EXAMEN D'ACCÈS CRFPA

SESSION 2026

Mardi 1er septembre 2026

NOTE DE SYNTHÈSE

Durée de l'épreuve : **5 heures**

Coefficient : **3**

Documents autorisés : Néant

Dès que ce sujet vous est remis, assurez-vous qu'il est complet.

Ce sujet comporte 30 pages numérotées de 1/30 à 30/30.

Extraits des recommandations de la Commission nationale à destination des jurys et des correcteurs d'épreuve, relativement à l'épreuve d'admissibilité de "Note de synthèse rédigée en cinq heures" (article 5-1° de l'arrêté du 17 octobre 2016) :

« L'épreuve est destinée à apprécier, notamment, les capacités de synthèse du candidat : la limite de quatre pages ne doit pas être dépassée.

La qualité rédactionnelle est prise en compte (les déficiences orthographiques et syntaxiques, les impropriétés de termes, l'inélégance de style, les obstacles divers à la lisibilité du texte sont sanctionnés).

Un plan apparent (avec des titres concis), dont la structuration est laissée à la libre appréciation du candidat, s'il n'est pas obligatoire, est recommandé.

La note de synthèse doit consister en une synthèse objective des éléments du dossier documentaire, et seules les informations contenues dans le dossier peuvent être utilisées. La référence au numéro du document peut s'avérer nécessaire à la bonne compréhension de la synthèse et est recommandée.

Une brève introduction est recommandée. Une conclusion n'est pas nécessaire ».

À partir des documents joints, vous établirez une note de synthèse sur le sujet suivant :

L'INTELLIGENCE ARTIFICIELLE

Liste des documents :

DOCUMENT 1 : CA Bordeaux, 2e ch., 31 janvier 2005, n° 03/05512

DOCUMENT 2 : Article 10 Loi n° 2023-380 du 19 mai 2023 *relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions* (extraits)

DOCUMENT 3 : Convention cadre du Conseil de l'Europe sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'Etat de droit, 17 mai 2024 (extraits)

DOCUMENT 4 : T. Lakssimi, "IA et philosophie du droit", *D.* 2026, p. 289

DOCUMENT 5 : Article 5 du règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 *établissant des règles harmonisées concernant l'intelligence artificielle* (extraits)

DOCUMENT 6 : Groupe de travail sur l'IA à la Cour de Cassation, "Cour de Cassation et intelligence artificielle : préparer la Cour de cassation de demain", avril 2025 (extraits)

DOCUMENT 7 : J.-B. Guyonnet, "Environnement et intelligence artificielle : *AI for Green* plutôt que *Green AI* ?", *RDI* 2025, p. 552 (extraits)

DOCUMENT 8 : K. Favro, C. Zolynski, "Quelle régulation pour les IA compagnons ? (Il est temps d'agir", *Dalloz IP/IT* 2026, p. 71 (extraits)

DOCUMENT 9 : A. Latil, "Endiguer la propagation. L'encadrement juridique des risques systémiques en matière d'intelligence artificielle", *APD* 2026, tome 66, p. 213 (extraits)

DOCUMENT 10 : Commission de l'intelligence artificielle, *IA : notre ambition pour la France,* Rapport remis à la Première ministre en mars 2024, p. 4 (extraits)

DOCUMENT 11 : G. Loiseau, « La personnalité juridique des robots, une monstruosité juridique »*, JCPG* 2018, p. 597 (extraits)

DOCUMENT 12 : Directive (UE) 2024/2853 du Parlement européen et du Conseil du 23 octobre 2024 *relative à la responsabilité du fait des produits défectueux et abrogeant la directive 85/374/CEE du Conseil* (extraits)

DOCUMENT 13 : CE, 30 janvier 2026, *Commune de Nice*, n° 506370

DOCUMENT 14 : Comité national pilote d'éthique du numérique, Avis n° 7, Systèmes d'intelligence artificielle générative : enjeux d'éthique, 30 juin 2023 (extraits)

DOCUMENT 15 : Défenseur des droits, *Algorithmes, systèmes d'IA et services publics : quels droits pour les usagers ? Points de vigilance et recommandations*, 2024 (extraits)

DOCUMENT 16 : CJUE, 27 février 2025, *Dun & Bradstreet Austria*, aff. C-203/22 (extraits)

DOCUMENT 17 : Articles 121-1, 121-2 et 121-3 du code pénal

DOCUMENT 18 : A. Seveno, « Chatbots, campagnes « augmentées »… l'IA s'immisce dans la politique française », *Le Monde*, 5 février 2026

DOCUMENT 1 : CA Bordeaux, 2e ch., 31 janvier 2005, n° 03/05512

Attendu que la S.A.S. A.T.E.V.I. soutient qu'elle a été victime d'une contrefaçon, ses plans découverts chez la S.A. Saunier bénéficiant d'une protection et sollicite de ce chef avant expertise l'allocation d'une provision de 155.000 € soit une marge brute de 30 % sur les ventes qu'elle a manquées.
Attendu qu'elle soutient qu'elle a été victime de concurrence déloyale et de parasitisme : ses plans ont été détournés, de même que ses clients, son personnel a été débauché et les produits contrefaisants ont été vendus à vil prix, elle sollicite de ce chef outre une mesure d'expertise l'allocation d'une somme de 100.000 € à titre de provision.
Attendu, sur la contrefaçon, qu'une œuvre de l'esprit même créée à partir d'un système informatique peut bénéficier des règles protégeant les droits d'auteur, à condition qu'elle laisse apparaître même de façon minime l'originalité qu'a voulu apporter son concepteur.

