2024

DATA ET IA

LES NOUVELLES RÈGLES DU JEU EN EUROPE

Les interconnectés
RÉSEAU DES TERRITOIRES INNOVANTS

FRANCE URBAINE
MÉTROPOLES, AGGLOS ET GRANDES VILLES

INTERCOMMUNALITÉS DE FRANCE

ÉDITO

Franckie Trichet
Président des Interconnectés,
Vice-président de Nantes métropole

Lors de la mandature qui vient de se terminer, les institutions Européennes se sont largement emparées du sujet numérique. Le cadre politique et réglementaire qui a été adopté vise à concilier la défense des droits de l'homme et les enjeux de compétitivité économique. Le Règlement Général sur la Protection des Données (RGDP) a montré la capacité des Européens à protéger nos droits face aux usages invasifs des technologies. Les discussions autour de l'IA Act notamment ont montré la complexité d'un équilibre entre régulation et innovation.

> RENFORÇONS LE RÔLE DE L'EUROPE EN TANT QUE RÉGULATEUR DU NUMÉRIQUE

Notre volonté d'accompagner la pratique d'un numérique responsable sur le plan social, environnemental et éthique, affirmée dès 2021 dans le Manifeste « Pour des territoires numériques responsables » nous encourage à renforcer nos relations avec l'Europe.

La période qui s'ouvre est importante car c'est le début d'une nouvelle mandature au niveau Européen et la mise en application de ces textes. Les collectivités peuvent faire entendre leur voix.

Il nous faut investir les instances de travail européennes dont découlent les priorités, les financements et appels à projets. Au niveau national, l'objectif est de ne pas envisager les textes comme des contraintes règlementaires imposées mais de saisir ce moment clé de l'implémentation comme un cadre commun et l'opportunité d'une mise en œuvre adaptée aux enjeux de nos territoires. C'est la clé pour que l'Europe garde ce rôle de régulation et accompagne nos pratiques locales y compris sur le volet social et solidaire.

Alors que les avancées technologiques connaissent une nouvelle accélération avec l'IA notamment, nous souhaitons que cette note permette aux élus et aux agents de s'emparer de ces textes. Nous pouvons peser sur les orientations européennes et nationales afin de définir une feuille de route et inscrire durablement un cadre clair pour une pratique responsable, solidaire et éthique du numérique.

SOMMAIRE

GUIDE DE LECTURE

Les principales définitions sont identifiées par le pictogramme

Les points de débat sont identifiés par le pictogramme

Les encadrés "parlons technique" sont identifiés par le pictogramme

Le tableau synthétique, en page 6, vous donne une vue d'ensemble des textes.
Le quizz, en page 11, vous permettra de tester, de manière ludique, votre connaissance du règlement sur l'intelligence artificielle (AI Act).

2019-2024, UNE PÉRIODE CHARNIÈRE EN MATIÈRE DE RÉGULATION DU NUMÉRIQUE

En juin dernier, les Européens ont élus les 720 députés du Parlement européen. Ces élections marquent aussi la fin de la mandature de la Commission européenne dirigée par Ursula Von der Leyen.
De 2019 à 2024, cette mandature a marqué une étape très importante en matière de régulation du numérique, avec l'adoption de plusieurs règlements structurants sur l'intelligence artificielle, les données ou encore les plateformes en ligne.

L'ensemble de ces textes (qu'il faut prendre comme un ensemble cohérent et non comme une série de régulations sectorielles), va déterminer les règles du jeu pour les dix à quinze prochaines années en Europe. Certaines de ces règles concernent en premier lieu les entreprises (et notamment les grandes plateformes), mais d'autres vont aussi s'adresser plus directement aux administrations publiques et aux collectivités.

La "décennie numérique"

La **transformation numérique** était présentée, en 2019, comme l'une des six priorités de la commission Von der Leyen, au même niveau que la transition climatique (avec le Pacte vert) ou l'emploi. L'ambition affichée s'étendait d'ailleurs sur deux mandats : il s'agit de la "décennie numérique" (digital decade). 5 ans après, qu'en est-il de l'ambition affichée ? S'il fallait résumer l'action de la commission en matière de régulation du numérique en une expression, ce serait sans doute celle d'activisme juridique et réglementaire. Rarement, dans l'histoire de l'Union européenne, autant de textes concernant le numérique n'auront été proposés, discutés et adoptés qu'en la période 2019-2024.

Les clés de lecture

Pour comprendre l'action de ces cinq dernières années, on peut adopter (au moins) deux clés de lecture.

La première est d'ordre géopolitique. En matière de numérique, l'Union européenne revendique de suivre une voie qui lui est propre, et surtout distincte des deux autres blocs géopolitiques que sont les États-Unis d'une part et la Chine d'autre part. L'UE entend ainsi marquer sa différence avec l'approche des grandes plateformes du numérique (basée sur une exploitation intensive des données personnelles) mais aussi avec le capitalisme d'État et la surveillance du régime chinois. Cette **troisième voie** entend promouvoir et soutenir l'innovation technologique, dans le respect des droits et valeurs fondamentales de l'Union européenne. Comme nous le verrons dans cette note (par exemple à propos de la régulation des modèles d'IA génératives), cette troisième voie ressemble parfois à un chemin de crête.

L'autre clé de lecture est temporelle : par essence, le temps de la régulation est un temps long. A titre d'illustration, six années séparent le premier projet de révision du droit des données à caractère personnel et la mise en application du RGPD. Or, le temps du numérique est un temps beaucoup plus rapide. Comment "attraper", par le droit, des usages toujours changeants, avec des ruptures technologiques et d'usage ? C'est aussi l'une des questions qui traversent le débat au niveau européen.

À l'origine était le RGPD

On ne peut pas comprendre les nouveaux textes adoptés, et la logique qui les sous-tend, sans avoir à l'esprit le retour d'expériences du Règlement général sur la protection des données (RGPD) et de son application en Europe depuis 2018.

Commençons par un chiffre : 4 milliards d'euros, c'est le montant des amendes infligées au titre de non-respect des obligations du RGPD sur la période 2018-2023. 145 000 plaintes ont été déposées au niveau européen, un nombre en forte progression. 69% des citoyens européens ont déclaré connaître le RGPD[1], ce qui fait de ce texte européen l'un des plus connus du grand public. Le règlement a aussi permis d'harmoniser le cadre juridique au niveau européen (et ainsi d'éviter que chaque État-membre développe sa propre législation). Le RGPD et, malheureusement aussi les épisodes de fuites massives de données, ont contribué à sensibiliser les Européens sur la gestion de leurs données à caractère personnel.

Mais la mise en œuvre du règlement a aussi fait l'objet de plusieurs critiques.

La première concerne le manque de proportionnalité des obligations (que l'on soit une PME, une petite association ou une grande entreprise, les obligations sont relativement semblables). La seconde difficulté est le choix de faire appliquer le RGPD par l'autorité de protection des données du pays d'installation de l'entreprise concernée - et non celui où résident les utilisateurs. En pratique, toutes les grandes plateformes du numérique ont leur siège social européen à Dublin, ce qui fait de facto de la "CNIL" irlandaise un acteur central … alors même que l'économie irlandaise dépend beaucoup de ces multinationales[2]. Certains droits prévus dans le RGPD, comme le droit à la portabilité des données personnelles, ne sont pas ou peu mis en œuvre.

Le retour d'expérience du RGPD, tant sur ses succès et ses demi-échecs, a beaucoup marqué le législateur européen. On en trouve la trace dans les grands textes qui se sont succédé depuis, dont le règlement IA ou le Digital Services Act.

Changer la manière de réguler le numérique

La plupart des textes qui sont présentés dans cette note partagent la même logique de régulation, caractérisée par :

1) une approche **par les risques,**
2) une approche **proportionnée** et
3) une attention particulière aux **rapports de force** existants.

