prétraitement des dossiers, permettant de vérifier leur complétude et de synthétiser automatiquement les documents de candidature. À un niveau plus avancé, elle peut proposer un classement des offres au regard des critères de notation définis et des prix proposés.

Tentons d'être rassurants, l'IA n'aura pas vocation à conclure des contrats en lieu et place de l'Administration (en remplaçant, ce faisant, le traditionnel « acheteur public ») ; elle servira plutôt d'outil « *de rationalisation de la prise de décision* »³¹⁶. Cette vision conduit à proposer le concept d'acheteur « *augmenté* », symbolisant cette alliance entre expertise humaine et intelligence artificielle.

Au stade de la passation, elle pourrait permettre à l'acheteur de définir son besoin avec plus grande précision. Pour les acheteurs publics, l'IA est « *susceptible de donner une autre dimension au sourcing* »³¹⁷ ; en permettant aux acheteurs de réaliser des analyses de marché et permettre la constitution de bases de données de fournisseurs.

Sur ce point, de nombreuses offres sont d'ores et déjà proposées. Certaines communes françaises³¹⁸ ont ainsi pu expérimenter – l'autoproclamé – « *sourcing cognitif* »³¹⁹. L'exception n'est pas française et aux États-Unis, par exemple, des agents d'IA conversationnels viennent automatiser les tâches administratives chronophages (préparer les appels d'offres, répondre aux demandes de précisions des opérateurs économiques, etc.) pour permettre aux acheteurs de se recentrer sur des tâches à haute valeur ajoutée³²⁰.

En outre, L'IA pourrait permettre de « *désinhiber la pratique contractuelle en mettant mieux en lumière tout le champ des possibles qu'offre le Code de la commande publique, souvent minoré ou méconnu par aversion du risque* »³²¹. En matière environnementale, par exemple, force est de constater que malgré un arsenal textuel fourni permettant la mise en œuvre de critères environnementaux, les acheteurs publics peinent à définir des indicateurs de performance (*KPI*) mesurables et vérifiables. Cette difficulté se traduit souvent par une

³¹⁶ A.-L. Girard, Volonté et décision administrative algorithmique, in *Le droit administratif au défi du numérique*, Dalloz, 2020, p. 199

³¹⁷ G. CLAMOUR, « *IA moyen* », Contrats et Marchés publics n° 8-9, Août 2023, repère 8

³¹⁸ V. pour exemples Meudon et Rosny-sous-Bois in I. Hasquenoph, « *L'intelligence artificielle et la commande publique* », AJDA 2024 p.76).

³¹⁹ <https://www.silex-france.com/silex/public/solutions/buyer/public.jsf>

³²⁰ CMS Law, The potential use of AI in public procurement processes in CEE :

<https://cms.law/en/hun/publication/the-potential-use-of-ai-in-public-procurement-processes-in-cee>

³²¹ G. CLAMOUR, « *IA moyen* », Contrats et Marchés publics n° 8-9, Août 2023, repère 8

approche simpliste consistant à exclure les opérateurs économiques ne respectant pas certains seuils – interdiction de soumissionner sans bilan de ses émissions de gaz à effet de serre.

Il y a fort à parier que l'IA puisse offrir des perspectives prometteuses pour dépasser cette approche binaire en élaborant des critères objectifs, quantifiables et adaptés à chaque secteur d'activité. Elle devrait également permettre, sous supervision humaine, de garantir leur interprétation et leur explicabilité aux candidats (et auprès des juridictions en cas de contentieux). Plus globalement, l'IA permettra sans doute d'établir des critères de sélection et d'évaluation des offres personnalisés et adaptés à l'objet du marché, proposer la rédaction de clauses voire accompagner l'évaluation des candidatures et des offres.

L'IA s'avère également être un moyen de renouveler les méthodes de lutte contre la fraude dans les marchés publics. Certains algorithmes de détection permettent déjà d'identifier certains manquements pour diligenter un audit de vérification³²². A titre d'exemple, l'Agence nationale de recherche a récemment lancé un projet d'algorithme visant à détecter la corruption dans les marchés publics, baptisé *DeCoMap*³²³. Dans le même sens, la Cour des comptes portugaise a mis en place, avec le soutien de la Commission européenne, un projet d'IA visant à permettre une détection précoce d'irrégularités dans la commande publique.

La plus-value de l'IA ne sera pas exclusive à l'acheteur public ; elle bénéficiera également aux opérateurs candidats à l'attribution du contrat. Elle peut constituer « *un nouveau moyen au service de l'accroissement des parts de marché et de la conquête de la commande publique* ». De nombreuses initiatives visent à fournir aux opérateurs économiques une aide à la rédaction des candidatures ; en leur permettant « *de se fondre dans la peau de l'acheteur public, en apportant les réponses et éléments de langage qu'il attend sans même en avoir forcément conscience* »³²⁴.

Elle peut également leur servir à déterminer le « juste » prix des prestations proposées. Ce dernier point s'avère particulièrement intéressant du point de vue de la concurrence puisqu'il permet un renouvellement des problématiques liées aux ententes au travers de possibles « *ententes algorithmiques* ». Si la possibilité qu'une coordination des prix soit réalisée par des algorithmes « *sans qu'une intervention humaine ait lieu* »³²⁵ fait l'objet d'une large

³²² V. K. Rabuzin et N. Modrusan, Prediction of public procurement corruption indices using machine learning methods, KMIS, p. 333

³²³ Pour « Détection de la Corruption dans les Marchés Publics ».

³²⁴ G. CLAMOUR, « *IA moyen* », Contrats et Marchés publics n° 8-9, Août 2023, repère 8

³²⁵ J.-C. Roda, « *L'entente algorithmique* », JCP 2019, n° 28

controverse doctrinale³²⁶, il est plus probable que des « *algorithmes apprenants [facilitent] des ententes [ou ajustent] les prix et les offres pour établir un équilibre collusif* »³²⁷. Une telle entente s'est d'ailleurs produite en 2006 lorsqu'un logiciel élaborait des offres de complaisance en « *générant automatiquement leurs barèmes de prix d'après le barème de l'offre rédigée pour remporter l'appel d'offres* »³²⁸.

A ce stade, toutefois, les retours d'expérience³²⁹ témoignent d'une rareté, voire d'une absence de ces technologies dans la pratique actuelle de la commande publique, malgré les avantages qui leur sont reconnus. L'IA commence seulement à être mobilisée en matière de passation, notamment par l'entremise de divers projets pilotes. L'efficacité de ces outils reste variable et leur appropriation par les administrations demeure limitée par des questions de coût, de formation et d'adaptation aux spécificités du secteur public.

En l'état, si les perspectives offertes par l'IA sont indéniables, leur concrétisation opérationnelle nécessite encore des développements technologiques, méthodologiques et réglementaires considérables avant de pouvoir prétendre à une généralisation.

Ces améliorations – aussi significatives soient-elles – ne doivent pas éclipser le renouvellement des risques auxquels elles exposent les administrations. Les enjeux de protection des données personnelles et de maîtrise humaine appellent une approche prudente et encadrée de ces nouvelles technologies.

II – L'indispensable encadrement du déploiement de l'IA dans la commande publique

Le Règlement sur l'intelligence artificielle³³⁰ (RIA) est venu harmoniser le cadre juridique applicable à l'intelligence artificielle au sein de l'Union européenne. Le texte, premier du genre à l'échelle mondiale, 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.

Alors que l'IA tend à s'immiscer progressivement dans la commande publique, l'Administration se trouve confrontée au besoin de maîtriser ces nouvelles règles, qui seront

³²⁶ V. A. V. Den Boer, J. M. Meylahn et M. P. Schinkel, *Artificial Collusion; Examining Supracompetitive Pricing by Q-Learning Algorithms*, Amsterdam Center for Law and Economics Working Paper, 2022, n° 2002-06

³²⁷ F. Marty, *IA et ententes anticoncurrentielles*, Document de travail, <https://droit.univ-cotedazur.fr/dl4t/ia-et-ententes-anticoncurrentielles>

³²⁸ Cons. conc. 21 mars 2006, n° 06-D-07, Conseil de la concurrence c/ Société Bec frères et al., D. 2006. 1165, obs. E. Chevrier; Autorité de la concurrence, Bundeskartellamt, *Algorithmes et concurrence*, 2016, p. 75

³²⁹ F. Lichère, « *Digitalisation de la commande publique : état des lieux et perspectives d'évolution* », *Contrats et Marchés publics* n° 6, Juin 2024, étude 5

³³⁰ Règlement (UE) 2024/1689 : Règlement sur l'intelligence artificielle (RIA).

en grande majorité applicables à compter du 2 août 2026³³¹. En pratique, le législateur européen a fait le choix d'une approche transversale, privilégiant une régulation « par le risque » plutôt qu'une régulation sectorielle. Cette absence de règle spécifique à la commande publique ne signifie pas pour autant qu'il ne s'y applique pas. Au contraire, les « *autorités publiques* » sont explicitement visées dans leur double qualité potentielle de fournisseur et de déployeur.

Il est ainsi possible, de manière prospective, de tenter d'appliquer les nouvelles règles du RIA au déploiement de l'IA dans la commande publique (A). Le RGPD – mais plus largement l'édifice normatif de protection des données personnelles – s'avère, à ce titre, une source d'inspiration éclairante (B).

A – L'application prospective du RIA à la commande publique « augmentée »

Ces règles peuvent très largement être appliquées au déploiement de l'IA dans la commande publique. Évidemment, en l'absence de lignes directrices, l'exercice est prospectif et sans doute hasardeux. Pour autant, en procédant par élimination, il est possible d'en tirer quelques enseignements.

Pour commencer, la personne publique doit déterminer son positionnement dans la « *chaîne de valeur* » (fournisseur, déployeur, mandataire, importateur ou distributeur). Sur ce point, le RIA prévoit explicitement la possibilité pour une « *autorité publique* » d'assumer la qualité de « *fournisseur* » ou de « *déployeur* » ; cette faculté n'est pas expressément prévue pour les mandataires, importateurs et distributeurs – des catégories qui, en tout état, apparaissent moins compatibles avec la nature des missions des personnes publiques.