DOCUMENT 2 : Article 10 Loi n° 2023-380 du 19 mai 2023 *relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions* (extraits)

(Modifié par LOI n°2026-201 du 20 mars 2026 - art. 47)

I. - A titre expérimental et jusqu'au 31 décembre 2027, à la seule fin d'assurer la sécurité de manifestations sportives, récréatives ou culturelles qui, par l'ampleur de leur fréquentation ou par leurs circonstances, sont particulièrement exposées à des risques d'actes de terrorisme ou d'atteintes graves à la sécurité des personnes, les images collectées au moyen de systèmes de vidéoprotection autorisés sur le fondement de l'article L. 252-1 du code de la sécurité intérieure ou au moyen de caméras installées sur des aéronefs autorisées sur le fondement du chapitre II du titre IV du livre II du même code, dans les lieux accueillant ces manifestations et à leurs abords ainsi que dans les véhicules et les emprises de transport public et sur les voies les desservant, peuvent faire l'objet de traitements algorithmiques. Ces traitements ont pour unique objet de détecter, en temps réel, des événements prédéterminés susceptibles de présenter ou de révéler ces risques et de les signaler en vue de la mise en œuvre des mesures nécessaires par les services de la police nationale et de la gendarmerie nationale, les services d'incendie et de secours, les services de police municipale et les services internes de sécurité de la SNCF et de la Régie autonome des transports parisiens dans le cadre de leurs missions respectives. Aux seules fins de signaler ces événements aux services de la police municipale, les agents mentionnés à l'article L. 132-14-1 dudit code peuvent être autorisés à accéder aux signalements du traitement, à condition d'être placés sous la supervision permanente d'au moins un agent de la police municipale.

II. - Les traitements mentionnés au I du présent article, y compris pendant leur conception, sont régis par les dispositions applicables du 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) et de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

III. - Le public est préalablement informé, par tout moyen approprié, de l'emploi de traitements algorithmiques sur les images collectées au moyen de systèmes de vidéoprotection autorisés sur le fondement de l'article L. 252-1 du code de la sécurité intérieure et de caméras installées sur des aéronefs autorisées sur le fondement du chapitre II du titre IV du livre II du même code, sauf lorsque les circonstances l'interdisent ou que cette information entrerait en contradiction avec les objectifs poursuivis.

Une information générale du public sur l'emploi de traitements algorithmiques sur les images collectées au moyen de systèmes de vidéoprotection et de caméras installées sur des aéronefs est organisée par le ministre de l'Intérieur.

IV. - Les traitements mentionnés au I du présent article n'utilisent aucun système d'identification biométrique, ne traitent aucune donnée biométrique et ne mettent en œuvre aucune technique de reconnaissance faciale. Ils ne peuvent procéder à aucun rapprochement, à aucune interconnexion ni à aucune mise en relation automatisée avec d'autres traitements de données à caractère personnel.
Ils procèdent exclusivement à un signalement d'attention, strictement limité à l'indication du ou des événements prédéterminés qu'ils ont été programmés à détecter. Ils ne produisent aucun autre résultat et ne peuvent fonder, par eux-mêmes, aucune décision individuelle ni aucun acte de poursuite.
Ils demeurent en permanence sous le contrôle des personnes chargées de leur mise en œuvre.

<u>DOCUMENT 3</u> : Convention cadre du Conseil de l'Europe sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'Etat de droit, 17 mai 2024 (extraits)

Chapitre II – Obligations générales

Article 4 – Protection des droits de l'homme

Chaque Partie adopte ou maintient des mesures pour veiller à ce que les activités menées dans le cadre du cycle de vie des systèmes d'intelligence artificielle soient cohérentes avec les obligations de protection des droits de l'homme, telles qu'elles sont définies par le droit international applicable et par son droit interne.

Article 5 – Intégrité des processus démocratiques et respect de l'État de droit

Chaque Partie adopte ou maintient des mesures visant à garantir que les systèmes d'intelligence artificielle ne sont pas utilisés pour porter atteinte à l'intégrité, à l'indépendance et à l'efficacité des institutions et processus démocratiques, y compris au principe de la séparation des pouvoirs, au respect de l'indépendance de la justice et à l'accès à la justice.
Chaque Partie adopte ou maintient des mesures qui visent à protéger ses processus démocratiques au cours des activités menées dans le cadre du cycle de vie des systèmes d'intelligence artificielle, y compris l'accès équitable et la participation des personnes au débat public, ainsi que leur capacité à se forger librement une opinion.

Chapitre III – Principes relatifs aux activités menées dans le cadre du cycle de vie des systèmes d'intelligence artificielle

Article 6 – Approche générale

Le présent chapitre énonce les principes généraux communs que chaque Partie met en œuvre à l'égard des systèmes d'intelligence artificielle, de manière adaptée à son ordre juridique interne et aux autres obligations nées de la présente Convention.

Article 7 – Dignité humaine et autonomie personnelle

Chaque Partie adopte ou maintient des mesures en faveur du respect de la dignité humaine et de l'autonomie personnelle en ce qui concerne les activités menées dans le cadre du cycle de vie des systèmes d'intelligence artificielle.

Article 8 – Transparence et contrôle

Chaque Partie adopte ou maintient des mesures pour veiller à ce que les exigences de transparence et de contrôle adaptées aux contextes et aux risques spécifiques soient en place pour les activités menées dans le cadre du cycle de vie des systèmes d'intelligence artificielle, y compris en ce qui concerne l'identification de contenu généré par des systèmes d'intelligence artificielle.

Article 9 – Obligation de rendre des comptes et responsabilité

Chaque Partie adopte ou maintient des mesures pour garantir l'obligation de rendre des comptes et d'assumer la responsabilité pour les impacts négatifs sur les droits de l'homme, la démocratie et l'État de droit qui résultent des activités menées dans le cadre du cycle de vie des systèmes d'intelligence artificielle.

Article 10 – Égalité et non-discrimination

Chaque Partie adopte ou maintient des mesures visant à garantir le respect de l'égalité, y compris l'égalité de genre, et l'interdiction de la discrimination dans les activités menées dans le cadre du cycle de vie des systèmes d'intelligence artificielle, comme le prévoit le droit international et interne applicable.