L'approche par les risques consiste à identifier, a priori, les risques posés par une technologie, un usage ou une application. Elle s'oppose à une approche basée sur les droits (à l'image du RGPD). Comme l'indique la Commission européenne à propos du règlement sur l'intelligence artificielle : "L'AI Act ne crée pas de nouveaux droits, il s'assure que les droits existants sont bien appliqués"[3], et ce en venant clarifier les responsabilités de chaque acteur de la chaîne intervenant dans la mise sur le marché ou la mise en service des systèmes d'IA.

L'approche est dite proportionnée car elle module les obligations en fonction des risques, mais aussi de la taille des acteurs (et de leurs nombres d'utilisateurs en Europe).

Enfin, ces textes tiennent compte aussi des **rapports de force** existants : les grandes plateformes sont ainsi qualifiées d'acteurs systémiques et sont soumises à des règles plus fortes que les autres acteurs. De même, plusieurs textes visent explicitement à éviter l'abus de position dominante des grands acteurs du numérique.

Enfin, pour ne pas reproduire les mêmes erreurs que le RGPD, ces nouveaux textes donnent souvent à la Commission elle-même des pouvoirs de régulation accrue, en lien avec les autorités de régulation des États-membres. Ils prévoient aussi la création de nouvelles structures dépendant directement de la Commission, comme l'AI Office ou l'European Centre for Algorithmic Transparency (ECAT).

(1) "Your rights matter: data protection and privacy", Fundamental rights survey 2019, Agence européenne des droits fondamentaux.
(2) "L'Irlande, seul pays du G20 à afficher une croissance positive grâce aux GAFA", Les Echos, 5 mars 2021.
(3) Source : entretien entre la délégation d'élus de France Urbaine et Martin Ulbrich, chef de l'unité A.2 de la DG Connect, Bruxelles, le 21 mars 2024.

Les principaux textes adoptés

	Ambition principale	Thèmes	Date d'application *(Calendrier prévisionnel)*	Niveau d'impact pour les collectivités
Règlement sur l'intelligence artificielle (AI Act)	Permettre le développement d'une IA de confiance et encadrer les usages	• Approche par les risques • Usages interdits en UE • Régulation des IA à usage général (ChatGPT)	**Fin 2024** *(Interdiction de certaines applications)* **Mi-2026 et 2027** *(Applications à haut-risque et risque limité)*	★★☆
Règlement sur la gouvernance des données (Data Governance Act)	Faciliter le partage sécurisé de données entre les acteurs européens	• Nouveaux modèles de gouvernance • Espaces communs de données • Altruisme de données	**Septembre 2023**	★★★
Règlement sur les données (Data Act)	Faciliter l'utilisation des données industrielles et non-personnelles	• Données de l'Internet des Objets • Partage de données B2G • Portabilité des données entre différents services cloud	**Septembre 2025**	★★☆
Directive NIS 2	Renforcer la cyber résilience au niveau européen	• Cybersécurité • Cadre de coopération européen	**Automne 2024**	★★☆
Règlement sur les services numériques (Digital Services Act)	Responsabiliser les (grandes) plateformes et les services numériques	• Régulation des plateformes • Haine en ligne, désinformation • Modération des contenus	**Février 2024**	★☆☆
Règlement sur les marchés numériques (Digital Market Act)	Renforcer la concurrence et mettre fin à la domination des géants du Net	• Abus de position dominante • Protection des PME	**Mars 2024**	★☆☆
Règlement sur l'Europe interoperable	Faciliter le déploiement de services publics numériques transeuropéens	• Services transeuropéens • Services transfrontaliers • Obligation de conformité en matière d'interopérabilité	**Pas avant 2025**	★☆☆

RÉGULER L'INTELLIGENCE ARTIFICIELLE : LE RÈGLEMENT IA

L'accord politique conclu le 8 décembre 2023 dans le cadre du trilogue (Commission européenne, Conseil représentant les États-membres et Parlement européen) illustre, à bien des égards, le parcours mouvementé du règlement sur l'Intelligence artificielle (AI Act). En effet, il a fallu plus de 3 jours de pourparlers-marathons pour faire converger les positions, parfois opposées, des différents acteurs sur ce texte. "En adoptant une approche proportionnée selon la nature des risques, le règlement définit le cadre de confiance nécessaire à l'utilisation de l'IA en Europe" s'est aussitôt félicité Thierry Breton, le commissaire européen au marché intérieur [(4)].

Une IA digne de confiance

L'approche européenne de l'intelligence artificielle s'inscrit dans un discours qui vise à proposer **une troisième voie,** distincte donc, de celles des Etats-Unis et de la Chine. Cette troisième voie veut concilier la capacité d'innovation et la réaffirmation des valeurs fondamentales de l'Union européenne, dont la protection des droits humains. "Une IA digne de confiance" (trustworthy AI), cela signifie concrètement que le développement de solutions d'intelligence artificielle doit être encadré par le droit, mais aussi que, sur le continent européen, certains usages sont interdits ou fortement encadrés.

En pratique, comme nous le verrons en détail, pour la plupart des applications d'IA, il s'agit principalement de faire preuve de **transparence**.

Quelle définition pour l'intelligence artificielle ?

La question de la définition de l'intelligence artificielle - et donc de facto du périmètre de l'AI Act - a fait l'objet de très nombreux débats ces dernières années.

Fallait-il privilégier une définition très large - comme le souhaitaient les organisations de la société civile et l'aile gauche du Parlement européen - ou, au contraire, restreindre l'IA aux seules techniques d'apprentissage machine - comme le souhaitaient les éditeurs de solutions logicielles, la majorité des États-membres et le PPE [(5)] ?

In fine, l'AI Act s'aligne sur la définition adoptée par l'OCDE :

Système d'intelligence artificielle

Un système automatisé qui, pour des objectifs explicites ou implicites, déduit, à partir d'entrées reçues, comment générer des résultats en sortie tels que des prévisions, des contenus, des recommandations ou des décisions qui peuvent influer sur des environnements physiques ou virtuels. Différents systèmes d'IA présentent des degrés variables d'autonomie et d'adaptabilité après déploiement [(6)]. (OCDE, 2023)

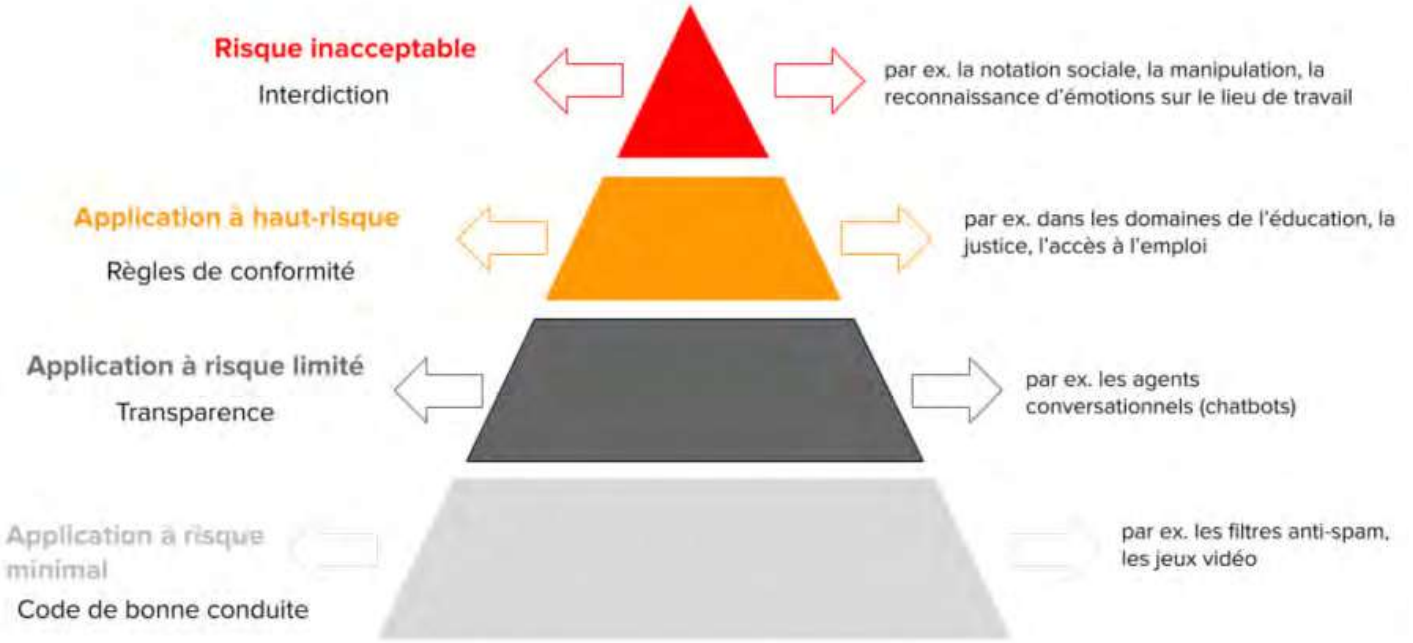
L'important, dans cette définition, est la dernière phrase concernant les "degrés variables d'autonomie et d'adaptabilité", qui laisse supposer que c'est bien la position pro-business du PPE et du Conseil (représentant les États-membres) qui a été retenue.