Il en ressort que le fournisseur est « *une personne (...), une autorité publique, (...) qui développe ou fait développer un système d'IA (...) 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* »³³² ; tandis qu'un déployeur est une « *personne (...), une autorité publique, (...) utilisant sous sa propre autorité un système d'IA* »³³³.

Ce faisant, une personne publique qui développe en interne un SIA ou en confie la conception à un tiers – par le biais d'un marché public – pour ses besoins propres relèvera de la qualification de « *fournisseur* » au sens du RIA. À l'inverse, lorsque l'Administration se borne

³³¹ Article 113 du RIA.

³³² Article 3, 3) du RIA.

³³³ Article 3, 4) du RIA.

à utiliser un SIA préexistant qu'elle n'a ni conçu ni fait concevoir, elle endosse la qualité de « *déployeur* ». La situation la plus complexe concerne les personnes publiques qui cumulent les fonctions de développement et de mise en service. Dans cette hypothèse de « double casquette », la collectivité se trouve simultanément investie des qualités de « *fournisseur* » et de « *déployeur* », configuration qui soulève des interrogations quant au régime juridique applicable. Une interprétation restrictive conduirait à considérer que cette dualité de statuts entraîne mécaniquement l'application cumulative de l'ensemble des obligations prévues par le RIA, qu'elles relèvent du régime du fournisseur ou de celui du déployeur.

Cette perspective, bien que logique au regard de la lettre du règlement, pourrait néanmoins générer une charge réglementaire disproportionnée pour les collectivités concernées, particulièrement celles de taille modeste qui développent des SIA pour leurs besoins propres sans intention commerciale. D'éventuelles lignes directrices devront préciser les modalités concrètes d'articulation de ces obligations, notamment pour éviter les redondances et garantir une mise en œuvre proportionnée aux enjeux réels de protection.

Outre la place occupée dans la chaîne de valeur, les acheteurs devront déterminer le risque du SIA qu'ils envisagent parmi quatre niveaux (pratiques interdites, haut-risque, risque en matière de transparence, minimal).

Au sommet de cette « pyramide » se trouvent les « *pratiques interdites* »³³⁴. Bien que l'entrée en vigueur du RIA soit échelonnée dans le temps, leur mise sur le marché / en service est d'ores et déjà interdite depuis le 2 février dernier³³⁵. Elle rassemble les cas d'usage les plus *orwelliens*³³⁶ et il s'avère peu probable qu'elle soit appliquée à la commande publique « *augmentée* ».

En dessous de ces pratiques interdites se trouvent les systèmes « *à haut risque* »³³⁷. Le RIA en distingue deux types : en premier lieu, appartiennent à cette catégorie les SIA utilisés comme composant de sécurité d'un produit couvert par la législation d'harmonisation de l'Union³³⁸ et devant faire l'objet d'une évaluation de conformité par un tiers en vue de sa mise sur le marché / en service. Cette première catégorie n'est guère d'une grande clarté et des lignes directrices sont attendues pour en interpréter plus directement le contenu.

³³⁴ Article 5 du RIA.

³³⁵ Article 113, a) du RIA.

³³⁶ La liste complète est détaillée à l'article 5 du RIA.

³³⁷ Article 6 du RIA

³³⁸ La liste de ces législations figure à l'annexe I du RIA

En second lieu, relèvent des SIA à « *haut risque* », les systèmes listés à l'annexe III du RIA. Sans prétendre à l'exhaustivité, ces SIA sont notamment ceux 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 ; ou qui, pour finir, sont utilisés pour évaluer l'éligibilité (mais également octroyer, diminuer ou révoquer) aux services publics et autres prestations sociales essentielles.

Au cas particulier, l'annexe III du RIA prévoit notamment, que les systèmes « *destinés à être utilisés pour le recrutement ou la sélection de personnes physiques, en particulier pour publier des offres d'emploi ciblées, analyser et filtrer les candidatures et évaluer les candidats* » ou « *destinés à être utilisés pour prendre des décisions influant sur les conditions des relations professionnelles, la promotion ou le licenciement dans le cadre de relations professionnelles contractuelles, pour attribuer des tâches sur la base du comportement individuel, de traits de personnalité ou de caractéristiques personnelles ou pour suivre et évaluer les performances et le comportement de personnes dans le cadre de telles relations* » ; relèvent de la catégorie des SIA à haut risque.

A priori, ces règles concernent plutôt les SIA utilisés qui sont utilisés dans le recrutement des personnes physiques. Il est néanmoins possible d'y voir un lien avec la commande publique ; en ce qu'elle a pour objet, dans le cadre de la passation du contrat, « *analyser et filtrer les candidatures et évaluer les candidats* », et dans le cadre de son exécution, de « *suivre et évaluer les performances et le comportement* » du titulaire du marché.

Côté obligations, les fournisseurs de SIA à haut risque seront soumis aux obligations les plus lourdes³³⁹ et seront garants du respect des exigences énoncées par la section 2 du RIA³⁴⁰ et doivent en démontrer le respect, à la demande de l'autorité nationale compétente. Quant aux dépouilleurs de SIA à haut risque, ils devront prendre de nombreuses mesures pour assurer la conformité de ces SIA aux articles 26 et suivants du RIA. 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

³³⁹ Art. 16 et suivants du RIA.

³⁴⁰ Notamment, mettre en œuvre, documenter et mettre à jour un « système de gestion des risques » (art. 9 du RIA), permettre techniquement l'enregistrement automatique des événements (selon les modalités prévues par l'article 12 du RIA), accompagner leur SIA d'une « notice d'utilisation » comprenant un ensemble d'informations (identité du fournisseur ; les caractéristiques, la capacité et les performances du SIA), etc.

nécessaires³⁴¹ ; lorsqu'ils sont des autorités publiques, respecter les obligations d'enregistrement prévues à l'article 49 ; réaliser une analyse d'impact relative à la protection des données (AIPD) ; informer les personnes physiques qu'un SIA à haut risque³⁴² prend ou facilite la prise de décision les concernant.

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. Il s'agit pour l'essentiel des SIA destinés à interagir directement avec des personnes physiques (*chatbots*). L'application de cette qualification à l'IA dans la commande publique est évidente ; particulièrement lorsque le SIA a pour objet de s'acquitter des formalités administratives (notamment, répondre aux demandes de précisions des opérateurs économiques). 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* »³⁴³.

Une quatrième et dernière catégorie peut enfin être constituée des SIA présentant un risque minimal. Pour schématiser, celle-ci est résiduelle et rassemble tous les SIA qui n'appartiennent à aucune des trois catégories précédemment évoquées. Bien qu'ils ne soient, *a priori*, soumis à aucune règle spécifique, les autres dispositifs en vigueur conservent leur pleine applicabilité. Ainsi, dès lors qu'ils manipuleront des données personnelles, les garanties du RGPD et de la LIL seront applicables.

Quoi qu'il en soit, celles-ci s'avèrent d'ailleurs source d'inspiration pour le déploiement « *maitrisé* » de l'IA dans la commande publique.

B – Le RGPD, source d'inspiration pour l'encadrement du déploiement de l'IA dans la commande publique

Face aux défis posés par l'opacité des systèmes décisionnels automatisés et aux biais algorithmiques potentiels, l'Administration doit être en mesure d'explicitier le fonctionnement des technologies qu'elle déploie, en clarifiant le rôle qu'elles ont joué dans la prise de décision. En matière de protection des données personnelles, un cadre juridique articulant

³⁴¹ La première obligation, commune aux fournisseurs et aux déployeurs – et 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 » (article 4 du RIA) ; V. également la « FAQ » de la Commission publiée le 13 mai 2025 sur les contours de l'obligation.

³⁴² Visé à l'annexe III

³⁴³ Art. 50 du RIA.

plusieurs textes³⁴⁴ complémentaires permet de concilier IA et protection des droits des administrés. Dans un exercice prospectif, celui-ci s'avère une source d'inspiration pour l'encadrement juridique du déploiement de l'IA dans la commande publique.

A ce titre, rappelons que le RGPD et la loi Informatique et libertés viennent encadrer la prise de décision automatisée lorsqu'elle se fonde exclusivement sur un traitement de données à caractère personnel. L'article 22§1 du RGPD précise ainsi que « *la personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire* ». Cette interdiction – à supposer même que ça en soit une – est assortie de trois dérogations : lorsque la décision est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ; lorsque qu'elle est autorisée par le droit de l'Union ou par le droit de l'État membre (v. *infra* art. 47 de la LIL) ; ou lorsque la personne concernée y consent explicitement.

Lorsqu'elle est autorisée, l'article 15, §1, h) du RGPD prévoit que la personne concernée a le droit d'obtenir du responsable du traitement, la confirmation que ses données sont traitées et d'être informée de « *l'existence d'une prise de décision automatisée (et) des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement* ».

L'article 47 de la loi Informatique et libertés reprend assez largement ces règles. S'appuyant sur la possibilité introduite par le RGPD, le législateur est venu ajouter la possibilité de prendre des « *décisions administratives individuelles* » (2°) sous réserve de respecter le cadre juridique du CRPA et de ne pas fonder sa décision sur des données sensibles (origine raciale, opinions politiques, convictions religieuses, données biométriques...).

Sur ce point, rappelons que depuis 2016, le CRPA impose une série d'obligations aux administrations lorsqu'elles s'appuient – en toute ou partie – sur un traitement algorithmique pour fonder une décision administrative individuelle. Évidemment, la première obligation consiste à prévenir l'intéressé par une « *mention explicite* » chaque fois qu'une décision individuelle est prise sur le fondement d'un traitement algorithmique³⁴⁵. Cette mention doit préciser la finalité poursuivie par le traitement et rappeler le droit d'obtenir la communication

³⁴⁴ Notamment, le Règlement général sur la protection des données (RGPD) et la Loi informatique et libertés, le Code des relations entre le public et l'administration (CRPA), et plus récemment, le Règlement européen sur l'intelligence artificielle (RIA).