Chaque Partie s'engage à adopter ou à maintenir des mesures visant à supprimer les inégalités dans les activités menées dans le cadre du cycle de vie des systèmes d'intelligence artificielle, afin d'obtenir des résultats impartiaux, justes et équitables, dans le cadre des obligations nationales et internationales qui lui incombent en matière de droits de l'homme.

Article 11 – Respect de la vie privée et protection des données à caractère personnel

Chaque Partie adopte ou maintient des mesures pour garantir que, en ce qui concerne les activités menées dans le cadre du cycle de vie des systèmes d'intelligence artificielle :

a) les droits à la vie privée des personnes et leurs données à caractère personnel sont protégés, notamment par les lois, normes et cadres nationaux et internationaux applicables ; et

b) des garanties et des protections effectives ont été mises en place pour les personnes, conformément aux obligations juridiques nationales et internationales applicables.

Article 12 – Fiabilité

Chaque Partie prend, le cas échéant, des mesures pour promouvoir la fiabilité des systèmes d'intelligence artificielle et la confiance en leurs résultats, ce qui pourrait inclure des exigences en matière de qualité et de sécurité adéquates tout au long du cycle de vie des systèmes d'intelligence artificielle.

Article 13 – Innovation sûre

En vue de favoriser l'innovation tout en évitant les impacts négatifs sur les droits de l'homme, la démocratie et l'État de droit, chaque Partie est appelée à permettre, le cas échéant, la mise en place d'environnements contrôlés pour le développement, l'expérimentation et l'essai de systèmes d'intelligence artificielle sous la surveillance de ses autorités compétentes.

<u>DOCUMENT 4</u> : T. Lakssimi, “IA et philosophie du droit”, *D.* 2026, p. 289

En 1804, le code civil incarnait une philosophie : un droit pensé par l'homme, pour l'homme. Mais pas n'importe quel homme : un homme libre propriétaire de biens immobiliers. Le livre I déterminait qui pouvait agir sur la scène juridique (le mari, le père, essentiellement) ; le livre II consacrait la propriété comme socle de l'ordre social ; le livre III organisait sa circulation. Cette structure, moyenâgeuse et archaïque, portait malgré tout un message philosophique puissant qui a fait la grandeur du code civil bien au-delà de nos frontières.

Deux siècles plus tard, où se trouve ce message ? Le code civil, érodé par des réformes successives et l'européanisation du droit, semble avoir perdu sa capacité à incarner une vision du monde juridique. Le droit des personnes vit désormais largement dans le règlement général sur la protection des données (RGPD), texte européen étudié tant par les publicistes que par les civilistes. Le code civil n'est plus le seul lieu où se cristallise la philosophie du droit français.

Cette migration révèle une absence : celle d'une réflexion sur le message que doit porter notre droit à l'ère de l'intelligence artificielle (IA). Car si le code civil de 1804 a marqué l'histoire, ce n'est pas tant par la plume de ses rédacteurs ou l'intelligence de son agencement - largement emprunté aux Institutes de Gaïus - que par la vision qu'il incarnait. Un code n'est grand que s'il porte un projet de société.

Aujourd'hui, on multiplie les réflexions sur les cas d'usage de l'IA, la protection des droits de l'homme face aux algorithmes, le contrôle du juge sur les décisions automatisées. Ces préoccupations sont nécessaires. Mais elles occultent l'essentiel : quelle place donnons-nous à l'IA dans notre philosophie du droit ?

La bonne nouvelle est que la France s'est fortement investie dans l'évolution des modèles d'IA à adopter, notamment en matière de justice, avec une sensibilité affirmée aux enjeux de souveraineté numérique. Mais cet investissement doit s'accompagner d'une ambition plus haute : mettre à l'épreuve nos principes ancestraux face à l'IA, à l'heure où l'état de droit est remis en cause par certains. Qu'est-ce que la justice ? Quelles institutions pour déterminer ce qui est juste ? Et quelle place pour l'IA dans cette détermination ?

Ces questions convoquent des interrogations concrètes sur les personnes qui élaborent les algorithmes et leur fonctionnement. Contrairement à une idée reçue, tout n'est pas « boîte noire » dans l'IA. Une simple IA de résumé ou de comparaison de documents repose sur des mécanismes que l'on contrôle parfaitement. Ces choix - quelles données d'entraînement, quels critères de pertinence - ne sont jamais neutres. Ils incarnent déjà une certaine conception de ce qui est pertinent, de ce qui fait sens juridiquement.

En 1804, on n'a pas seulement réglementé la propriété : on a pensé le type de société que cette réglementation devait servir. En 2026, alors que l'IA redéfinit les frontières entre l'humain et la machine, entre la décision et l'algorithme, nous devons retrouver cette ambition.

Notre tradition civiliste nous a appris à penser le droit comme un système cohérent porteur de sens. Revenir aux sources et à cette capacité d'incarner une philosophie du droit dans des

textes fondateurs constitue la condition pour que le droit français demeure un modèle. L'IA doit trouver sa place dans une vision d'ensemble du droit, au même titre que la propriété en 1804. C'est à ce prix que nous pourrons prétendre avoir su penser notre époque, et non simplement la subir.