(4) "Thierry Breton : L'IA Act n'entrave aucunement la révolution en mouvement de l'intelligence artificielle, tribune publiée dans le journal Le Monde, 16 décembre 2023.
(5) Le Parti populaire européen est le premier groupe du Parlement européen. Il regroupe 70 partis de centre-droit et de droite dont les Républicains en France et la CDU en Allemagne. La présidente de la Commission européenne, Ursula Von der Leyen, est issue du PPE.
(6) Recommandation du Conseil sur l'intelligence artificielle, adoptée le 22.05.2019, amendée le 12.11.2023, OCDE

Un encadrement proportionné des risques de l'IA

L'approche du règlement sur l'IA est basée sur les risques et distingue 4 niveaux : les applications formellement interdites, les applications à haut-risque, les applications à risque limité et les applications à risque minimal ou nul.

Les obligations sont proportionnelles aux risques - c'est à dire que plus une application est considérée comme risquée, plus elle sera encadrée.



L'approche par les risques

(traduit de l'Ada Lovelace Institute, 2022)

En pratique, la très grande majorité des applications de l'Intelligence artificielle seront classées à risque limité ou minimal, et à ce titre soumises à des obligations de transparence peu contraignantes. Le texte lui-même se concentre sur les applications à haut-risque, et intègre une série d'obligations pour mettre sur le marché européen (c'est-à-dire développer ou importer) de telles solutions. Ces obligations sont réparties entre les différents acteurs de la chaîne mais elles pèsent essentiellement sur le fournisseur de la solution d'IA et non sur la collectivité qui l'utilise.

Les applications à risque inacceptable sont interdites

La **notation sociale,** à des fins publiques ou privées, est interdite car contraire aux valeurs de l'Union européenne et aux droits fondamentaux. Cet exemple illustre bien aussi la volonté européenne de se démarquer de la Chine, où un tel système de social scoring est massivement utilisé. Les techniques de manipulation du comportement, ainsi que les **techniques subliminales** figurent aussi sur la liste des applications interdites, de même que les applications qui ciblent les vulnérabilités des personnes (par exemple en raison de leur âge, de leur handicap ou de leur situation personnelle et sociale, comme l'extrême pauvreté). La reconnaissance des émotions sur le lieu de travail ou d'enseignement est aussi interdite. La commercialisation ou l'importation d'une application interdite est passible d'une amende de **35 millions d'euros ou 7% du chiffre d'affaires annuel mondial.**

(7) Le règlement sur l'IA utilise le terme anglais GPAI (general purpose artificial intelligence).
(8) "EU AI Act compliance analysis: general-purpose AI models in focus", The Future Society, décembre 2023.

Les applications à haut-risque font l'objet d'un contrôle accru et, dans certains cas, d'un contrôle par une autorité indépendante.

Le règlement sur l'intelligence artificielle liste une série d'applications considérées à haut-risque :

1) Sont tout d'abord considérés les systèmes qui sont intégrés dans des équipements déjà soumis à des **obligations de sécurité,** comme par exemple une IA dans un dispositif médical, un jouet ou un véhicule : tous ces équipements font l'objet aujourd'hui d'une certification obligatoire pour être mis sur le marché européen (donnant lieu pour certains à un marquage CE) et sont soumis à une surveillance particulière tout au long de leur durée de vie,

2) Les systèmes d'IA identifiés comme à haut risque comprennent en outre la technologie de l'IA utilisée dans certains **secteurs** comme les **infrastructures critiques** (par exemple les transports), susceptibles de mettre en danger la vie et la santé des citoyens ; la **formation** éducative ou professionnelle, qui peut déterminer l'accès à l'éducation et au cours professionnel de la vie d'une personne (par exemple, la notation des examens) ; **l'emploi** (par exemple, un logiciel de tri de CV pour les procédures de recrutement) ; **les services publics** et privés essentiels (par exemple, l'évaluation d'un dossier de demande d'allocation ou d'attribution d'une place en crèche), la gestion des **migrations,** de l'asile et du contrôle aux frontières (par exemple, vérification de l'authenticité des documents de voyage), le secteur répressif ou encore la **justice.**

Pour les **applications à haut-risque,** ce sont les organisations qui développent, importent et commercialisent ces solutions qui devront mettre en oeuvre la plus grande partie des obligations de l'AI Act, parmi lesquelles la mise en place d'un système de **gestion des risques,** un audit des **données d'apprentissage** (pour s'assurer que ces données sont fiables, représentatives et ne présentent pas de biais préjudiciables), tenir à jour une documentation technique dans une optique de conformité, et **s'enregistrer** auprès des autorités compétentes pour obtenir le marquage CE. A défaut, les entreprises qui développent, commercialisent et importent des solutions à haut-risque sont passibles d'une amende de 15 millions d'euros ou 3% du chiffre d'affaires annuel mondial.

Pour les **applications à risque faible,** comme les agents conversationnels (chatbots) ou la réalisation de deep fakes et images de synthèse à des fins artistiques, la principale obligation est liée à la transparence : les utilisateurs doivent être informés que le contenu a été généré par une intelligence artificielle, sous peine d'une amende pouvant atteindre **7,5 millions d'euros ou 1,5% du chiffre d'affaires annuel mondial.** Enfin pour **les applications à risque minime** (faible ou nul), le règlement sur l'IA recommande l'adoption volontaire de codes de conduite.

L'irruption de ChatGPT : comment réguler les systèmes d'IA à usage général ?

Le temps de la régulation est un temps long, par définition opposé au temps rapide de l'innovation technologique. **A titre d'illustration :** plus de 6 années séparent la première proposition de la Commission européenne sur l'évolution de la réglementation des données à caractère personnel et l'entrée en vigueur du RGPD, texte qui ne mentionne d'ailleurs à aucun moment l'intelligence artificielle. Dès lors, l'irruption de nouvelles technologies, et de nouveaux usages comme l'IA générative (ChatGPT, Mid Journey, ...) représente un défi pour le régulateur. La principale différence entre les applications déjà citées et des systèmes et modèles comme des LLM c'est que ces derniers sont à usage général[7] : c'est l'utilisateur qui détermine in fine l'usage qu'il fera de cette technologie. Qui doit être soumis à des obligations : le développeur du modèle de fondation ou l'utilisateur ? Certains - en premier lieu la France - sont même allés plus loin : il ne faudrait pas appliquer de règles trop contraignantes ("sur-réguler") des technologies émergentes, au risque de brider l'innovation et le développement de champions européens.