³⁴⁵ L311-3-1 du CRPA

des règles définissant le traitement et les « *principales caractéristiques de sa mise en œuvre* »³⁴⁶. Les modalités d'exercice de ce droit et, le cas échéant, de saisine de la CADA doivent également être rappelées. Très concrètement, s'il en fait la demande, l'Administration doit communiquer à l'intéressé, « *sous une forme intelligible* » et sous réserve de ne pas porter atteinte à un secret protégé, le « *degré et le mode de contribution du traitement algorithmique à la prise de décision* », « *les données traitées et leurs sources* », « *les paramètres* » (et le cas échéant leur pondération), et les « *opérations effectuées par le traitement* »³⁴⁷.

Une nouvelle fois, nous ne ferons pas l'économie de rappeler que cette disposition est complétée par l'obligation – qui demeure aujourd'hui un rendez-vous manqué – pour les administrations employant plus de 50 agents (en équivalent temps plein³⁴⁸) de publier en ligne les « *règles définissant les principaux traitements algorithmiques utilisés dans l'accomplissement de leurs missions lorsqu'ils fondent des décisions individuelles* »³⁴⁹.

Reprenant très largement les textes précités, le RIA pose un « *droit à l'explication des décisions individuelles* » lorsque celles-ci sont prises par un déployeur sur la « *base des sorties d'un SIA à haut risque* »³⁵⁰ et qu'elles produisent « *des effets juridiques ou affecte significativement cette personne de façon similaire d'une manière qu'elle considère comme ayant des conséquences négatives sur sa santé, sa sécurité ou ses droits fondamentaux* ». Dans pareille hypothèse, la personne concernée peut obtenir du déployeur des « *explications claires et pertinentes sur le rôle du système d'IA dans la procédure décisionnelle et sur les principaux éléments de la décision prise* ». L'articulation de ce droit avec les autres textes applicables obéit à un principe de subsidiarité : il ne trouve à s'appliquer que dans la mesure où aucun autre fondement juridique n'est mobilisable.

Toutes ces règles s'avèrent inspiratrices et peuvent assez largement être transposées à l'encadrement du déploiement de l'IA dans la commande publique. En la matière, il est peu probable que celui-ci soit interdit ; plusieurs précautions devront néanmoins l'accompagner. La première est évidente : informer par une mention explicite le candidat que la procédure à laquelle il se porte candidat est assistée (en partie / en totalité) par un traitement algorithmique.

³⁴⁶ R311-3-1-1 du CRPA

³⁴⁷ R311-3-1-2 du CRPA

³⁴⁸ D312-1-4 du CRPA

³⁴⁹ L.312-1-3 du CRPA

³⁵⁰ Mentionné à l'annexe III, à l'exception des « infrastructures critiques » (2°).

Sur ce point, de nombreuses informations – similaires à celles transmises au destinataire d'une décision individuelle – pourraient être transmises, sur demande, au candidat : les opérations effectuées par le traitement, ses principaux paramètres, les données traitées, le degré de contribution du SIA (prétraitement, analyse de la complétude, pré-notation, notation etc.). Toutes ces informations devront être transmises sous une forme intelligible ; la communication d'un code source ne suffisant pas. Cette explication devra permettre à la personne concernée de comprendre « *dans quelle mesure une variation, au niveau des données prises en compte, aurait conduit à un résultat différent* »³⁵¹. Le responsable du traitement devra faire preuve d'une démarche active de vulgarisation et d'adaptation du discours technique pour rendre intelligible le processus ayant conduit à la décision.

Évidemment, ce partage sera effectué sous respect des secrets protégés. Le fournisseur de solution peut être « tenté » d'invoquer le secret des affaires pour s'exonérer de son devoir d'explication ; toutefois, il y a fort à parier qu'il soit contraint de communiquer les *informations prétendument protégées* à l'autorité de contrôle / à la juridiction compétente, laquelle sera chargée de pondérer les droits et intérêts en présence pour déterminer l'étendue du droit d'accès³⁵².

L'identification de ces tensions structurelles et l'analyse des mécanismes d'encadrement du déploiement de l'IA dans la commande publique appellent désormais une réflexion plus opérationnelle sur les modalités concrètes de mise en œuvre d'une protection effective des données personnelles.

Section II - La gouvernance des données personnelles à l'ère de la commande publique augmentée

L'avènement de l'IA dans la sphère publique transforme radicalement les modalités traditionnelles de traitement des données personnelles et impose une refonte des approches de gouvernance. Cette mutation technologique s'accompagne d'un bouleversement réglementaire majeur : émergence du Règlement sur l'intelligence artificielle (RIA) aux côtés du RGPD, créant un environnement juridique complexe mais complémentaire. Cette évolution conduit à repenser les cadres de conformité traditionnels pour assurer une protection effective des données dans un contexte de commande publique *augmentée* par l'IA.

³⁵¹ CJUE, C-203/22, Dun & Bradstreet Austria du 27 février 2025, Point 62.

³⁵² *Ibid.*

Cette transformation impose une double exigence : d'une part, articuler de manière cohérente l'application du RGPD et du RIA, en tirant parti de leur complémentarité pour construire une conformité véritablement intégrée (I) ; d'autre part, ériger la gouvernance des données en véritable garantie d'un déploiement *maîtrisé* de l'IA (II).

I – Du RGPD au RIA, entre continuité et complémentarité normatives

L'entrée en vigueur du RIA ne constitue pas une rupture avec le cadre normatif préexistant en matière de protection des données, mais plutôt son prolongement logique et sa spécialisation. Cette continuité normative facilite l'émergence d'une conformité « *intégrée* », où l'application conjointe des deux textes s'avère non seulement possible mais souhaitable (A). Cette articulation se trouve d'ailleurs facilitée par une architecture réglementaire pensée de manière complémentaire, où la conformité préalable au RGPD conditionne l'effectivité de l'application du RIA (B).

A – L'application conjointe des deux régimes, vers une conformité « intégrée »

Certains grands principes posés par le RGPD – pour ne pas dire tous – s'accommodent difficilement des possibilités induites par l'émergence de l'IA. Réel levier d'innovation dans la commande publique, l'IA est également un énorme facteur de brassage de données. C'est probablement à ce titre qu'elle doit le plus attirer l'attention des tenants d'un développement *maîtrisé* et respectueux des données personnelles.

L'adoption du Règlement sur l'intelligence artificielle (RIA), si elle a indubitablement introduit de nouvelles obligations – et parfois lourdes – ne doit pas occulter l'architecture réglementaire préexistante en matière de protection des données à caractère personnel. Pour l'exprimer simplement, le RIA s'analyse largement comme une actualisation des principes et des obligations prévues par le RGPD et la loi Informatique et libertés.

Les sanctions prévues par le RIA – si elles peuvent paraître importantes – sont en réalité assez modestes comparées à celles imposées par le RGPD (v. *supra*), qui s'appliquera concurremment dès lors que des données personnelles seront concernées. Pour n'en citer qu'une, on rappellera que le fait de détourner les informations collectées de leur finalité³⁵³ est une infraction pénale réprimée de peines pouvant atteindre 5 ans d'emprisonnement et de 300 000 euros d'amende. En pratique, cette infraction particulière sera applicable dès lors qu'un

³⁵³ Art. 226-21

SIA sera entraîné sur des jeux de données comprenant des données à caractère personnel collectées sans que la finalité du traitement ne soit précisée.

A ce titre, il convient d'insister sur un point. Le RIA précise explicitement n'avoir « *aucune incidence* »³⁵⁴ sur le RGPD. Il n'a donc aucunement vocation à « remplacer » le RGPD ; les deux Règlements ayant chacun leur champ d'application respectif. Les champs d'application des deux régimes ne peuvent par ailleurs être compris qu'un intégrant l'acception très large des éléments de définition (v. *supra*). Au regard des champs respectifs de l'IA et du RGPD, il est évident que les zones d'application conjointes des régimes seront très importantes et – souvent – délicates à manier.

En effet, si le RIA a principalement vocation à s'appliquer au développement, à la mise sur le marché et au déploiement des systèmes et modèles d'IA, nous rappellerons que le RGPD retient se caractérise par sa grande neutralité technologique et son approche transversale des traitements de données. Pour autant, les interrogations pratiques soulevées par cette dualité réglementaire n'ont rien d'insurmontables et, en pratique, trois configurations seront possibles.

La première hypothèse est celle dans laquelle aucun des deux régimes n'impose de contraintes. Tel sera notamment le cas lorsqu'un SIA présentant un risque minimal sera déployé sans recourir à des traitements de données à caractère personnel. Ce cas de figure sera probablement assez marginal dans la pratique des administrations, les SIA mobilisant souvent des données personnelles, ne serait-ce qu'indirectement.

Deuxièmement, l'un de ces deux Règlements pourra s'appliquer sans l'autre. Le RIA s'appliquera seul, lorsqu'un SIA présentant un certain degré de risque fonctionnera sans avoir recours à des données personnelles (par exemple, un SIA qui répond aux demandes de précisions des opérateurs économiques). Dans le même sens, le RGPD pourra également s'appliquer seul : typiquement lorsqu'un SIA à risque minimal est amené à manipuler des données à caractère personnel (par exemple, un SIA qui se contente de vérifier la complétude des pièces sans les analyser).

Troisièmement, en pratique, au regard des cas d'usages qui se développent déjà, le cas le plus courant sera celui de l'application simultanée de deux textes. La difficulté principale sera alors de bien qualifier juridiquement chaque acteur au regard des qualifications propres à chaque Règlement : au titre du RIA, principalement « *fournisseur* » ou « *déploieur* » et, au

³⁵⁴ L'article 2 du RIA précise expressément n'avoir aucune « incidence sur le règlement (UE) 2016/679 »

titre du RGPD, « *responsable du traitement* » (éventuellement conjoints) ou « *sous-traitant* ». En pratique, les qualifications des deux Règlements ne coïncident que partiellement.