<u>DOCUMENT 5</u> : Article 5 du règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 *établissant des règles harmonisées concernant l'intelligence artificielle* (extraits)

Article 5
Pratiques interdites en matière d'IA

1. Les pratiques en matière d'IA suivantes sont interdites :
a) la mise sur le marché, la mise en service ou l'utilisation d'un système d'IA qui a recours à des techniques subliminales, au-dessous du seuil de conscience d'une personne, ou à des techniques délibérément manipulatrices ou trompeuses, avec pour objectif ou effet d'altérer substantiellement le comportement d'une personne ou d'un groupe de personnes en portant considérablement atteinte à leur capacité à prendre une décision éclairée, amenant ainsi la personne à prendre une décision qu'elle n'aurait pas prise autrement, d'une manière qui cause ou est raisonnablement susceptible de causer un préjudice important à cette personne, à une autre personne ou à un groupe de personnes ;

b) la mise sur le marché, la mise en service ou l'utilisation d'un système d'IA qui exploite les éventuelles vulnérabilités dues à l'âge, au handicap ou à la situation sociale ou économique spécifique d'une personne physique ou d'un groupe de personnes donné avec pour objectif ou effet d'altérer substantiellement le comportement de cette personne ou d'un membre de ce groupe d'une manière qui cause ou est raisonnablement susceptible de causer un préjudice important à cette personne ou à un tiers ;

c) la mise sur le marché, la mise en service ou l'utilisation de systèmes d'IA pour l'évaluation ou la classification de personnes physiques ou de groupes de personnes au cours d'une période donnée en fonction de leur comportement social ou de caractéristiques personnelles ou de personnalité connues, déduites ou prédites, la note sociale conduisant à l'une ou l'autre des situations suivantes, ou aux deux :

i) le traitement préjudiciable ou défavorable de certaines personnes physiques ou de groupes de personnes dans des contextes sociaux dissociés du contexte dans lequel les données ont été générées ou collectées à l'origine ;

ii) le traitement préjudiciable ou défavorable de certaines personnes ou de groupes de personnes, qui est injustifié ou disproportionné par rapport à leur comportement social ou à la gravité de celui-ci ;

d) la mise sur le marché, la mise en service à cette fin spécifique ou l'utilisation d'un système d'IA pour mener des évaluations des risques des personnes physiques visant à évaluer ou à prédire le risque qu'une personne physique commette une infraction pénale, uniquement sur la base du profilage d'une personne physique ou de l'évaluation de ses traits de personnalité ou caractéristiques; cette interdiction ne s'applique pas aux systèmes d'IA utilisés pour étayer l'évaluation humaine de l'implication d'une personne dans une activité criminelle, qui est déjà fondée sur des faits objectifs et vérifiables, directement liés à une activité criminelle ;

e) la mise sur le marché, la mise en service à cette fin spécifique ou l'utilisation de systèmes d'IA qui créent ou développent des bases de données de reconnaissance faciale par le moissonnage non ciblé d'images faciales provenant de l'internet ou de la vidéosurveillance ;

f) la mise sur le marché, la mise en service à cette fin spécifique ou l'utilisation de systèmes d'IA pour inférer les émotions d'une personne physique sur le lieu de travail et dans les établissements d'enseignement, sauf lorsque l'utilisation du système d'IA est destinée à être mise en place ou mise sur le marché pour des raisons médicales ou de sécurité ;

g) la mise sur le marché, la mise en service à cette fin spécifique ou l'utilisation de systèmes de catégorisation biométrique qui catégorisent individuellement les personnes physiques sur la base de leurs données biométriques afin d'arriver à des déductions ou des inférences concernant leur race, leurs opinions politiques, leur affiliation à une organisation syndicale, leurs convictions religieuses ou philosophiques, leur vie sexuelle ou leur orientation sexuelle; cette interdiction ne couvre pas l'étiquetage ou le filtrage d'ensembles de données biométriques acquis légalement, tels que des images, fondés sur des données biométriques ou la catégorisation de données biométriques dans le domaine répressif ;

h) l'utilisation de systèmes d'identification biométrique à distance en temps réel dans des espaces accessibles au public à des fins répressives, sauf si et dans la mesure où cette utilisation est strictement nécessaire eu égard à l'un des objectifs suivants :

i) la recherche ciblée de victimes spécifiques d'enlèvement, de la traite ou de l'exploitation sexuelle d'êtres humains, ainsi que la recherche de personnes disparues;

ii) la prévention d'une menace spécifique, substantielle et imminente pour la vie ou la sécurité physique de personnes physiques ou d'une menace réelle et actuelle ou réelle et prévisible d'attaque terroriste ;

iii) la localisation ou l'identification d'une personne soupçonnée d'avoir commis une infraction pénale, aux fins de mener une enquête pénale, d'engager des poursuites ou d'exécuter une sanction pénale pour des infractions visées à l'annexe II et punissables dans l'État membre concerné d'une peine ou d'une mesure de sûreté privatives de liberté d'une durée maximale d'au moins quatre ans.

<u>DOCUMENT 6</u> : Groupe de travail sur l'IA à la Cour de Cassation, "Cour de Cassation et intelligence artificielle : préparer la Cour de cassation de demain", avril 2025 (extraits)

5 – La mise en exergue de principes directeurs pour développer une IA judiciaire

Les réflexions menées au sein du groupe de travail ont permis de prendre la mesure des enjeux du développement de l'IA, au sein de la Cour, comme pour l'ensemble de l'institution judiciaire.

Bien que la réflexion du groupe de travail ait été centrée sur les cas d'usage pour les besoins propres de la Cour, plusieurs de ceux dont il a été préconisé le développement intéressent l'ensemble des juridictions. Ainsi, l'usage des SIA documentaires de recherche dans les bases de données interne et externe, comme les SIA d'analyse de données jurisprudentielles massives ont vocation à être accessibles aux magistrats des juridictions du fond. De même, les cas d'usage d'aide à la rédaction pourraient aboutir à la création de technologies utilisables ensuite pour l'élaboration d'outils adaptés aux besoins des juridictions du fond.

Le groupe de travail a été convaincu des potentialités qu'offre d'ores et déjà l'IA, potentialités qui devraient être décuplées à l'avenir tant les progrès sont rapides.