Parlons technique : LLM et modèles de fondation

Un **modèle de fondation** est un modèle d'intelligence artificielle entraîné sur de très grands volumes de données et qui peut être adapté à un large éventail de tâches, comme la production de texte, d'images ou de contenu audio. Dans le domaine du traitement du langage, les modèles de fondation sont dénommés des **LLM** (large modele langage), ou modèles de langage de grande taille, comme GPT-3 et **GPT-4** développés par OpenAI. Mais il existe aussi des modèles de fondation capables de traiter et générer des images, comme DALL-E, Stable Diffusion ou celui utilisé par **Mid Journey.** Entraîner un modèle de fondation comme GPT-4 demande des investissements très conséquents - de l'ordre de **500 millions de dollars** selon des estimations indépendantes[8], et est très consommateur d'énergie. La plupart des grands acteurs de l'économie numérique ont développé leurs propres LLM (comme LLaMA pour Meta, la maison-mère de Facebook). Mais il est aussi possible d'entraîner (ou de ré-entraîner) un LLM sur un corpus de données plus restreintes et pour un usage plus spécialisé, par exemple pour *écrire du code informatique,* préparer des *délibérations* ou encore dessiner un *nouvel épisode de Tintin !*

La régulation des modèles de fondation a bien failli faire capoter l'accord politique obtenu en trilogue. En particulier, la France s'est fermement opposée à la Commission, au Parlement et à la majorité des autres États-membres sur ce point. Fait inhabituel, le Président de la République a ainsi publiquement critiqué l'accord obtenu en trilogue, en indiquant son désaccord sur la régulation des modèles de fondation. De nombreux observateurs, en France et en Europe, ont souligné que la position de la France visait avant tout à défendre son champion national, la société Mistral AI[9], en arguant notamment de la souveraineté technologique européenne.

L'accord finalement obtenu prévoit plusieurs cas de figure, selon la puissance du modèle de fondation (mesurée par la puissance de calcul utilisée pour l'entraînement) et le caractère open source (ou non) du modèle. Il distingue ainsi les **modèles à risque systémique**[10] (par exemple les futures versions de GPT d'OpenAI) et les modèles de base. Dans les deux cas, les développeurs devront publier un résumé détaillé des jeux de données et respecter la directive européenne sur le copyright. Les modèles à risque systémique (c'est-à-dire les plus puissants) sont soumis à des obligations renforcées en partie similaires à celles des applications à haut-risque mais aussi spécifiques, notamment en matière de cybersécurité et de consommation d'énergie. Les modèles open source, qu'ils soient systémiques ou non, voient leurs obligations allégées par rapport à des modèles propriétaires. Enfin, point important, le texte prévoit que la Commission puisse identifier de nouveaux critères, qualitatifs, pour déterminer les modèles qui présentent des risques systémiques (et seront donc soumis à des obligations renforcées).

L'usage de la biométrie (dont la reconnaissance faciale) dans l'espace public

Le second "sujet chaud" de la discussion autour du règlement sur l'intelligence artificielle porte sur l'usage de la biométrie dans l'espace public, notamment par les forces de police. La biométrie s'est beaucoup développée ces dernières années dans l'espace public, notamment avec l'émergence de systèmes de reconnaissance faciale et de caméras dites intelligentes. Ces technologies présentent des risques importants en matière de libertés individuelles et publiques (risque de biais discriminatoires et de faux positifs, réduction de la liberté de circulation, mais aussi de la liberté de manifester sur la voie publique). Par essence, un visage est un identifiant unique que chaque individu garde tout au long de sa vie et qu'on ne peut pas changer. Le règlement européen encadre ainsi certains usages de la biométrie dans les espaces publics par les forces de police. Sont en particulier concernés les systèmes d'identification à distance en temps réel.

Parlons technique : la biométrie et ses usages

Les systèmes biométriques, c'est comme les champignons : certains sont comestibles sans danger, d'autres non. On distingue ainsi deux types d'usages : la **vérification** et **l'identification**.

Dans le premier cas, il s'agit de vérifier si un visage (ou l'iris d'un œil, une empreinte palmaire ou tout autre élément biométrique) correspond bien à un profil déjà enregistré, par exemple pour déverrouiller un smartphone (FaceID sur iPhone).

Dans le second cas, le visage est comparé à plusieurs autres profils présents dans une base de données. Les usages de la biométrie pour la vérification sont beaucoup moins invasifs en termes de vie privée (ils ne demandent pas la constitution d'une base centralisée de profils et restent la plupart du temps en local, sous le contrôle de l'utilisateur). A l'inverse, les usages pour l'identification nécessitent la constitution d'une base de données centrales, et le plus souvent le transfert à distance de ces données biométriques[11].

Le règlement pour l'intelligence artificielle interdit l'usage de systèmes d'identification à distance en temps réel par les forces de police (law enforcement), mais de nombreuses exceptions à cette interdiction ont été introduites par les États-membres (et leurs ministères de l'Intérieur). Ainsi, il sera possible de déployer de tels systèmes pour rechercher des personnes disparues, prévenir une menace imminente et substantielle, identifier des suspects de crimes sérieux.

Dans ces cas-là, les forces de police devront, avant tout déploiement, réaliser une étude de l'impact sur les droits fondamentaux et enregistrer leur système dans un registre européen. Une autorisation devra être obtenue auprès de la justice ou d'une autorité administrative indépendante. Cependant, exception dans l'exception, il sera possible de déployer de tels systèmes dans des situations d'urgence, à condition de faire une demande d'autorisation sous 24 heures.

(9) Mistral AI, start up fondée par d'anciens de Deepmind (une filiale de Google spécialisée dans l'IA), est aujourd'hui valorisée à plus de 2 milliards d'euros. Elle compte notamment à son capital l'ancien secrétaire d'Etat au numérique Cédric O.
(10) Sont dits à risques systémiques les modèles ayant une incidence significative sur le marché de l'Union en raison de leur portée ou d'effets négatifs réels ou raisonnablement prévisibles sur la santé publique, la sûreté, la sécurité publique, les droits fondamentaux ou la société dans son ensemble, pouvant être propagé à grande échelle tout au long de la chaîne de valeur (AI Act).
(11) Pour en savoir plus, voir notamment "Remote biometric identification: a technical & legal guide", EDRi, janvier 2023.

QUIZ

Selon vous, quel niveau de risques pour les applications suivantes de l'IA dans une collectivité ?

(réponses en dernière page)

	Risque inacceptable (interdiction)	Application à haut-risque	Applique à risque limité ou faible	Application à risque minime ou nul	Ça dépend !
1) Un système de tri automatique des CVs pour des candidats à un poste de catégorie A					
2) Un système de notation des habitants en fonction de leur comportement de bons citoyens en matière de collecte et recyclage des déchets					
3) La création d'une image de synthèse pour illustrer le magazine de la ville					
4) Un système de comptage de nombre de piétons utilisant des caméras de vidéosurveillance					
5) Un chatbot aidant les administrés dans leurs démarches administratives sur le site Internet de la Mairie					
6) Un outil d'aide à la rédaction de délibérations pour les agents des collectivités					
7) Un système analysant des images satellites pour repérer des décharges sauvages					
8) Un système vidéo IA permettant à la police municipale de repérer dans une foule les individus n'ayant pas payé la cantine scolaire					

Règlement sur l'intelligence artificielle : beaucoup de bruit pour rien ? Quel impact pour les collectivités ?

De l'aveu même de ses concepteurs, l'AI Act ne concerne qu'une minorité des applications de l'intelligence artificielle : "Seulement 10 à 15% des systèmes d'intelligence artificielle seront soumis à des obligations au titre du règlement sur l'intelligence artificielle" indique le cabinet du rapporteur du texte au Parlement européen[12].

De prime abord, on peut considérer que l'impact de cette nouvelle régulation sur les usages de l'IA par les collectivités sera **relativement limité.** En effet, la vaste majorité des cas d'usages aujourd'hui identifiés[13] relèvent a priori de la catégorie à risque limité, voire nul. De plus, la plupart des obligations incombent à ceux qui développent et importent des solutions d'IA sur le territoire européen, et pas directement sur les utilisateurs.