Ces qualifications, qui ne se recoupent pas toujours et qui présentent parfois des zones de complexité, doivent inciter les collectivités à structurer leurs relations contractuelles et leurs procédures internes selon une logique « *intégrée* » : penser RGPD et RIA de manière concomitante. Une analyse au cas par cas sera nécessaire pour déterminer concrètement les rôles de chacun, chaque projet d'IA pouvant soulever des enjeux spécifiques.

En pratique, si les deux textes ont vocation à s'appliquer de manière simultanée pour les SIA – dès lors qu'ils sont qualifiés de SIA « à haut risque » ou qu'ils présentent un risque particulier en matière de transparence – traitant des données à caractère personnel, la conformité au RIA passera par une conformité préalable au RGPD.

B – Une application concomitante facilitée par une conformité préalable au RGPD

En réalité, l'analyse des obligations imposées par le RIA permet de dresser le constat de son imbrication avec le RGPD. En effet, parmi les nouvelles obligations introduites par le RIA figure l'établissement, pour chaque système d'IA à haut risque (SIA), d'une déclaration UE de conformité³⁵⁵. Cette déclaration, dont le contenu est détaillé à l'annexe V du RIA, doit notamment attester que le SIA respecte le RGPD dès lors qu'il implique un traitement de données à caractère personnel³⁵⁶. La conformité du système d'IA aux exigences posées par le RGPD est une condition de la conformité du SIA au RIA.

Dans le même sens, le RIA prévoit explicitement l'obligation pour les « *organismes de droit public ou des entités privées fournissant des services publics* » d'effectuer une analyse de l'impact que l'utilisation de SIA à haut risque pourrait avoir sur les droits fondamentaux. Prévue et décrite à l'article 27 du RIA, 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 et les mesures à prendre en cas de matérialisation des risques.

En réalité, cette analyse d'impact sur les droits fondamentaux (AIDF), prévue par le RIA, vient compléter l'analyse d'impact sur la protection des données (AIPD), imposée par le

³⁵⁵ Article 47 du RIA.

³⁵⁶ Annexe V ; point 5 du RIA

RGPD chaque fois qu'un traitement est « *susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées* », en particulier par le recours à de « *nouvelles technologies* »³⁵⁷ ; l'allusion à l'IA est ici flagrante. Rappelons également que la protection des données à caractère personnel devra être garantie « *tout au long du cycle de vie du système d'IA* »³⁵⁸. Cette exigence implique une approche globale qui s'étend de la phase de conception du SIA à son retrait.

Une nouvelle fois, les deux textes s'imbriquent presque parfaitement. D'une part, le RIA prévoit que les déployeurs puissent réutiliser les informations fournies dans la notice d'utilisation accompagnant le SIA pour procéder à une AIPD³⁵⁹ et s'appuyer sur des analyses d'impact existantes réalisées par le fournisseur. D'autre part, il prévoit également la possibilité pour l'AIPD de venir compléter l'AIDF lorsqu'elle remplit déjà une des obligations mentionnées à l'article 27 du RIA.

Pour « *éviter un formalisme trop contraignant* »³⁶⁰, il semble même qu'en pratique ces deux analyses – AIPD et AIDF – puissent être regroupées en un document unique.

Reste que, si la proximité entre les obligations des deux Règlements facilite leur application conjointe, le déploiement maîtrisé de l'IA ne pourra se faire qu'en établissant une véritable gouvernance des données.

II – La gouvernance des données, garantie d'un déploiement maîtrisé de l'IA

La gouvernance des données s'avère être la garantie d'un déploiement *maîtrisé* de l'IA. La première grande question pratique est managériale. Il semble pourtant que cette double conformité réglementaire puisse être assurée par un l'intermédiaire d'un référent unique (A).

En pratique, le respect des obligations imposées des obligations imposées par le RGPD et le RIA dépendra largement de leur traduction opérationnelle dans les contrats liant l'Administration aux opérateurs économiques fournisseurs de SIA. Les obligations de « *maîtrise* », de transparence et d'explicabilité demeureront de simples déclarations d'intention si elles ne sont pas traduites en clauses contractuelles précises, assorties de mécanismes de contrôle et de sanctions appropriées (B).

³⁵⁷ Article 35 du RGPD

³⁵⁸ Considérant 69 du RIA

³⁵⁹ Article 26, 9 du RIA

³⁶⁰ Entrée en vigueur du règlement européen sur l'IA : les premières questions-réponses de la CNIL 12 juillet 2024.

A – Double conformité, référent unique

Si l'interdiction de l'usage de l'IA par l'Administration – que ce soit dans le cadre de la commande publique, comme dans le cadre de ses missions d'intérêt général – est théoriquement possible, précisons d'emblée qu'elle ne nous semble ni envisageable, ni souhaitable. Premièrement, l'IA se répand indirectement, par le biais d'applications classiques, qui sont progressivement enrichies par les éditeurs des suites logicielles « classiques » (Copilot dans la suite Microsoft 365, ou encore Gemini dans la suite Google Workspace, par exemple). Deuxièmement, il serait risqué de penser le secteur public épargné par le phénomène émergent du *shadow IA*³⁶¹ quand 68%³⁶² des Français qui utilisent des IA génératives dans un cadre professionnel, confient le faire sans en informer leur supérieur hiérarchique. « *Fermez-lui la porte et elle entrera par la fenêtre* »³⁶³. Impossible donc, en pratique, de ne pas s'emparer du sujet.

Inutile de rappeler que toutes les obligations de transparence imposées, à double titre par le RGPD et le RIA, ne pourront être respectées que si l'Administration a connaissance des cas dans lesquels des processus automatisés (même partiellement) sont mis en place. Si les risques intrinsèques aux SIA peuvent être maîtrisés, les usages dissimulés posent des risques juridiques significatifs (que ce soit en termes de réplification des biais, de violation du RGPD, et souvent même de cybersécurité). La réponse adéquate semble plutôt résider dans l'acculturation, la sensibilisation et la formation des agents aux risques induits par l'usage de l'IA. Sur ce point, les nouvelles obligations de formation imposées par le RIA³⁶⁴ trouvent toute leur pertinence.

En pratique, bien que le RIA n'exige pas – contrairement au RGPD³⁶⁵ – qu'un référent soit nommé ; atteindre la double conformité sera facilité par une centralisation du contrôle, impliquant la désignation d'un « *référent IA* »³⁶⁶, dont le statut et les missions pourraient être inspirées de celles du délégué à la protection des données (DPD / DPO).

³⁶¹ Utilisations non déclarées de l'intelligence artificielle sur le lieu de travail.

³⁶² Les Français et les IA génératives, Ifop pour Talan, mai 2023.

³⁶³ Y. GOUTAL, T. SIMON, « *Le recensement des traitements algorithmiques* », La Gazette des Communes n°2776, 21 juil. 2025.

³⁶⁴ Article 4 du RIA.

³⁶⁵ Article 37 du RGPD.

³⁶⁶ Y. GOUTAL, T. SIMON, « *Faut-il désigner un référent IA dans les collectivités ?* », La Gazette des communes n° 2775, 14 juil. 2025

Trop employé dans la période récente³⁶⁷, le terme est dévalorisé et devra être employé avec prudence. Mais le fait est que la matière conduit naturellement à désigner un « *agent-centralisateur* » (ou une équipe, si la structure en a les moyens) quel que soit le nom qu'on lui donne, qui pourra s'emparer du sujet et accompagner les services, à la fois techniquement et juridiquement.

Nous l'évoquions, les deux sujets sont très proches et interagissent souvent. Bon nombre d'administrations pourraient faire le choix d'étendre les missions du DPD pour y inclure la conformité au RIA. Cette solution présente l'avantage de mutualiser certaines compétences et sera particulièrement adaptée aux « petites » collectivités. Elle nécessite cependant un renforcement des moyens alloués au DPD et une formation spécifique aux enjeux et à l'encadrement juridique de l'IA. Les collectivités disposant de ressources plus importantes ou prévoyant de faire un usage « intensif » de l'IA favoriseront plutôt la création d'un poste dédié, qui permettra une spécialisation accrue et facilitera l'identification d'un interlocuteur privilégié.

De nombreux arguments plaident en faveur du rôle significatif que pourrait jouer le DPD, ne serait-ce que dans la supervision des analyses d'impact. À l'instar des audits internes menés par le DPD s'agissant de la protection des données, le référent IA pourrait organiser des vérifications régulières de la conformité des SIA au RIA. Ces audits permettront d'identifier les éventuelles non-conformités et de les corriger le cas échéant.

Dans tous les cas, si une nomination distincte est envisagée, une étroite collaboration avec le DPD devra être établie pour garantir la cohérence des politiques de conformité et assurer la protection des données dans tous les projets d'IA de la collectivité.

La véritable valeur ajoutée du référent résidera dans sa capacité à entendre les différents candidats à l'utilisation, à traduire les obligations réglementaires en procédures opérationnelles et à anticiper les éventuelles évolutions normatives. Cette approche préventive s'avèrera particulièrement pertinente dans un contexte où le cadre juridique applicable à l'IA est encore en construction et où de nombreuses dispositions laissent encore place à l'interprétation. Par ailleurs, en cas de contentieux, la responsabilité des administrations sera vraisemblablement appréciée au regard des mesures préventives mises en œuvre dans l'utilisation des SIA.

³⁶⁷ Pour illustrer la grande diversité des « référents », voir par exemple : S. DYENS, P. VILLENEUVE, « *Comment coordonner les fonctions de référent dans sa collectivité* », La Gazette des communes, 15 mai 2024.