Le développement de l'IA constitue ainsi une opportunité à saisir, non seulement pour gagner en efficacité, à l'heure où l'institution est confrontée à une crise de moyens sans précédent,

puisque l'IA est en capacité de réaliser en quelques secondes des tâches chronophages et sans réelle valeur ajoutée quand elles sont assurées par l'humain, mais encore pour gagner en qualité. Ce gain de qualité est particulièrement évident, par exemple, s'il s'agit de repérer, dans une grande masse de données, des questions nouvelles et/ou sérielles ou de détecter des divergences de jurisprudence. De telles recherches, qui ne sont pas réalisables raisonnablement sans l'assistance de l'IA, permettraient notamment aux juridictions de rationaliser et de mieux coordonner le traitement des contentieux émergents et d'enrichir le débat juridique et le dialogue des juges.
Cependant, le groupe de travail estime que l'engagement dans la voie de l'IA est conditionné à la réalisation de prérequis sur les plans de la technique, de l'éthique et de la gouvernance.
En premier lieu et sur le plan technique, le groupe de travail souligne l'interaction très forte qui existe entre les projets d'IA et le bénéfice d'un système d'information solide, fiable, centré sur les besoins des utilisateurs et prenant en considération des objectifs de bonne structuration et conservation des données utiles. Par ailleurs, la question de l'hébergement des services et de la puissance de calcul doit répondre à des impératifs de souveraineté. La maîtrise directe de l'hébergement, soit sur les serveurs de la Cour de cassation, soit sur des clouds obéissant à des exigences de sécurité et de territorialité pour s'inscrire dans le droit applicable à l'Union européenne, permet de garantir l'indépendance des juridictions dans leur fonctionnement, la sécurité des données et la transparence de leur utilisation.
En deuxième lieu, le groupe de travail entend insister sur la primauté des principes directeurs éthiques.
En effet, le respect du RGPD et du RIA, pour essentiel qu'il soit, et bien qu'il contribue à protéger les droits fondamentaux, ne suffit pas à garantir un usage de l'IA vertueux, qui préserve la plénitude de l'office du juge et ne vienne pas amoindrir ou fragiliser les équilibres fondamentaux du procès équitable. Le groupe de travail insiste sur la nécessité, en complément des impératifs de conformité juridique, de prendre ainsi en considération des principes éthiques relevant de l'impact sur la fonction de juger, de l'impact sur les droits fondamentaux, comme de la transparence, de l'éthique et de la frugalité des algorithmes.
A cet égard, le groupe de travail considère que la Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires de la CEPEJ, adoptée en décembre 2018, demeure un document de référence ayant conservé toute son actualité malgré les évolutions techniques majeures intervenues depuis. Le groupe de travail a pris en compte les cinq principes dégagés par la charte de respect des droits fondamentaux, de non-discrimination, de qualité et sécurité des algorithmes, de transparence et d'explicabilité ainsi que de maîtrise humaine des décisions. Ce dernier principe est essentiel pour conserver intact l'office du juge. Sa mise en œuvre impose de toujours conserver une intervention humaine dans les différentes étapes du processus décisionnel, depuis l'analyse du dossier jusqu'à la rédaction de la décision, le recours à l'IA n'intervenant que pour apporter une aide ponctuelle et toujours à la demande et sous le contrôle du magistrat. Les critères éthiques, qui s'appuient sur les droits humains comme sur des considérations épistémologiques, déontologiques ou sociales, constituent, selon le groupe de travail, des principes directeurs ou cardinaux, qui précédent et priment les autres critères fonctionnels, juridiques, techniques et économiques. Ils doivent dicter le choix des outils d'IA à retenir, mais aussi accompagner leur développement et guider les juges dans leur utilisation, ce qui pose la question de la gouvernance des IA judiciaires.

<u>DOCUMENT 7</u> : **J.-B. Guyonnet, "Environnement et intelligence artificielle : *AI for Green* plutôt que *Green AI* ?", *RDI* 2025, p. 552 (extraits)**

Le déploiement de l'IA en faveur de l'environnement (*AI for Green*)
Dans le cadre du Green Deal, les institutions européennes soutiennent très clairement le déploiement de l'IA comme une solution pertinente et centrale pour répondre aux enjeux

environnementaux. Le règlement sur l'IA porte la marque de cette orientation, faisant de la protection de l'environnement un motif d'allègement des obligations et contraintes juridiques. Cette orientation repose toutefois sur le véritable angle mort de la prise en compte des risques environnementaux liés aux réponses apportées par le système d'IA en lui-même.

Un motif d'allégement des obligations et contraintes juridiques

Le règlement sur l'IA retranscrit l'orientation retenue plus largement dans le Green Deal d'une IA conçue comme moyen privilégié d'atteindre les objectifs de décarbonation. Au-delà du règlement sur l'IA, l'Union européenne favorise ainsi le déploiement des systèmes d'IA en matière environnementale. Dans différents secteurs, l'Union européenne soutient par exemple le déploiement de l'IA en lien avec l'environnement au travers de programmes de recherche, ou en invitant les États membres à « *tirer parti des possibilités offertes par l'intelligence artificielle* » dans la mise en place de systèmes de surveillance environnementale. À ce titre, le déploiement de l'IA en matière environnementale se heurte à des freins persistants. Ainsi que l'indique la Commission européenne dans la Stratégie pour l'application de l'IA, « *le potentiel de l'IA en matière d'action pour le climat et l'environnement reste inexploité, en raison de la complexité scientifique et technique de la modélisation climatique et environnementale fondée sur l'IA, conjuguée à des déficits persistants de capacités et de compétences parmi les autorités locales, les PME et la société civile* ». Elle ajoute que « *la fragmentation de l'écosystème des outils, des ensembles de données et des services d'IA liés au climat et à l'environnement aggrave encore ces défis* ».

Ces observations convergent toutes vers des difficultés qui se situent en amont du système d'IA et tiennent à la capacité à générer et gérer des données environnementales de nature à assurer l'efficacité et la pertinence du système d'IA. À plusieurs titres, les « données environnementales » ou liées à l'environnement et à sa protection soulèvent des problématiques spécifiques. Notamment, les données peuvent se heurter tant à un processus de collecte divisé qu'à d'autres intérêts, mais aussi à des réticences à les collecter, les transmettre et les diffuser largement. La question a pu par exemple se poser de la place du consentement des agriculteurs à la mise en place de systèmes de collecte de données permettant la transition vers une agriculture de précision. De manière générale, le *Data Governance Act* envisage en ce sens un « *altruisme en matière de données* » pour favoriser le partage volontaire de données moyennant compensation des coûts supportés pour des objectifs d'intérêt général tels que « *les soins de santé, la lutte contre le changement climatique, l'amélioration de la mobilité* ». L'initiative *Green Data4All* vise en outre à renforcer le partage et l'exploitation des données environnementales en envisageant une refonte de la directive « INSPIRE ».