En clair : si une collectivité achète une solution qui intègre une intelligence artificielle, c'est bien la société qui lui vend le système qui sera responsable de la mise en conformité avec le règlement, pas la collectivité utilisatrice (sauf cas spécifiques mentionnés). Si la collectivité développe elle-même des applications d'intelligence artificielle, par exemple en utilisant des modèles de fondation de type LLM, alors elle sera elle-aussi soumise à certaines obligations, en particulier si cette application relève des domaines à haut-risque (emploi, éducation, accès aux services publics). Les administrations publiques seront notamment tenues de réaliser une étude d'impact sur les droits fondamentaux[14].

De là cependant à considérer que, finalement, ce règlement ne change rien pour les collectivités ("beaucoup de bruit pour rien"), il y a un pas qu'il ne faut pas franchir, au moins pour deux raisons. Tout d'abord il ne faut pas sous-estimer **le lien existant entre régulation et acceptabilité sociale.** L'exemple du RGPD nous montre que, au-delà même des obligations nouvelles, l'existence de ce règlement a eu un impact fort sur la sensibilisation du public aux enjeux de vie privée. Parallèlement, les nombreux exemples de fuite de données à caractère personnel et de détournement d'usage ont alimenté une demande plus forte de protection de la part des individus. Il est tout à fait possible qu'il en soit de même pour l'intelligence artificielle.

Cela implique des efforts, de la part des collectivités, non seulement pour bien appliquer le corpus juridique existant (le règlement sur l'IA n'annule pas le RGPD, bien au contraire !) mais aussi pour s'assurer de l'acceptabilité sociale des solutions déployées, quand bien même celles-ci présenteraient un risque minime ou nul au sens du règlement IA.

Ensuite, il faut bien comprendre que le règlement sur l'intelligence artificielle ne règle pas tout. Il y a de la place pour des engagements propres (la doctrine internet de la collectivité en matière d'IA et de données, les engagements de type chartes) mais aussi pour les législations nationales (comme l'obligation de transparence et d'information sur les traitements algorithmiques par les acteurs publics, obligation introduite par la Loi pour une République numérique).

(12) Source : rencontre entre la délégation d'élus de France Urbaine et Dan Nechita, directeur de cabinet du député européen Dragos Tudorache, Bruxelles, 21 mars 2024.
(13) Par exemple par l'Observatoire Data Publica dans le cadre de son enquête annuelle auprès des collectivités et de la note de conjoncture La Poste et Banque des Territoires.
(14) Pour en savoir plus : article 27 : l'évaluation de l'impact sur les droits fondamentaux des systèmes d'IA à haut-risque

RÉGULER L'ÉCONOMIE DES DONNÉES : LE DATA ACT ET LE DATA GOVERNANCE ACT

La commission Von der Leyen a été particulièrement active en matière de données, notamment avec la publication de la stratégie européenne pour la donnée (2020). L'ambition est de créer un marché unique européen en matière de données, en facilitant le partage et l'usage des données. En pratique, il s'agit de d'assurer une nouvelle liberté de circulation - celles des données - en complément de la libre circulation des individus, des biens et services et des capitaux déjà garanties par l'Union européenne. La stratégie européenne a été déclinée dans deux textes majeurs : le règlement sur la gouvernance des données (Data Governance Act, 2022) et le règlement sur les données (Data Act, 2023). Par ailleurs, la directive sur l'Open Data (Open Data Directive, 2019) est venue préciser le cadre existant en matière d'ouverture des données publiques.

Une clé de lecture : gagner la bataille des données non-personnelles et industrielles

L'objectif de la stratégie est clairement affiché : "L'UE devrait mettre en place un environnement attrayant pour parvenir à ce que, d'ici à 2030, la part de l'Union dans l'économie fondée sur les données corresponde au moins à son poids économique, non par le fruit du hasard, mais par choix[15]." Pour comprendre l'enjeu, il faut partir d'un constat : la bataille des données à caractère personnel est, dans une large mesure, en passe d'être gagnée par des acteurs non-européens, états-uniens et chinois en tête. Ces deux blocs géopolitiques - et en premier lieu les américains - concentrent la majorité de la création de valeur par l'usage intensif des données personnelles, notamment celles des Européens. Mais, pour nombre d'observateurs, la **prochaine bataille** est celle des données non-personnelles, industrielles et, plus globalement, celle de l'Internet des objets (IoT). Le Data Governance Act et le Data Act s'inscrivent parfaitement dans cette ambition.

Enfin une définition officielle des données !

Le premier mérite du Data Governance Act est de proposer une définition officielle des données. Aussi curieux que cela puisse paraître, au regard des nombreux textes adoptés ces dernières années (notamment la directive sur l'open data), c'est la première fois que la définition des données est clarifiée au niveau européen. On notera que la définition proposée est assez large, et qu'elle va donc plus loin que celle des données tabulaires gérées dans un logiciel comme Excel ou Open Office.

Donnée

"Toute représentation numérique d'actes, de faits ou d'informations et toute compilation de ces actes, faits ou informations, notamment sous la forme d'enregistrements sonores, visuels ou audiovisuels"

(Data Governance Act, 2022).

(15) Stratégie européenne sur les données, Commission européenne, 2020.

Faciliter la circulation et la réutilisation des données de l'Internet des objets

Un nombre croissant de produits et services génèrent des données liées à leur utilisation. On estime par exemple qu'un véhicule électrique de la marque Tesla génère plusieurs téraoctets de données par jour (une grande partie de ce volume n'est pas transférée à distance, mais certaines données - et non des moindres - le sont)[16]. Grâce au développement des réseaux de communication (5G, LoRA et autres), il est maintenant courant que de tels objets transmettent des données.

Les cas d'usages sont multiples, tant dans le **secteur public** (télérelève de compteurs d'eau, suivi à distance de la consommation énergétique des bâtiments publics, remontée des places de stationnement disponibles, accompagnement post-opératoire des patients à domicile, ...) que **privé** (maintenance préventive des moteurs d'avion, suivi de flotte de véhicules de livraison et dispatching en temps réel, suivi des machines agricoles, ...).

Le potentiel de réutilisation de ces données est considérable : on pourrait imaginer par exemple qu'un propriétaire de véhicule puisse transférer les données d'entretien au garagiste de son choix, ou encore qu'une collectivité puisse faire analyser, par la startup de son choix, les données de consommation énergétique de ses bâtiments publics.

Mais trop souvent, selon la Commission européenne, l'accès et la réutilisation de ces données de l'Internet des objets est rendu difficile, parfois par les fabricants eux-mêmes de ces objets connectés.

Le Data Act vise à lever les obstacles en :

1) **obligeant les fabricants** à développer des outils pour accéder aux données générées dans le cadre de l'utilisation de l'objet,

2) en ouvrant la possibilité, **pour les utilisateurs,** d'accéder aux données et de les **partager** avec des tiers, sous leur contrôle **(le droit à la portabilité,** l'un des principes du RGPD, est étendu aux données non-personnelles), par exemple pour accéder à des services après-vente ou des services fondés sur les données.

Des espaces communs de données

Le Data Governance Act et le Data Act accompagnent aussi le développement de nouveaux modèles de partage et de gouvernance des données, comme les **espaces communs de données.** Il s'agit en fait d'offrir, aux acteurs publics et privés, une diversité d'options de partage et de sortir de l'alternative ouvert / fermé[17]. Les espaces communs de données sont le plus souvent sectoriels, comme par exemple en France *Agdatahub* qui regroupe les acteurs de la filière agricole, ou au niveau européen, *Dates* et *DSFT* pour les acteurs du tourisme.