À la croisée des enjeux techniques et juridiques, le « référent IA » jouera un rôle d'interface entre l'Administration et les autorités compétentes, entre la Direction et ses services et entre les services eux-mêmes. Une mission fondamentale du référent consistera à cartographier³⁶⁸ – de manière dynamique – l'ensemble des IA utilisées par l'administration à laquelle il est rattaché. Pour chaque système, cette cartographie devra notamment préciser toute une série d'informations (finalité(s), classification en fonction du niveau de risque, type de données traitées, acteurs impliqués etc...).

Bien que l'élaboration d'une charte dédiée à l'IA³⁶⁹ n'apparaisse pas dénuée de sens, le plus urgent devra être d'intégrer les exigences du RIA dans les cahiers des charges des différents projets envisagés, à anticiper les obligations de transparence et surtout à les traduire contractuellement.

De fait, la rédaction des contrats devra faire l'objet d'une attention particulière pour garantir un déploiement *maitrisé* de l'IA.

B – Le contrat, outil au service de la gouvernance des données

Depuis de nombreuses années, la commande publique est « *instrumentalisée* »³⁷⁰ au service d'objectifs sociaux et environnementaux bien plus larges que la simple satisfaction des besoins de l'Administration. Ce rôle de régulateur joué par l'acheteur public s'avère largement transposable à la gouvernance des données.

La commande publique peut jouer un rôle crucial à travers la mise en place de stratégies contractuelles aptes à assurer le respect par l'IA de « *valeurs jugées souhaitables* »³⁷¹. Elle peut en effet être mobilisée pour imposer aux opérateurs économiques des exigences « *destinées à garantir le développement d'une IA éthique, responsable, digne de confiance et même respectueuse de l'égalité entre hommes et femmes* »³⁷². Cette « *régulation par le contrat* »³⁷³ suscite néanmoins de nombreuses controverses doctrinales³⁷⁴.

³⁶⁸ Cette mission de recensement n'est certes pas formellement imposée. Mais elle est en pratique indispensable, et elle décalque largement l'obligation de publication en ligne des règles définissant les principaux traitements algorithmiques qui fondent des décisions individuelles (art. L312-1-3 du CRPA).

³⁶⁹ Ce document permettrait, entre autres, de définir les bonnes pratiques, d'identifier les outils autorisés et les usages proscrits...

³⁷⁰ I. Hasquenoph, « *Commande publique : quels enjeux au lendemain du règlement européen sur l'intelligence artificielle ?* », AJCT 2025, p. 147

³⁷¹ A. Sanchez-Graells, « *Public Procurement of Artificial Intelligence : Recent Developments and Remaining Challenges in EU Law* », Legal Tech Journal, 2/2024, p. 122-131

³⁷² UNESCO, *I'd blush if I could : closing gender divides in digital skills through education*, 2019

³⁷³ I. Hasquenoph, « *Commande publique : quels enjeux au lendemain du règlement européen sur l'intelligence artificielle ?* », AJCT 2025, p. 147

En matière de commande publique, rappelons d'ailleurs que le RIA a confié au Bureau de l'IA, la mission d'évaluer et de promouvoir « *la convergence des bonnes pratiques en matière de procédures de passation de marchés publics en ce qui concerne les systèmes d'IA* »³⁷⁵.

Dès l'origine, il convient de partir du besoin fonctionnel et non de l'offre commerciale de tel ou tel opérateur au marketing séduisant. Une fois les besoins cernés, il convient de les traduire en clauses contractuelles et en critères de sélection pertinents. La promesse commerciale permet certes souvent de déclencher la réflexion, mais elle doit rester un point de départ. L'offre doit déclencher quelques questions préalables : A quel « besoin-métier » l'outil doit-il répondre ? Quelle plus-value l'IA doit-elle apporter par rapport à une solution « traditionnelle » ? Toutes les performances « attendues » – et *a contrario* les erreurs tolérées – devront être définies contractuellement.

C'est à l'acheteur de traduire ces attentes en exclusions, en critères de sélection entre les candidatures et les offres présentées, puis en exigences contractuelles et enfin en sanctions (faute contractuelle, pénalités, résiliation etc.).

Puisque les données constituent la matière première de tout SIA, on ne saurait trop insister sur l'importance stratégique de leur maîtrise. Dans un contexte où les cyberattaques (hameçonnage, rançongiciels, etc.) visant les collectivités se multiplient, le déploiement de l'IA doit être traité comme une nouvelle zone de risque et les clauses des contrats doivent permettre de refléter le sérieux des personnes publiques en imposant des obligations précises aux fournisseurs.

En matière d'*Open data* également, les collectivités devront reproduire à l'égard de leurs cocontractants, les obligations (v. *supra*) auxquelles elles sont assujetties. Il est donc impératif de définir contractuellement le statut des données, leur accessibilité, ainsi que les modalités de leur réutilisation. En pratique, la mention d'une solution « ouverte » ou « interopérable » dans le cahier des charges ne suffit pas : il faut mentionner l'utilisation de formats standards, ouverts et non propriétaires pour les données produites ou traitées, de manière à permettre leur réutilisation par d'autres systèmes ou services (y compris en cas de mutualisation entre collectivités). Les métadonnées associées devront être suffisamment « riches » pour garantir la compréhension et la réutilisation des données produites.

³⁷⁴ V. par exemple : A. Sanchez-Graells, « *Digital Technologies and Public Procurement* », p. 106.

³⁷⁵ Article 62, 3^o, d, du RIA.

Dans le même sens, pour se conformer à son obligation de publication en ligne des principaux traitements algorithmiques, l'administration doit prévoir contractuellement la fourniture par l'opérateur économique de l'ensemble des documents prévus, que la collectivité devra ensuite diffuser.

Côté RGPD, la conformité devra être prévue et organisée dès la conception du SIA, par défaut et figurer en bonne place parmi les engagements du fournisseur. Plusieurs clauses devront être insérées dans le contrat : définir clairement la finalité du traitement et encadrer (ce qui peut signifier interdire) toute autre utilisation des données par le fournisseur ; bien qualifier juridiquement les parties ; établir une base légale pour chaque traitement ; minimiser la collecte ; définir la durée de conservation et les modalités de suppression des données dans un calendrier précis ; fixer les modalités de réalisation des analyses d'impact ; définir avec précision les modalités d'exercice des droits des personnes concernées, etc.

La question du droit de propriété intellectuelle sur les données est également importante, de même que la maîtrise des droits afférents aux résultats produits. Schématiquement, il convient en premier lieu que l'Administration s'assure qu'elle dispose de tous les droits afférents aux données fournies par elle en entrée (*inputs*) et qu'elle les conservera tout au long du contrat. Il convient également d'encadrer toute réutilisation ou commercialisation de ces données par le fournisseur (que ce soit pour l'entraînement d'autres modèles, le développement de services tiers etc.). La vigilance s'impose également quant à la préservation des informations couvertes par le secret des affaires, notamment si le SIA porte sur le traitement des dossiers de commande publique.

De nombreuses dispositions éparses visent à assurer la transparence algorithmique et atténuer l'effet « *boite noire* ». Ces règles ont pour objectif commun d'assurer la transparence et l'explicabilité des décisions rendues. En pratique, il est essentiel d'intégrer une clause obligeant le cocontractant à fournir les documents *ad hoc* détaillant le fonctionnement du SIA mis en œuvre afin d'assurer le respect des droits candidats. Le fournisseur devra fournir les outils nécessaires pour permettre à l'administration de comprendre comment les données sont utilisées, transformées et enrichies. Les opérations effectuées par le traitement devront être décrites et détaillées de manière intelligible en s'inspirant des modalités prévues en matière de protection des droits des administrés (v. *supra*).

Le meilleur SIA n'est pas à l'abri d'erreurs, de défaillances techniques, de biais algorithmiques. Dès lors que c'est l'administration qui répondra de ces erreurs, il est

important que le contrat organise efficacement la garantie par le fournisseur du SIA. Sur ce point précis, le Conseil d'Etat note d'ailleurs que le régime de responsabilité « rejoint la responsabilité civile du fait des choses, en ce sens que le gardien de la chose - ici, l'administration utilisatrice du système d'IA - est responsable des dommages qu'elle cause aux tiers par l'utilisation d'un tel logiciel »³⁷⁶. Evidemment, les clauses limitatives de responsabilité sont concevables, mais doivent rester réalistes en ne vidant pas de leur substance les obligations contractuelles du fournisseur et en garantissant à la collectivité une indemnisation réaliste en cas de dommage.

Reste que, par nature, l'IA est évolutive et ses performances dépendent d'une actualisation régulière. En conséquence, le contrat doit prévoir les modalités de mises à jour, de correction des biais algorithmiques, d'accompagnement post-déploiement, de rapports réguliers de performances, d'audit du SIA (biais algorithmique, risque cyber...). Dans le même esprit, une clause dédiée à la réversibilité du système devra être prévue : il s'agit de prévoir avec précision la fin du contrat, et notamment les éléments devant être restitués, détruits ou conservés, ainsi que les formats d'exportation des données ; finalement, dans la même logique que le sort des données personnelles au terme du contrat (v. *supra*). L'objectif étant de permettre la réutilisation effective des données par le service ou par un nouveau prestataire.

Enfin, dans un domaine qui reste en partie exploratoire, l'amélioration du prochain marché doit être un objectif prioritaire, que ce soit pour compléter, approfondir ou alléger le dispositif : obligations, contrôle, pénalités, ne doivent pas être fixées une fois et pour toujours. Le référent (IA ou DPD, les deux pouvant se recouper) devra collecter les besoins d'évolution, afin que les contrats futurs soient améliorés.

³⁷⁶ V. I. Hasquenoph, « L'intelligence artificielle et la commande publique », AJDA 2024 p.76.