À deux endroits, le règlement sur l'IA cherche par ailleurs à favoriser le déploiement de l'IA dans le sens d'une finalité favorable à l'environnement. D'une part, l'article 46 permet à une autorité de surveillance de marché de déroger à la procédure d'évaluation de la conformité prévue par l'article 43 pour les systèmes d'IA à haut risque « pour des raisons exceptionnelles de sécurité publique ou pour assurer la protection de la vie et de la santé humaines, la protection de l'environnement ou la protection d'actifs industriels et d'infrastructures d'importance majeure » et ainsi autoriser leur mise sur le marché ou leur mise en service sur le territoire de l'État membre concerné, pendant une période limitée. Ici, la protection de l'environnement apparaît donc comme la justification d'une procédure temporairement allégée. D'autre part, en vertu des articles 57 et suivants du règlement, il est prévu de soutenir l'innovation notamment par la mise en place d'au moins un bac à sable réglementaire au niveau national au plus tard le 2 août 2026. Or, dans ce cadre, l'article 59 prévoit que les données collectées légalement à d'autres fins peuvent être traitées en vue du développement, de l'entraînement et de la mise à l'essai de certains systèmes d'IA dans le bac à sable, notamment lorsque les systèmes d'IA sont développés pour préserver des intérêts publics importants dans des domaines parmi lesquels « *un niveau élevé de protection et d'amélioration*

de la qualité de l'environnement, la protection de la biodiversité, la protection contre la pollution, les mesures de transition écologique et les mesures d'atténuation du changement climatique et d'adaptation à celui-ci », ou encore la « *durabilité énergétique* ».

On peut s'interroger sur la pertinence de l'allègement des obligations procédurales et contraintes juridiques prévu par le règlement sur l'IA. Si l'article 46 trouve une justification dans des « raisons exceptionnelles », il conduit à un abaissement de la surveillance aux conséquences bien incertaines en faisant échapper le système à toute évaluation de sa conformité, qu'il s'agisse du système de gestion de la qualité garantissant le respect du présent règlement ou de la documentation technique. Or, en vertu de l'article 17, le système de gestion de la qualité comprend notamment « *la gestion des ressources, y compris les mesures liées à la sécurité d'approvisionnement* ». De même, l'article 59 revient à déroger aux principes prévus par le règlement général sur la protection des données (RGPD), qu'il s'agisse de la minimisation des données ou du principe de finalité. En ce sens, ces deux dispositions organisent une perte de maîtrise des impacts environnementaux, eu égard aux incertitudes qui résulteraient de leur mise en œuvre quant à leur coût énergétique notamment, à des fins environnementales, ce qui semble à tout le moins paradoxal. Le paquet « Omnibus IA », qui cherche à alléger les règles du RGPD pour les mettre en accord avec le règlement sur l'IA, ne devrait pas arranger ce constat. C'est ainsi l'angle mort des risques environnementaux liés à l'IA qui semble particulièrement problématique dans ce règlement.

<u>DOCUMENT 8</u> : K. Favro, C. Zolynski, "Quelle régulation pour les IA compagnons ? (Il est temps d'agir)", *Dalloz IP/IT* 2026, p. 71 (extraits)

Les premiers cas de suicide largement relayés par la presse ont conduit à une prise de conscience brutale du grand public. En réaction aux actions intentées aux États-Unis à la suite du décès de Sewell Setzer et d'Adam Raine, des premiers textes de lois issus du législateur américain tant au niveau fédéral qu'étatique se sont saisis de la problématique propre aux IA compagnons. Leur synthèse conduit à proposer la définition suivante : le terme IA compagnon désigne un système d'IA doté d'une interface en langage naturel qui fournit des réponses aux entrées de l'utilisateur personnalisées, semblables à celles d'un être humain et en lien avec ses besoins sociaux, qui sont conçues pour encourager et faciliter la simulation d'une interaction interpersonnelle ou émotionnelle, en présentant des caractéristiques anthropomorphiques et pouvant entretenir une relation prolongée tenant compte des multiples interactions.

Ce type d'interactions peut désormais résulter d'une diversité de services proposant différentes interactions, fonctionnalités et contextes possibles. Peuvent en effet relever de cette catégorie : des services spécialisés d'amis virtuels, comme Replika ou Character AI ; des agents conversationnels généralistes pouvant être utilisés comme tels, à l'image de ChatGPT ; différentes fonctionnalités nouvelles ou *patchs* qui s'ajoutent à des services numériques comme les réseaux ou médias sociaux. Leur déploiement concerne désormais bon nombre de secteurs, à l'image des jeux vidéo pour animer un personnage non joueur, jusqu'aux jouets pour enfants. Les IA compagnons s'immiscent très rapidement dans le quotidien d'une grande masse d'utilisateurs, en particulier les plus jeunes suscitant des préoccupations grandissantes.