Mais les collectivités, en France et en Europe, mettent en place, voire exploitent déjà ce qui ressemble fortement à des espaces communs de données voire s'en revendique, comme par exemple le *Climate Data Hub* de la Région Centre Val de Loire, *Rennes Urban Data Interface* (RUDI), le Data space territorial multi-sectoriel (Ekitia) ou encore *Intelligent Data Exchange* (Pays-Bas), une plateforme d'échanges de données sur les travaux routiers et de voirie (croisement de données sur les travaux prévus et les données de trafic temps réel via les opérateurs mobiles). Le Data Governance Act fournit un cadre juridique pour sécuriser la mise en place de tels espaces communs de données, notamment en indiquant les obligations qui incombent aux **intermédiaires de données[18],** qui devront faire preuve de transparence, s'enregistrer auprès de l'UE et fournir des garanties en matière d'usages des données[19].

(16) Voir à ce sujet l'enquête en 3 parties publiées par le Magazine IEEE Spectrum : "The radical scope of Tesla's data hoard", août 2022. Lecture déconseillé aux propriétaires de Tesla qui auraient le cœur sensible.
(17) Attention, cela ne signifie pas que l'obligation d'open data par défaut est caduque pour les données publiques, dans les conditions définies dans le Code des relations entre le public et l'administration.
(18) Présentation des règles concernant les intermédiaires de données en vidéo : "La stratégie européenne sur les données, épisode 3" (Simon Chignard, 2022).
(19) Les collectivités peuvent-elles prétendre au statut d'intermédiaires de données, au sens de l'UE ? A ce stade la réponse n'est pas entièrement tranchée.

L'accès aux données du secteur privé à des fins d'intérêt général

Certaines données produites par le secteur privé (ou associatif) pourraient être utiles pour concevoir, mettre en œuvre des politiques publiques et plus généralement, contribuer à l'intérêt général. Lors de la pandémie de Covid-19, des données d'opérateurs de téléphonie mobile ont été utilisées, en France et ailleurs en Europe, pour suivre les déplacements de population à l'annonce des périodes de confinement. De même, depuis quelques années, l'institut national de la statistique et des études économiques (INSEE) utilise des données anonymisées de caisses issues de la grande distribution, pour calculer une partie de l'indice des prix (la mesure officielle de l'inflation).

Il ne fait guère de doutes que des données, produites hors cadre de missions de service public, pourraient être très utiles aux acteurs publics ; mais sous quelles conditions ?

La Commission européenne a proposé un mécanisme d'accès et de réutilisation de ces données, sous le terme de partage de données business-to-government **(B2G Data Sharing).**

Faut-il obliger les entreprises à mettre à disposition leurs données à des fins d'intérêt général ?

Cette mise à disposition doit-elle être gratuite ou payante ? Les modalités pratiques du partage de données B2G ont constitué l'un des principaux sujets chauds du débat. Les représentants d'intérêt des entreprises - et en premier lieu des opérateurs de téléphonie mobile et de l'industrie automobile - souhaitaient limiter l'accès à quelques situations particulières, et laisser les mécanismes de marché s'appliquer dans la majorité des cas. Il faut dire que certaines entreprises, à l'image d'Orange ou Telefonica, commercialisent auprès des acteurs publics et privés des solutions basées sur les données anonymisées[20]. A l'inverse, plusieurs associations (dont *Open Future,* the Center for European Policy Studies et *Eurocities,* représentant les collectivités locales) ont pris publiquement position en faveur d'un cadre plus favorable aux acteurs publics.

Les cas d'accès gratuit aux données pour les acteurs publics

Le Data Act, adopté en décembre 2023, encadre les conditions du partage de données B2G. En pratique, les conditions d'accès aux données varient selon le contexte et la situation. Le seul cas où l'accès est gratuit correspond à des situations exceptionnelles de réponses à des urgences publiques.

En clair : utiliser des données pour répondre à une situation telle qu'une catastrophe naturelle, une inondation, un séisme ou un incendie. Dans ce cas-là, les acteurs publics pourront demander et obtenir un accès gratuit aux données (à condition de ne pas les partager avec des tiers, ce n'est pas de l'open data !). Le second cas de figure correspond à la prévention des situations d'urgence.

Concrètement, on peut imaginer qu'une collectivité accède à des données de flux autoroutier pour dimensionner un plan d'évacuation d'une ville. Pour ce cas de figure, les détenteurs de données sont en droit de réclamer une compensation financière. Enfin, le Data Act prévoit aussi des mécanismes quand les données sont jugées nécessaires à l'exercice d'une mission de service public - on peut penser par exemple à des données sur les montants des loyers pratiqués dans un quartier, dans le cadre d'une politique d'encadrement des dits loyers. Dans ce dernier cas de figure, ce sont les règles du marché qui s'appliquent.

L'altruisme des données : le partage volontaire au service de l'intérêt général

Le Data Governance Act entend faciliter l'altruisme des données, défini comme la mise à disposition **volontaire,** par des individus ou des organisations, de données (personnelles ou non-personnelles) à des fins d'intérêt général. Les cas d'usage pour les collectivités sont multiples, comme l'illustre l'initiative Bike Data Projet dans la région de Bruxelles : les individus qui le souhaitent sont invités à connecter leur application Strava, qui enregistre leurs déplacements à vélo, avec la plateforme. Les données ainsi collectées sont anonymisées, puis mises à disposition des acteurs du territoire - par exemple pour l'aménagement des voies cyclables, ou une meilleure compréhension des pratiques.

L'altruisme des données met clairement l'accent sur une démarche proactive de la part des individus. En ce sens, il constitue un signal positif pour un rééquilibrage des relations entre les individus et ceux qui exploitent leurs données.

Le Data Governance Act propose aux organisations qui mettent en place l'altruisme de données de s'enregistrer et de se faire connaître au niveau européen. Elles s'engagent alors à respecter des règles en matière de transparence sur leur financement, leur fonctionnement et l'usage des données qu'elles collectent. L'une des premières organisations reconnues est la plateforme DataLog qui propose aux habitants de Barcelone de partager leurs données de consommation énergétique.

La directive sur l'open data (Open data Directive, 2019) vise à mettre à jour la directive de 2003 centrée sur les informations du secteur public (Public Sector Information Directive, 2003). En pratique, depuis l'adoption de la Loi pour une République numérique, la plupart des principes posés par cette révision existaient déjà dans le droit français. L'une des principales nouveautés concerne les ensembles de données de forte valeur (high-value datasets). Similaire, dans l'esprit, aux données de référence de la Loi pour une République numérique, ces données relèvent des six thématiques suivantes : données géospatiales, observations de la Terre et de l'environnement, météorologie, statistiques, entreprises et propriétés d'entreprises, mobilité[21]. Les administrations et organisations publiques qui produisent de telles données seront tenues de les mettre à disposition librement et gratuitement par le biais d'interfaces de programmation (API).

(21) La Commission a publié en 2022 une liste détaillée des données à forte valeur.

LES AUTRES TEXTES ADOPTÉS CES 5 DERNIÈRES ANNÉES EN MATIÈRE DE NUMÉRIQUE

La présente note s'est concentrée sur les principaux textes en rapport direct avec les données et l'intelligence artificielle. Mais la commission Von der Leyen a imprimé sa marque sur d'autres textes majeurs en matière de numérique. En voici un bref résumé, ainsi qu'une sélection de liens pour en savoir plus.

La directive NIS 2

L'Union européenne a adopté une révision de la directive NIS (Network and Information Security directive) afin de faire face à l'augmentation de la menace cyber et la multiplication des attaques contre les systèmes d'information des entreprises et des administrations. NIS 2 est qualifié de changement de paradigme, dans la mesure où elle étend le périmètre des acteurs concernés et les obligations pesant sur les acteurs. Le texte doit faire l'objet d'une transposition dans le cadre d'un projet de loi attendu pour 2024. L'Agence nationale de sécurité des systèmes d'information (ANSSI) a entrepris une démarche de concertation, notamment avec les associations d'élus, pour définir le périmètre exact des entités concernées par NIS 2 (la directive européenne laissant une certaine marge de manœuvre aux États-membres) mais aussi le mode de collaboration entre ces entités et l'ANSSI. En l'état actuel des discussions, il est fort probable que la transposition de NIS 2 étende très sensiblement le nombre d'opérateurs concernés par ces nouvelles obligations en matière de cybersécurité - de quelques centaines à quelques, voire plusieurs, milliers. Les grandes villes, les agglomérations et les métropoles devraient, selon toute vraisemblance, faire partie des "entités essentielles" au sens de la directive[22].