Conclusion de la seconde partie

L'analyse de l'articulation entre droit de la commande publique et RGPD révèle un paysage juridique en mutation profonde, caractérisé par des tensions structurelles persistantes mais aussi par des dynamiques d'adaptation prometteuses. L'étude met en évidence l'existence d'un chantier inachevé, où la logique protectrice du RGPD peine encore à s'imposer face aux impératifs économiques de la commande publique.

L'examen approfondi des mécanismes de la commande publique démontre l'existence de contradictions fondamentales entre les philosophies juridiques qui sous-tendent ces deux corpus normatifs. D'un côté, la commande publique s'enracine historiquement dans une logique de marché privilégiant la transparence, la concurrence et l'optimisation de l'utilisation des deniers publics. De l'autre, le RGPD institue une logique protectrice centrée sur la responsabilisation (*accountability et compliance*) des acteurs et la préservation des droits individuels.

Cette confrontation se cristallise notamment autour de l'opposition entre l'exigence de transparence propre à la commande publique et l'impératif de confidentialité inhérent à la protection des données personnelles. L'étude de la hiérarchie implicite des secrets révèle que le droit de la commande publique accorde une protection privilégiée au secret des affaires, reléguant la protection de la vie privée au rang de préoccupation secondaire. Cette priorisation témoigne de l'ancrage persistant de la commande publique dans une logique économique qui demeure, *in fine*, peu réceptive aux enjeux de protection des données personnelles.

Cette confrontation se manifeste avec une acuité particulière dans la gestion du sort des données au terme de l'exécution des contrats. L'absence de droit de propriété sur les données personnelles, conjuguée à la reconnaissance de droits de propriété intellectuelle sur les bases de données, crée un cadre juridique complexe que les CCAG et les dispositions du CCP peinent à appréhender pleinement.

L'émergence de l'IA dans l'écosystème de la commande publique constitue un catalyseur de ces tensions préexistantes. L'IA exacerbe, par nature, les problématiques de protection des données personnelles tout en ouvrant des perspectives inédites d'optimisation des processus d'achat public. Cette (r)évolution technologique s'accompagne d'un bouleversement réglementaire majeur avec l'adoption du Règlement sur l'intelligence artificielle. L'analyse prospective de son application à la commande publique révèle la nécessité d'une approche intégrée, articulant de manière cohérente les exigences du RGPD et celles du RIA. Cette

double conformité, loin de constituer un simple empilement normatif, dessine les contours d'une gouvernance renouvelée.

L'étude des mécanismes de gouvernance souligne l'importance déterminante de la traduction contractuelle des obligations réglementaires. Le contrat s'affirme comme l'outil privilégié de cette gouvernance, permettant de transformer les exigences abstraites du RGPD et du RIA en obligations concrètes et vérifiables. Cette contractualisation suppose néanmoins une expertise technique et juridique approfondie, que la désignation d'un référent spécialisé pourrait utilement consolider.

L'émergence du concept d'acheteur « *augmenté* » symbolise cette transformation en cours, où l'alliance entre expertise humaine et intelligence artificielle redéfinit les modalités d'actions classiques de la commande publique. Cette évolution impose toutefois une vigilance constante pour préserver l'équilibre entre innovation technologique et protection des droits fondamentaux.

Si l'adaptation progressive du cadre juridique témoigne d'une prise de conscience croissante des enjeux, de nombreux défis demeurent. La généralisation de l'IA dans la commande publique nécessitera des développements normatifs complémentaires, une montée en compétence des praticiens et une évolution des pratiques contractuelles.

Conclusion générale

La présente étude avait pour ambition d'examiner l'articulation entre le droit de la commande publique et le RGPD, en questionnant l'adaptation du cadre contractuel aux impératifs de protection des données personnelles. Il convient de dresser le bilan nuancé d'une transformation juridique en cours, marquée par des avancées significatives mais aussi par des limites structurelles persistantes.

L'étude a d'abord révélé l'omniprésence des traitements de données personnelles dans la commande publique, témoignant de la profondeur de la numérisation de l'action publique. Face à cette réalité, le droit de la commande publique a opéré une adaptation progressive, visible tant au stade de la passation des contrats qu'à celui de leur exécution. Les évolutions récentes notamment l'intégration de dispositions relatives à la protection des données dans les CCAG de 2021, traduisent une prise de conscience croissante des enjeux de conformité.

Toutefois, cette intégration demeure imparfaite et inachevée. L'application des notions fondamentales du RGPD aux acteurs de la commande publique nécessite encore une appréciation au cas par cas, source de complexité pour les praticiens. La coexistence de deux régimes juridiques de sous-traitance distincts – celui de la commande publique et celui du RGPD – illustre parfaitement cette difficulté d'harmonisation.

L'analyse approfondie a mis en évidence l'existence de tensions structurelles entre deux logiques juridiques aux fondements distincts. D'un côté, le droit de la commande publique privilégie une approche économique, de l'autre, le RGPD consacre une logique de protection des droits données, basée sur la responsabilisation (*accountability*) et la conformité dès la conception du traitement et par défaut (*by design / by default*).

Ces tensions se manifestent particulièrement dans la gestion du sort des données au terme de l'exécution des contrats, où l'absence de droit de propriété sur les données personnelles se confronte à la reconnaissance de droits de propriété intellectuelle sur les bases de données. L'existence d'une hiérarchie implicite entre secret des affaires et secret de la vie privée confirme la prééminence des considérations économiques sur la protection des données personnelles dans le régime actuel.

L'émergence de l'intelligence artificielle dans la commande publique vient amplifier ces problématiques en soulevant des défis inédits. Si l'IA offre des perspectives prometteuses d'optimisation de l'action publique, elle nécessite une approche intégrée pour concilier

l'application du RIA et du RGPD. La gouvernance des données s'impose alors comme le vecteur privilégié d'un déploiement maîtrisé de l'IA, appelant à repenser les pratiques contractuelles.

En réponse à la problématique initiale, il apparaît que la commande publique peut constituer un cadre adapté à l'application du RGPD à condition d'une harmonisation plus poussée entre les deux régimes. Celle-ci passe nécessairement par une clarification des rôles et responsabilités des acteurs, une meilleure articulation des régimes de sous-traitance, et l'adoption d'une approche préventive intégrée dans la passation des contrats.

L'effectivité de cette conciliation dépendra avant tout de la capacité des pouvoirs publics à dépasser les tensions structurelles identifiées pour construire un cadre juridique cohérent, alliant l'efficacité de l'action publique et le respect des droits fondamentaux.

Cette évolution s'avère d'autant plus nécessaire que la numérisation de l'action publique et le déploiement inéluctable de l'IA rendent inévitable une réflexion approfondie sur l'articulation entre innovation technologique et protection des données personnelles.

Plan détaillé

Partie I – L’application perfectible du RGPD aux contrats de la commande publique.....	11
Chapitre I – L’encadrement complexe du traitement de données à caractère personnel.....	12
Section I – L’omniprésence du traitement de données à caractère personnel dans les contrats de la commande publique	12
I – L’approche extensive du traitement de données à caractère personnel retenue par le RGPD	12
A – La conception englobante de la « donnée à caractère personnel »	13
B – L’acception étendue du « traitement » de données	14
II – La large typologie de données traitées dans les contrats de la commande publique	16
A – Le traitement de données, objet du contrat	16
B – Le traitement de données, accessoire au contrat.....	18
Section II – L’application casuistique des qualifications du RGPD aux acteurs de la commande publique	19
I – L’identification délicate du responsable du traitement	19
A – Le cas de la responsabilité « exclusive » du traitement appliqué au contrat public.....	20
B – L’hypothèse réaliste d’une responsabilité « conjointe » du traitement.....	22
II – Les défis de la qualification du sous-traitant	23
A – L’identification <i>in concreto</i> du sous-traitant RGPD	23
B – La dualité des régimes de sous-traitance, source de confusion pratique	25
Chapitre II - La prise en compte partielle des exigences relatives à la protection des données personnelles par le droit de la commande publique	26
Section I – L’intégration de la protection des données au stade la passation du contrat..	27
I – La conformité RGPD, prérequis à l’attribution du contrat	27
A – L’exclusion possible des opérateurs défaillants en matière de protection des données.....	27
B - Le respect des données personnelles comme critère de sélection des offres	29
II – L’encadrement contractuel de la sous-traitance du traitement de données.....	30
A – L’intégration des clauses contractuelles, garantie de l’applicabilité du RGPD.	31
B – Une prise en compte des exigences de protection des données facilitée par les CCAG.....	32
Section II - L’intégration de la protection des données au stade de l’exécution du contrat	34
I – Le RGPD comme source du renforcement des obligations des parties	34
A – L’élargissement du panel des sanctions contractuelles envisageables.....	35
B – L’élargissement du « devoir » de contrôle de l’autorité contractante.....	37

II – Le RGPD comme source du renforcement de la responsabilité des parties au contrat.....	38
A – L’aggravation du volet pénal de la commande publique	38
B – L’adjonction d’un large éventail de sanctions prévues par la CNIL.....	39
Conclusion de la première partie.....	42
Partie II - L’articulation inachevée du droit de la commande publique et du RGPD.....	43
Chapitre I – L’existence de tensions inhérentes à l’application des garanties de protection des données personnelles aux contrats de la commande publique.....	43
Section I – La difficile conciliation entre logique de marché et protection des données personnelles.....	44
I – Les fondements économiques de la commande publique comme limite intrinsèque à la protection des données.....	44
A – La prééminence des impératifs économiques dans la commande publique	45
B – L’ <i>Accountability</i> du RGPD, une logique antagoniste aux impératifs économiques.....	47
II – Le déséquilibre structurel entre transparence de la commande publique et confidentialité des données personnelles	49
A – Le respect du RGPD comme limite à l’ouverture des données publiques	49
B – L’existence implicite d’une hiérarchie des secrets en droit de la commande publique.....	52
Section II - L’enjeu complexe et négligé du sort des données personnelles au terme du contrat.....	54
I – L’épineuse question de la propriété des données	55
A – L’absence avérée de droit de propriété sur les données personnelles.....	55
B – La reconnaissance d’un droit de propriété des « bases de données ».....	58
II – Le sort différencié des données au terme de l’exécution du contrat.....	60
A – Le cadre structuré des CCAG, entre « connaissances antérieures » et « résultats ».....	60
B – Le régime complexe des concessions, entre « biens de retour » et continuité du service public.....	63
Chapitre II - L’essor de l’IA dans la commande publique ou le renouvellement des problématiques liées à la protection des données personnelles.....	67
Section I – L’intégration inéluctable de l’IA dans l’écosystème de la commande publique	68
I – L’IA examinée au prisme du droit de la commande publique	68
A – L’intelligence artificielle, objet du contrat de la commande publique	68
B – L’intelligence artificielle, outil au service de la commande publique	70
II – L’indispensable encadrement du déploiement de l’IA dans la commande publique	73
A – L’application prospective du RIA à la commande publique « augmentée »	74