Il semble dès lors urgent de se saisir de ces nouveaux enjeux compte tenu des risques qu'ils peuvent comporter. Cela conduit à envisager ce qu'on a fait ou ce que l'on peut faire en l'état

de la régulation (I). D'importantes limites en résultent qui nous invitent à nous demander ce que l'on doit faire pour saisir les enjeux identifiés (II).
[...]
B - Des solutions largement inadaptées et insuffisantes
État des lieux. Ces préoccupations paraissent désormais partagées par les pouvoirs publics. On a vu récemment émerger le sujet dans le cadre de l'élaboration des lignes directrices. Celles relatives à l'article 5 du règlement sur l'intelligence artificielle (RIA) concernant les usages interdits évoquent l'exemple des IA compagnons et illustrent les cas possibles d'application de l'article 5 § 1, b) s'agissant des personnes vulnérables. Tel est également le cas des lignes directrices de juillet 2025 concernant l'article 28 du *Digital Services Act* (DSA) qui impose aux plateformes accessibles aux mineurs de garantir un haut niveau de protection de leur vie privée, de leur sûreté et de leur sécurité. Cela vient s'ajouter aux premières décisions prises sur le fondement du règlement général sur la protection des données (RGPD).
L'apport limité du RIA. Si cette prise de conscience doit être saluée, les enjeux évoqués conduisent toutefois à formuler d'importants regrets au regard de la portée de ces différents textes. S'agissant du RIA, les agents conversationnels figurent par principe dans la catégorie des risques « acceptables ». Leurs usages ne sont soumis qu'à une simple obligation de transparence minimale pour permettre aux personnes humaines de reconnaître une interaction avec les systèmes d'IA, conformément à l'article 50 § 1 du RIA. On sait pourtant que cette transparence ne suffit pas à écarter les risques de tromperie et de manipulation résultant notamment des projections anthropomorphiques. Cette obligation d'information paraît en outre largement insuffisante compte tenu des effets délétères des IA compagnons précédemment mentionnés. On pourrait alors envisager d'inscrire les IA compagnons dans la liste des usages interdits définie par l'article 5 du RIA. À ce titre, et alors que l'on peut regretter la portée limitée de l'interdiction de la reconnaissance émotionnelle, il s'agit d'envisager l'application de l'article 5 § 1, b) visant l'exploitation préjudiciable de certaines formes de vulnérabilité. Il est vrai que les lignes directrices relatives à l'interprétation de ce texte, publiées en février 2025, citent en exemple ce type de service. Un doute subsiste toutefois sur l'application de cette interdiction dès lors que les exigences probatoires requises par le texte pour interdire l'usage d'un système d'IA au nom du risque inacceptable qu'il comporte pour la sécurité et les droits humains sont particulièrement élevées. Cela laisse craindre une interdiction difficilement mobilisable, d'autant plus qu'il existe de forts enjeux en termes d'innovation en ce domaine.

Il est alors envisageable de se tourner vers l'application du Règlement sur les services numériques (DSA), dont on observe ici encore plusieurs limites. La seule mention des IA compagnons dans les lignes directrices de l'article 28 manque clairement d'envergure en ce qu'elles ne visent que les utilisateurs mineurs, et surtout dans la mesure où les différentes mesures évoquées restent très superficielles et ne sont pas à la hauteur des enjeux, notamment lorsque ces fonctionnalités viennent s'ajouter aux comptes de réseaux sociaux proposés en particulier aux mineurs. L'application du DSA à des services d'IA généralistes comme ChatGPT - qui est actuellement discutée - pourrait en particulier être intéressante dès lors qu'elle permettrait de responsabiliser les très grands fournisseurs en les soumettant aux différentes obligations imposées par le texte. Songeons tout particulièrement à l'analyse des risques systémiques des articles 34 et 35 complétés de l'accès aux données de l'article 40. Dans le même temps, cela pourrait poser plusieurs difficultés qu'il est important d'anticiper, notamment relatives à l'application du régime de responsabilité allégée, alors que l'impact des usages des IA compagnons invite plutôt à considérer un renforcement de l'obligation de

sécurité qu'il conviendrait de reconnaître à l'égard de leur fournisseur en instaurant une obligation de résultat quant à la conception de leurs services.

Au-delà, on perçoit avec les IA compagnons toute la difficulté à saisir des services qui n'existaient pas lors de l'adoption de ces textes et les effets de silotage pouvant résulter de leur application distributive en fonction du service visé, sans cohérence d'ensemble. Il faut regretter l'absence de message clair adressé à l'égard d'un modèle possiblement toxique susceptible de prendre différentes formes.

Fort de ce constat, quelle solution préconiser ? La tentation est grande de consacrer une définition de laquelle découleraient une qualification et un régime juridique. Cela pourrait s'avérer inefficient compte tenu de l'évolution rapide des usages et du risque d'obsolescence d'un texte lié à des retours d'expérience. Telle est la critique que l'on peut adresser aux propositions portées aux États-Unis par l'État fédéral et les textes adoptés en Californie et dans l'État de New York qui ne visent que les risques observés dans les affaires récentes et ne prônent aucunement l'approche globale nécessaire à l'identification des possibles effets domino. Le risque de ne pas pouvoir saisir l'usage de l'IA serait trop important pour que cette qualification soit efficace notamment à l'égard des IA généralistes.

S'il n'est pas primordial de poser la définition juridique des IA compagnons, il est indispensable de bloquer l'évolution d'un modèle d'affaires possiblement toxique, en particulier en s'attelant frontalement à l'ensemble des effets de la publicité ciblée pour proposer son interdiction. Cela permettrait par la même occasion d'appréhender toutes les manipulations de l'utilisateur valorisant son engagement lequel est, dans le cadre des IA compagnons, particulièrement utilisé et amplifié. Il faudrait alors se saisir plus fermement du cœur du problème, à savoir la conception du système. Cela n'a pas été suffisamment fait pour les réseaux sociaux et l'on en voit aujourd'hui les terribles conséquences ; il suffit ici d'évoquer les difficultés rencontrées pour bloquer les effets « spirale » de contenus toxiques en dépit de leur possible impact, notamment sur la santé mentale et physique des plus jeunes utilisateurs. Il y a bien urgence à agir en ce sens, d'autant que ces effets pourraient être considérablement décuplés avec l'usage des IA compagnons. Un mode opératoire adapté doit être proposé à cette fin.