Le Digital Services Act (DSA)

"Ce qui est illégal hors-ligne l'est aussi en-ligne" : c'est en ces termes que le commissaire européen Thierry Breton présente la philosophie du règlement sur les services numériques (DSA).

Les enjeux sont multiples : multiplication de la haine en ligne - y compris contre des candidats et des élus - , de la désinformation, manipulation et ingérence étrangère, contrefaçon de produits et services, … Les services en ligne, et en premier lieu les grandes plateformes numériques et leurs services (Meta, Google, Amazon, Microsoft, …) sont de formidables outils de communication et de mise en relation, mais ils constituent aussi le terrain privilégié des dérives individuelles et collectives. Le DSA est l'un des premiers textes européens à adopter une nouvelle approche de la régulation numérique. Le règlement vise tout particulièrement les mécanismes algorithmiques d'éditorialisation et d'amplification de contenus, et les moyens que les fournisseurs de ces services mettent en œuvre pour assurer la modération des contenus. Il définit en outre des obligations supplémentaires pour les très grandes plateformes (VLOPs - very large online platforms) qui ont plus de 45 millions d'utilisateurs par mois en Europe[23].

(22) Pour en savoir plus sur la directive NIS 2 et ses impacts pour les collectivités territoriales : "La directive NIS 2", ANSSI, 2023.
(23) Pour en savoir plus sur le DSA et les obligations qui pèsent sur plateformes en ligne : "DSA : le règlement européen sur les services numériques vise une responsabilisation des plateformes", Vie publique, août 2023.

Parlons technique : l'éditorialisation algorithmique

Depuis au moins une vingtaine d'années, le débat autour des plateformes en ligne tourne autour du statut juridique applicable à ces plateformes.

Il existe dans le droit français deux principaux statuts :

- **d'un côté le statut d'éditeur,** qui s'applique notamment à la presse et aux médias. L'éditeur est responsable juridiquement du contenu publié, car il prend notamment des décisions éditoriales (c'est-à-dire qu'il décide de ce qui sera publié ou non). En cas de conflit (par exemple un procès en diffamation), la responsabilité de l'éditeur peut-être engagée ;
- **de l'autre côté le statut d'hébergeur,** qui s'appliquait traditionnellement à la plupart des plateformes en ligne. Comme son nom l'indique, un hébergeur héberge du contenu produit par des tiers (par exemple les internautes eux-mêmes). A ce titre son niveau de responsabilité est différent, il est "juste" tenu de supprimer dans un délai raisonnable les contenus manifestement illicites et, le cas échéant, de les signaler à la justice.

Cette distinction entre éditeur et hébergeur est par exemple au cœur de la LCEN - loi pour la confiance dans l'économie numérique de 2004. Le DSA part d'un constat : les grandes plateformes ne sont ni tout à fait des éditeurs de presse (car les contenus ne sont pas nécessairement produits par la plateforme mais plutôt par les utilisateurs, ni de simples hébergeurs. En effet, toutes les plateformes ont mis en œuvre une éditorialisation algorithmique. En moyenne, un utilisateur de Facebook, X-Twitter ou LinkedIn ne voit que **10 à 15% des contenus publiés** par ceux qu'il suit en ligne ! Des algorithmes interviennent pour rendre visibles certains contenus et en invisibiliser d'autres. Dès lors, le DSA propose de s'intéresser au "cœur du réacteur", c'est-à-dire le fonctionnement de ces mécanismes algorithmiques et non aux contenus eux-mêmes.

Le Digital Market Act (DMA)

L'ambition du Digital Market Act est tout d'abord économique et part du constat que si plus de 10 000 plateformes en ligne opèrent en Europe (dont 90% sont gérées par des petites et moyennes entreprises), les grandes plateformes (dites "systémiques") captent l'essentiel de la valeur créée. Le DMA vise à adresser ce manque de concurrence entre les acteurs, et à lutter contre la position dominante des grands opérateurs, au profit des petites et moyennes entreprises.

Pour comprendre l'enjeu, on peut partir d'un exemple, celui joué par la plateforme Amazon, qui concentre à elle seule plus de 20% du marché du commerce en ligne en France (c'est le double en Allemagne). Contrairement à une idée répandue dans le grand public, Amazon vend des produits en direct, mais elle a surtout une fonction de place de marché (marketplace) qui offre une présence en ligne et un accès au marché à de très nombreux commerçants en ligne. Or le risque est grand qu'Amazon utilise cette position de "garde-barrière" (gatekeeper) ou "contrôleur d'accès" pour restreindre la concurrence, ou encore qu'elle utilise les données de vente des produits pour développer sa propre offre concurrente (car Amazon fabrique aussi ses propres produits, sous la marque Amazon Basics).

Le DMA introduit des règles pour lutter, à priori (ex-ante), contre les pratiques anti-concurrentielles des grandes plateformes[24]. En pratique, les impacts du DMA sur les collectivités sont a priori assez limités.

L'Interopérable Europe Act

Le règlement pour une Europe interopérable[25] (Interoperable Europe Act) vise à créer un nouveau cadre de coopération pour les administrations publiques au niveau européen, en facilitant l'interopérabilité des solutions déployées en matière d'administrations numériques dans les différents pays. Le règlement fixe des obligations applicables aux "services publics numériques transeuropéens" (notamment concernant l'évaluation obligatoire d'interopérabilité), crée des mécanismes de coopération entre les administrations nationales et locales en Europe, et prévoit la mise en place d'un catalogue de solutions d'interopérabilité. Le texte est encore susceptible d'évoluer - l'accord provisoire entre le Conseil, la Commission et le Parlement datant de la fin 2023. En pratique, l'Interoperable Europe Act intéressera en premier lieu les collectivités transfrontalières, qui pourrait y trouver de nouveaux leviers et moyens d'actions. Pour les autres collectivités, les enjeux apparaissent moins immédiats.

(24) Pour en savoir plus sur le Digital Market Act : "DMA : le règlement sur les marchés numériques veut mettre fin à la domination des géants du Net", Vie publique, septembre 2023.
(25) Pour en savoir plus sur l'Interoperable Europe Act "Règlement pour une Europe interopérable: le Conseil et le Parlement parviennent à un accord pour des services publics numériques plus efficaces dans l'ensemble de l'UE", Conseil de l'UE, novembre 2023.

LES PRIORITÉS DES 5 PROCHAINES ANNÉES

La période 2019-2024 a été très riche en matière de régulation du numérique. Jamais l'Europe n'avait adopté autant de textes en matière de données, de plateformes et d'intelligence artificielle. La présente note se concentre sur les principaux textes, mais le sujet du numérique est aussi présent dans bien d'autres réglementations adoptées depuis 2019, à l'image de l'accord récent sur les droits des travailleurs des plateformes.

A quoi faut-il s'attendre pour les cinq prochaines années ? Quelles sont les priorités ?

Une partie de la réponse tient bien sûr dans les résultats des élections européennes de juin 2024. Une poussée électorale des partis populistes, telle qu'elle est annoncée dans les sondages, pourrait entraîner un retour en arrière (backlash) sur un certain nombre de textes déjà adoptés, en premier lieu le Pacte vert. Mais, au-delà même des incertitudes du prochain scrutin, la plupart des observateurs s'accordent sur un point : pour la régulation du numérique, les années 2019-2024 étaient sans aucun doute une parenthèse, une période relativement unique et qui ne devrait pas se reproduire. La prochaine mandature aura avant tout pour mission de mettre en œuvre les textes adoptés au cours de ces cinq dernières années, et non d'en proposer de nouveaux.