B – Le RGPD, source d’inspiration pour l’encadrement du déploiement de l’IA dans la commande publique	77
Section II - La gouvernance des données personnelles à l’ère de la commande publique <i>augmentée</i>	80
I – Du RGPD au RIA, entre continuité et complémentarité normatives.....	81
A – L’application conjointe des deux régimes, vers une conformité « intégrée »....	81
B – Une application concomitante facilitée par une conformité préalable au RGPD	83
II – La gouvernance des données, garantie d’un déploiement maîtrisé de l’IA.....	84
A – Double conformité, référent unique.....	85
B – Le contrat, outil au service de la gouvernance des données.....	87
Conclusion de la seconde partie	91
Conclusion générale	93
Plan.....	95

BIBLIOGRAPHIE

OUVRAGES

AUBY J.-B., *Droit administratif général*, 5e éd., Dalloz, coll. « Précis », 2019.

BELLI L. et GUGLIELMI G. J. (dir.), *L'État digital*, Berger Levrault, 2022, 367 p.

Droit des données personnelles, Dalloz décryptage, 2020.

DESGENS-PASANAU G., *La protection des données personnelles, Le RGPD et la nouvelle loi française*, 3e éd., LexisNexis, 2018.

GAUTRAIS V., *Neutralité technologique : rédaction et interprétation des lois face aux changements technologiques*, Thémis, 2012.

HAAS G., *Guide juridique du RGPD*, 2e éd., ENI, 2020.

JÈZE G., *Les contrats administratifs*, t. II, 1932.

ORWELL G., 1984.

PÉQUIGNOT G., *Théorie générale du contrat administratif*, 1945.

TARLET F., *Les biens publics mobiliers*, Dalloz, Nouv. bibl. de thèses, 2017.

TERWANGNE C. de et ROSIER K., *Le Règlement général sur la protection des données (RGPD / GDPR), Analyse approfondie*, Larcier, 2018.

AFDA, *Le droit administratif au défi du numérique*, Dalloz, 2019.

BASDEVANT A. et MIGNARD J.-P., *L'empire des données, Essai sur la société, les algorithmes et la loi*, Don Quichotte, 2018.

BRUGUIÈRE J.-M., *Les données publiques et le droit*, Litec, 2002.

BRUGUIÈRE J.-M., *L'émergence d'un droit des données*, 2023.

SANCHEZ-GRAELLS A., *Public Procurement and the EU Competition Rules*, Hart Publishing, 2015.

ARTICLES

ANCI AUX A. et FARCHY J., « L'instauration de droits de propriété sur les données personnelles, une légitimité économique contestable », *Rev. éco. ind.*, 2017, n° 158, p. 9.

AUBY J.-B., « Contrats publics et smart cities », *Contrats et Marchés publics*, n° 10, octobre 2017, étude 11.

AUBY J.-B., « Données publiques et administration numérique », *JurisClasseur Administratif*, fasc. 109-20, 2023.

AUBY J.-B., « Orientations du droit des données publiques », *JurisClasseur Administratif*, fasc. 109-20.

BAER M., "Governing Corporate Compliance", *B. C. L. Rev.*, vol. 50, 2009, p. 949-1019.

BANEL S. et DELESALLE C., « Appliquer les pénalités contractuelles au titulaire d'un contrat public », *La Gazette des communes*, mai 2023.

BENOIT F.-P., « Le droit administratif français », *D.*, 1968, n° 1161.

BOER A. V. DEN, MEYLAHN J. M. et SCHINKEL M. P., « Artificial Collusion; Examining Supracompetitive Pricing by Q-Learning Algorithms », *Amsterdam Center for Law and Economics Working Paper*, 2022, n° 2002-06.

BOUCHER P., « Safari ou la chasse aux Français », *Le Monde*, mars 1974.

CLUZEL-MÉTAYER L. et PRÉBISSY-SCHNALL C., *JurisClasseur Administratif*, fasc. 109-32.

DAIGRE J.-J., « Compliance entreprise et Europe », in M.-A FRISON-ROCHE, *Pour une Europe de la compliance*.

DU MARAIS B., « Compliance », in *Dictionnaire des régulations*, LexisNexis, 2016, p. 191.

DREYFUS J.-D., « Fichiers, bases de données : quel droit de propriété ? », *CP ACCP*, 2009, n° 88, p. 39.

DYENS S. et VILLENEUVE P., « Comment coordonner les fonctions de référent dans sa collectivité », *La Gazette des communes*, 15 mai 2024.

GIRARD A.-L., « Volonté et décision administrative algorithmique », in *Le droit administratif au défi du numérique*, Dalloz, 2020, p. 199.

GINSBURG J., « Fédéralisme et propriété intellectuelle », in M.-F. TOINET (dir.), *L'État en Amérique*, Presses de la fondation nationale des sciences politiques, 1989, p. 193.

« Intelligence artificielle et droit administratif », *RFDA*, 2025.

LUBBERS J., « Electronic Administration in the United States », in J.-B. AUBY (dir.), *Droit comparé de la procédure administrative/ Comparative Law of Administrative Procedure*, Bruylant, 2016, p. 821-831.

MARTY F., « IA et ententes anticoncurrentielles », Document de travail, <https://droit.univ-cotedazur.fr/dl4t/ia-et-ententes-anticoncurrentielles>.

NETTER E. et CHAIGNEAU A., *Les biens numériques*, Paris, PUF, coll. CEPRISCA, 2015.

RABUZIN K. et MODRUSAN N., « Prediction of public procurement corruption indices using machine learning methods », *KMIS*.

REES C., *Who Owns Our Data ?*, août 2013.

ROCHFELD J., « Contre l'hypothèse de la qualification des données personnelles comme des biens », in E. NETTER et A. CHAIGNEAU, *Les biens numériques*, Paris, PUF, coll. CEPRISCA, 2015, p. 221-236.

BASSI T., « Les données collectées par le concessionnaire de service public », *AJDA*, 2019, p. 496.

BERNELIN M., « La patrimonialisation des données personnelles : entre représentation(s) et réalité(s) juridiques », *JCP G*, n° 46, 11 novembre 2019, doct. 1172.

BOURCIER D. et DE FILIPPI P., « Vers un droit collectif sur les données de santé », *RDSS*, 2018, p. 444.

BOUL M., « Réflexions sur la notion de donnée publique », *RFAP*, 2018/3, p. 473.

CHATRY S., « Droits des producteurs des bases de données », *JCl. Civil Code*, fasc. 1650.

CLAMOUR G., « IA moyen », *Contrats et Marchés publics*, n° 8-9, août 2023, repère 8.

CLUZEL-MÉTAYER L., « La loi pour une République numérique : l'écosystème de la donnée saisi par le droit », *AJDA*, 2017, p. 340.

CORIO LAND S., « Commande publique et risque pénal », *AJ Pénal*, 2022, p. 563.

FONTAINE M. et JUILLET S., « La donnée numérique : l'or noir du XXIe siècle ? », *LPA*, 8 septembre 2017, n° 179-180, p. 90.

FOLLIOT-LALLIOT L., « Obligations contractuelles et pouvoirs de l'Administration », *JurisClasseur Administratif*, fasc. 775.

GOUTAL Y., « Intelligence artificielle et droits des administrés », *AJCT*, 2025, p. 142.

GOUTAL Y. et SIMON T., « Le recensement des traitements algorithmiques », *La Gazette des Communes*, n° 2776, 21 juillet 2025.

GOUTAL Y. et SIMON T., « Faut-il désigner un référent IA dans les collectivités ? », *La Gazette des communes*, n° 2775, 14 juillet 2025.

GRIGUER M. et SCHWARTZ J., « Privacy by Design/Privacy by Default. Une obligation de conformité et un avantage concurrentiel », *CDE*, 2017, n° 3.

HASQUENOPH I., « Commande publique et protection des données personnelles », *AJDA*, 2021, p. 2339.

HASQUENOPH I., « L'intelligence artificielle et la commande publique », *AJDA*, 2024, p. 76.

HASQUENOPH I., « Commande publique : quels enjeux au lendemain du règlement européen sur l'intelligence artificielle ? », *AJCT*, 2025, p. 147.

HOEPFFNER H., « Le pouvoir de direction et de contrôle », in V. BOUHIER et D. RICCARDI (dir.), *L'exécution des contrats administratifs*, Le Moniteur, 2018, p. 74.

KALFLÈCHE G., « Secteur public et concurrence : la convergence des droits », *AJDA*, 2007, p. 2420.

KOEBEL B., « Transmission à l'autorité concédante des données et bases de données », *Contrats et Marchés publics*, n° 6, juin 2020, comm. 190.

LAFaix J.-F., « La maîtrise et la protection des données liées aux contrats de la commande publique : approche théorique », *JCP A*, n° 51-52, 26 décembre 2023, 2396.

LESSIG L., « Privacy as property », *Social Research: An International Quarterly*, 69, 2002, p. 257.

LICHÈRE F., « Digitalisation de la commande publique : état des lieux et perspectives d'évolution », *Contrats et Marchés publics*, n° 6, juin 2024, étude 5.

MATTHIOS F. J., « Données à caractère personnel : la CNIL découvre un trou dans la raquette », *JCP A*, n° 24, 14 juin 2021, 2181.

MULLER E., « Propriété intellectuelle et commande publique », *AJDA*, 2017, p. 2056.

MULLER E., « La réciprocité dans l'accès à la commande publique européenne : un enjeu de politique industrielle », *Rev. CMP*, 2021, n° 5, repère 5.

OCHOA N., « Pour en finir avec l'idée d'un droit de propriété sur ses données personnelles : ce que cache véritablement le principe de libre disposition », *RFDA*, 2015, p. 1157.

PAILLER L., « Le paradoxe de la compliance dans le droit de la protection des données », *Cahiers de droit de l'entreprise*, n° 1, janvier-février 2025, dossier 8.

PERRAY R., « La sanction complexe des personnes publiques », *Communication Commerce électronique*, n° 3, mars 2024, dossier 5.

POULLET Y., « La "propriété" des données : balade au "pays des merveilles à l'heure du big data" », in *Penser le droit de la pensée, Mélanges en l'honneur de Michel Vivant*, Dalloz, 2020, p. 338.

RODA J.-C., « L'entente algorithmique », *JCP*, 2019, n° 28.

ROLIN F., « Le rôle de la pratique dans la construction du droit des contrats administratifs », *in A propos des contrats des personnes publiques, Mélanges en l'honneur du Professeur Laurent Richer*, LGDJ, 2013, p. 9.

SAINT-AUBIN T., « Les nouveaux enjeux juridiques des données (big data, web sémantique et linked data), Les droits de l'opérateur de données sur son patrimoine numérique informationnel », *RLDI*, 2014, n° 102.

SANCHEZ-GRAELLS A., « Public Procurement of Artificial Intelligence : Recent Developments and Remaining Challenges in EU Law », *Legal Tech Journal*, 2/2024, p. 122-131.

SOUYRIS J.-P., « La DAJ et la CNIL parlent-elles le même langage ? », *achatpublic.info*.

TERNEYRE P., « Sur la faculté d'exclure de la commande publique les offres en provenance d'États tiers à l'Union européenne », *Rev. CMP*, 2022, n° 4, étude 4.

UNTERSINGER M., « Ce que les "révélations Snowden" ont changé depuis 2013 », *Le Monde*, 13 septembre 2019.

VANDEVEN E., « La protection des données personnelles pleinement intégrée dans les CCAG », *achatpublic.info*, 3 juin 2021.

TEXTES EUROPEENS

Règlements européens

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD).

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

Directives européennes

Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Directive 96/9/CE du Parlement européen et du Conseil, du 11 mars 1996, concernant la protection juridique des bases de données.

Directive 2014/24/UE, PE et Cons. UE, sur la passation des marchés publics.

Directive 2014/25/UE, PE et Cons. UE, relative à la passation de marchés passés par des entités opérant dans les secteurs de l'eau, de l'énergie, des transports et des services postaux.

Directive 2014/23/UE, PE et Cons. UE, sur l'attribution de contrats de concession.

JURISPRUDENCE

Conseil d'État

CE, 3 avril 1925, *Commune de Mascara*, Lebon, p. 382.

CE, 18 juillet 1930, *Compagnie des Chemins de fer PLM*, Lebon, p. 753.

CE, 5 novembre 1937, *Caire*, Lebon, p. 899.

CE, 22 février 1952, *Société pour exploitation procédés Ingrand*, Lebon.

CE, 7 novembre 1958, *Société Électricité et eaux de Madagascar*, Lebon, p. 530.

CE, 23 mars 1960, n° 46221, *Société Spiesshofer et Braun*, Lebon 215.

CE, 10 juillet 1996, n° 168702, *Société Direct Mail Promotion*, Lebon 277.

CE, 21 décembre 1906, n° 19167, *Syndicat des propriétaires et contribuables du Quartier Croix-de-Seguey-Tivoli à Bordeaux*, Lebon p. 962.

CE, avis, 29 juillet 2002, n° 246921, *Société Maj Blanchisseries de Pantin*.

CE, 30 septembre 1983, *SARL Comexp*, Lebon, p. 393.

CE, Sect., 30 mars 1990, *Mme Degorge Boëtte*, n° 90237.

CE, 29 décembre 2008, n° 296930, *SARL OPHLM de Puteaux*.

CE, 12 septembre 2018, n° 420454 et 420512, *SIOM de la vallée de Chevreuse*, Lebon T. 2018.

CE, 12 juin 2019, n° 427397, *ministre des Armées*.

CE, Ass., 21 décembre 2012, n° 342788, *Commune de Douai*.

CE, 16 mai 2022, n° 459904, *Commune de Nîmes*.

Cour de Justice

CJCE, 15 mai 1986, aff. 222/84, *Marguerite Johnston c/ Chief Constable of the Royal Ulster Constabulary*.

CJCE, 9 juillet 1989, aff. C-265/87, *Hermann Schröder*.

CJCE, 20 février 1979, aff. 120/78, *Rewe-Zentral AG c/ Bundesmonopolverwaltung für Branntwein* (Cassis de Dijon).

CJCE, 7 décembre 2000, aff. C-324/98, *Telaustria*.

CJCE, 9 novembre 2004, aff. C-203/02, *RTD com.* 2005, p. 90, obs. F. Pollaud-Dulian.

CJUE, 14 juillet 2016, aff. C-406/14, *Wroclaw-Miasto Na Prawach Powiatu*.

CJUE, 19 octobre 2016, aff. C-582/14, *Breyer*, EU:C:2016:779.

CJUE, 20 décembre 2017, aff. C-434/16, *Novak*.

CJUE, 17 novembre 2022, aff. C-54/21, *Antea Polska SA*.

CJUE, 27 février 2025, C-203/22, *Dun & Bradstreet Austria*.

Cour de cassation

Civ. Ire, 9 novembre 1983, *JurisData* n° 1983-702217.

Civ. 1re, 8 novembre 1983, n° 82-13.547, Bull. civ. I, n° 260.

Civ. 1re, 25 mai 1992, n° 90-19.460, Bull. civ. I, n° 161.

Civ. 1re, 20 janvier 2004, n° 00-19.577.

Civ. 1re, 22 septembre 2011, n° 10-23.073.

Civ. 2e, 30 janvier 2014, n° 12-24.145, Bull. civ. II, n° 26.

Conseil constitutionnel

Conseil constitutionnel, 26 juin 2003, n° 2003-473 DC, *Loi habilitant le gouvernement à simplifier le droit*.

Conseil constitutionnel, 29 décembre 2003, n° 2003-489 DC, *Loi de finances pour 2004*.

Autres juridictions

CAA Paris, 20 mars 2012, *Caisse nationale d'assurance vieillesse travailleurs salariés (CNAVTS)*.

CAA Douai, 10 mai 2007, *Commune de Maromme c/ Société X*, n° 06DA00353.

CAA Douai, 17 janvier 2013, *Commune d'Hazebrouck*, n° 12DA00780.

CA Paris, 18 mars 1993, *Société du journal téléphoné*, *AJDA*, 1993, p. 652.

RAPPORTS

Banque des territoires et Intercommunalités de France, « Baromètre de la commande publique », mars 2023.

Ifop pour Talan, « Les Français et les IA génératives », mai 2023.

Conseil d'État, « Le numérique et les droits fondamentaux », 2014.

Conseil d'État, « Intelligence artificielle et action publique : construire la confiance, servir la performance », 31 mars 2022.

VILLANI C., « Donner un sens à l'intelligence artificielle », 2018.

GUIDES, FICHES TECHNIQUES, AVIS ET LIGNES DIRECTRICES

CNIL, *Guide du sous-traitant*, septembre 2017.

CNIL, *Guide « La responsabilité des acteurs dans le cadre de la commande publique »*.

CNIL, *Guide pratique de la publication en ligne et de la réutilisation des données publiques (« Open data »)*.

CNIL, « Sous-traitance : exemple de clauses », 4 octobre 2017.

CNIL, « Entrée en vigueur du règlement européen sur l'IA : les premières questions-réponses de la CNIL », 12 juillet 2024.

DAJ Bercy, « Fiche L'IMPACT DU RGPD SUR LE DROIT DE LA COMMANDE PUBLIQUE », octobre 2018.

DAJ Bercy, « Réforme des cahiers des clauses administratives générales (CCAG) 2021 », avril 2021.

DAJ Bercy, « Conseils aux acheteurs et aux autorités concédantes. Les pénalités dans les marchés publics », 1er avril 2019.

DAJ Bercy, « La publication des données essentielles de la commande publique », juin 2024.

Décret n° 74.938 du 8 novembre 1974.

Réponse ministérielle n° 13693, *JO Sénat*, 12 mars 2020, p. 1270.

DAJ Bercy et CADA, « La communication des documents administratifs en matière de commande publique », 1er avril 2019.

CNIL, délib. n° SAN-2018-001, 8 janvier 2018.

CNIL, délib. n° SAN-2021-003, 12 janvier 2021.

CNIL, délib. n° SAN-2021-019, 29 octobre 2021.

CNIL, délib. n° 2022-032, 24 mars 2022.

CADA, avis n° 20033429, 28 août 2003.

CADA, conseil n° 20031928, 15 mai 2003.

CADA, conseil n° 20004574, 7 décembre 2000.

CADA, conseil n° 20073859, 11 octobre 2007.

CEPD, *Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD.*

Groupe de travail « Article 29 », *Avis n° 4/2007 du 20 juin 2007 sur le concept de données à caractère personnel.*

Groupe de travail « Article 29 », *Opinion n° 05/2014 du 10 avril 2014 sur les techniques d'anonymisation.*

Groupe de travail « Article 29 », *Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », 16 février 2010.*

Circulaire NOR : PRMG9400081C du 14 février 1994 relative à la diffusion des données publiques.