La priorité : mettre en œuvre ces nouvelles règles

Interrogés sur les priorités des cinq prochaines années, l'ensemble des interlocuteurs rencontrés par la délégation d'élus de France Urbaine - Les Interconnectés[26] (tant au niveau de la Commission européenne que du Parlement européen) ont répondu par le même mot : **implémentation.** La priorité des cinq prochaines années c'est d'abord de "finir le travail". Car, contrairement à une idée répandue, la publication officielle d'un texte comme le règlement sur l'intelligence artificielle ne marque pas la fin de l'histoire, mais son début.

L'implémentation, c'est le passage de l'idée à l'action. C'est le moment où les textes qui ont été patiemment imaginés, discutés, négociés, vont devenir une réalité. C'est le moment aussi où l'on espère pouvoir en voir concrètement les premiers effets. Comme l'a montré le retour d'expériences du RGPD (cf. page 4) la mise en œuvre n'est jamais simple. C'est un jeu complexe qui mobilise les États-membres, les autorités de régulation de chaque pays mais aussi, de manière croissante, la Commission européenne elle-même à travers par exemple l'AI Office.

(26) Délégation d'élus de France Urbaine - Les Interconnectés à Bruxelles, les 21 et 22 mars 2024.

CONCLUSION : L'EUROPE, UNE OPPORTUNITÉ POUR LES COLLECTIVITÉS FRANÇAISES

60% à 70% de la réglementation européenne *a un impact direct au niveau local et régional. Il y a plusieurs manières de lire cette statistique.*

La première lecture *est de voir la réglementation européenne comme une source supplémentaire de normes et de contraintes, qui plus est en provenance d'un échelon (l'Union européenne) qui semble parfois trop éloigné. Pour nombre de collectivités, cela semble compliqué d'influer sur l'agenda européen. C'est sans doute vrai au niveau individuel de chaque collectivité. Mais, collectivement, les collectivités peuvent* ***faire entendre leur voix*** *si elles sont capables de s'appuyer sur des réseaux nationaux (France Urbaine, Les Interconnectés) et, à fortiori, européens (Eurocities, Conseil des Communes et des Régions d'Europe).*

Une autre lecture est possible : *les échelons locaux sont les premiers terrains d'application des nouvelles règles. En ce sens, la réglementation n'est pas seulement une contrainte, c'est aussi une opportunité car elle donne un* ***cadre d'action*** *pour les acteurs locaux.*

Prenons trois exemples concrets d'opportunités à saisir dans les prochains mois :

1 En matière d'intelligence artificielle…

Le règlement IA prévoit que les administrations publiques devront réaliser dans certains cas une **étude d'impact sur les droits fondamentaux** (cf. page 15). Le bureau pour l'intelligence artificielle (AI Office) est chargé d'aider à la mise en œuvre de cette obligation. Nul doute que les collectivités françaises pourraient légitimement apporter un point de vue et un retour d'expérience pour aider ce nouveau service de la Commission européenne dans cette tâche.

2 En matière de données…

Le Data Governance Act introduit le concept **d'altruisme de données,** que l'on peut définir comme le partage volontaire de données à des fins d'intérêt général (cf. page 20 et suivante). Les collectivités françaises pourraient se saisir de ce nouveau cadre par exemple dans le domaine de la lutte contre le changement climatique, de la santé ou des mobilités.

3 En matière de plateformes…

Le Digital Services Act introduit de nouveaux mécanismes pour mieux **lutter contre la haine en ligne** (cf. page 20 et suivante). La haine en ligne est un problème mondial, mais l'échelon local n'est pas épargné, et les élus sont parfois aussi les cibles de la haine en ligne. Les collectivités locales peuvent se rapprocher du régulateur national (en l'occurrence, l'ARCOM) pour agir ensemble.

BIBLIOGRAPHIE

Rapports et documents

"Mise en conformité AI Act : les clés pour comprendre et appliquer la loi sur l'IA" France Digitale - Wavestone, février 2024

"The EU AI Act : a summary of its significance and scope", Ada Lovelace Institute, avril 2022

Les 4 règles d'or de la régulation numérique Sébastien Soriano, 1er février 2024

"Intelligence artificielle et action publique : construire la confiance, servir la performance", Conseil d'État, août 2022

Articles de presse

"The radical scope of Tesla's Data Hoard", IEEE Spectrum, 3 août 2022

"Entre amende record et bataille en coulisses, le RGPD fête ses cinq ans sur un bilan contrasté", L'Usine digitale, 25 mai 2023

"La loi européenne obligeant les géants d'Internet à réguler leurs contenus est entrée en vigueur", Le Monde, août 2023 (sur abonnement)

"La France accepte de valider l'AI Act après sept mois d'opposition", Le Monde, 2 février 2024 (sur abonnement)

"Les coulisses de l'opposition de la France à la réglementation des modèles d'IA", Euractiv, 29 novembre 2023

"Kit de survie pour humains sur l'intelligence artificielle", Contexte, 13 avril 2023 (sur abonnement)

"Ces collectivités qui prennent le train de l'IA", dossier d'actualités La Gazette des Communes, février 2024 (sur abonnement)

"Régulation du numérique : il était une fois dans l'Ouest (de l'Europe)", Simon Chignard, La Gazette des Communes, avril 2024 (sur abonnement).

Vidéos

"La stratégie européenne pour la donnée en 3 épisodes" : *l'altruisme des données*, *le partage de données B2G*, *les intermédiaires de données*, Simon Chignard, 2022

"Présentation de la directive NIS 2" : *épisode 1* et *épisode 2*, ANSSI, 2023

"Les maîtres du monde, l'Europe face aux géants du numérique", documentaire de la RTBF, 93 minutes, 2024.

Podcasts

"ChatGPT dans le texte", Le code a changé, France Inter, 9 juin 2023

"Black box: the collision", The Guardian, mars 2024

RÉPONSE AU QUIZ

Selon vous, quel niveau de risques pour les applications suivantes de l'IA dans une collectivité ?

	Risque inacceptable (interdiction)	Application à haut-risque	Applique à risque limité ou faible	Application à risque minime ou nul	Ça dépend !
1) Un système de tri automatique des CVs pour des candidats à un poste de catégorie A		√			
2) Un système de notation des habitants en fonction de leur comportement de bons citoyens en matière de collecte et recyclage des déchets		√			
3) La création d'une image de synthèse pour illustrer le magazine de la ville			√		
4) Un système de comptage de nombre de piétons utilisant des caméras de vidéosurveillance					√
5) Un chatbot aidant les administrés dans leurs démarches administratives sur le site Internet de la Mairie			√		
6) Un outil d'aide à la rédaction de délibérations pour les agents des collectivités			√		
7) Un système analysant des images satellites pour repérer des décharges sauvages				√	
8) Un système vidéo IA permettant à la police municipale de repérer dans une foule les individus n'ayant pas payé la cantine scolaire	√				

DATA ET IA

LES NOUVELLES RÈGLES DU JEU EN EUROPE

REMERCIEMENTS ET CONTEXTE

La présente note a été rédigée par Simon Chignard à la demande, et pour le compte des Interconnectés. Elle a pour ambition d'offrir un regard critique sur les principaux textes relatifs à la donnée et l'intelligence artificielle adoptés au cours de la mandature 2019-2024 de la Commission européenne dirigée par Ursula Von der Leyen.

Le propos s'adresse en premier lieu aux collectivités et à leurs élus en charge du numérique. Ils y trouveront, outre la présentation des textes (AI Act, Data Governance Act, Data Act, ...) des clés de lecture pour comprendre l'intention du législateur, identifier les points qui font débat, mais aussi s'emparer des opportunités que ces nouvelles règles du jeu représentent pour les acteurs publics locaux.

L'auteur remercie Anthéa Serafin pour sa relecture du document.

Les interconnectés
RÉSEAU DES TERRITOIRES INNOVANTS

FRANCE URBAINE
MÉTROPOLES, AGGLOS ET GRANDES VILLES

INTERCOMMUNALITÉS DE FRANCE