<u>DOCUMENT 9</u> : A. Latil, "Endiguer la propagation. L'encadrement juridique des risques systémiques en matière d'intelligence artificielle", *APD* 2026, tome 66, p. 213 (extraits)

Trois niveaux de gouvernance des risques systémiques doivent être distingués : organisationnel, régulatoire et judiciaire. Chacun de ces trois niveaux soulève des enjeux distincts. Endiguer les propagations implique cependant une bonne articulation entre ces trois strates.

Gouvernance interne et collective des organisations. Le niveau organisationnel correspond d'abord aux modalités de gestion des risques au sein des organisations (entreprises, administrations, associations, etc.). Il est étroitement lié aux obligations de compliance analysées plus haut. Un des principaux objectifs de ces obligations consiste en effet à préparer les organisations à la gestion de crise, à travers notamment des obligations de cartographie des risques, la mise en place d'un plan de continuité des organisations, etc. Mais la gouvernance des organisations ne saurait toutefois être seulement interne : il existe aussi une forme d'organisation collective de la gestion des risques. Plusieurs organisations mettent alors en commun des ressources afin de lutter collectivement contre les risques. Le

secteur de la cybersécurité constitue à cet égard un modèle avec la création des centres de réponse à un incident (les CSIRT, de l'anglais *Computer Security Incident Response Team*), en particulier lorsqu'ils sont dits « sectoriels », c'est-à-dire destinés à l'ensemble des acteurs d'un secteur donné.
Une telle gouvernance collective des risques de l'intelligence artificielle demeure pour l'instant inexistante. Mais il est possible de l'imaginer. Ainsi, par exemple, les organisations de la presse et des médias pourraient mettre en commun des ressources afin de déjouer les risques informationnels liés à l'intelligence artificielle. Le caractère sectoriel de telles organisations semble particulièrement pertinent dans la mesure où l'analyse et la remédiation des risques en matière d'intelligence artificielle restent aujourd'hui très coûteuses en matière d'expertise.

Autorités de régulation de l'intelligence artificielle. La mise en place d'autorités de régulation, dont la mission consiste notamment à freiner la propagation des risques, constitue le deuxième étage de la gouvernance. Au niveau de l'Union européenne, le RIA a institué plusieurs organes compétents en matière d'intelligence artificielle : le Bureau européen de l'intelligence artificielle (art. 64), le Comité de l'intelligence artificielle (art. 65), le Forum consultatif (art. 66) et le Groupe scientifique d'experts indépendants (art. 67). Ces organes ne disposent cependant pas de pouvoirs d'injonction et d'action propres en matière de risques systémiques, autres que de guider la mise en place des mesures organisationnelles de gestion des risques (notamment à travers la publication du chapitre sur la *safety and security* du code de bonnes pratiques dans le cadre du l'*AI Pact*). Au niveau national, les autorités de régulation sont investies du pouvoir de surveillance de marché et de contrôle des systèmes d'intelligence artificielle (art. 74 et suivants). Les entités contrôlées doivent leur signaler les incidents graves (art. 73). Les autorités nationales doivent alors prendre toutes mesures qui s'imposent dans un délai de sept jours (art. 73 al. 8).

Gestion de crises. Aucune structure ne dispose cependant pour l'instant de pouvoirs ou prérogatives comparables au réseau EU-CyCLONe en matière de cybersécurité, ou encore au Haut conseil de stabilité financière et l'*European Systemic Risk Board* en matière financière. Aucune disposition similaire à celles adoptées sur le plan sanitaire en matière la lutte contre la propagation des maladies n'est non plus prévue en matière d'I.A. Les structures dont les missions se rapprochent le plus de la gestion des risques systémiques sont les *AI Safety Institutes*. En France, sur le modèle de l'ANSES, l'INESIA (Institut national pour l'évaluation et la sécurité de l'I.A.), créé en 2024, a en effet pour mission d'évaluer la sécurité de l'I.A. Cet organisme constitue en réalité un agrégat d'agences étatiques et d'organismes de recherche (ANSSI, INRIA, LNE, PEReN). Au niveau européen, ce rôle est dévolu en particulier au panel scientifique du Bureau de l'I.A.. Dans tous les cas, il s'agit d'éclairer la décision publique plutôt que d'agir par des mesures d'urgence afin d'endiguer les risques systémiques.

Autorités juridictionnelles. Freiner la propagation des risques systémiques passe naturellement aussi par la voie juridictionnelle, comme c'est le cas par exemple pour le juge administratif avec les circonstances exceptionnelles, qui ont par exemple justifié la restriction de l'accès au réseau social TikTok en Nouvelle-Calédonie en mai 2024. Sur ce terrain non plus le droit de l'intelligence artificielle ne connaît pas de mécanismes propres. Il reste que les mesures du droit commun de l'urgence doivent pouvoir s'y appliquer.
Enfin, plutôt que de multiplier les mesures sectorielles de prévention et de gestion des risques systémiques, il serait pertinent de développer les expertises d'une manière transversale, à travers par exemple la création d'une organisation chapeau destinées à diffuser les bonnes pratiques et les alertes.

<u>DOCUMENT 10</u> : Commission de l'intelligence artificielle, *IA : notre ambition pour la France,* Rapport remis à la Première ministre en mars 2024, p. 4 (extraits)

SYNTHÈSE GÉNÉRALE, NOTRE VISION ET NOS RECOMMANDATIONS CLÉS

L'intelligence artificielle est une révolution technologique incontournable. L'émergence soudaine et la diffusion de l'IA générative marquent une étape importante de cette révolution. Nous ne pouvons que constater la simplicité d'utilisation de certains outils, la rapidité de la génération du contenu, le réalisme des textes, images et sons générés, et plus généralement les aptitudes des récents modèles d'IA.

Cette révolution technologique affecte tous les domaines d'activité. Elle a des effets sur l'économie, l'emploi, les services publics, l'environnement, l'information, le secteur culturel… Tous les pans de notre société sont concernés et le seront davantage à l'avenir, tant son potentiel est considérable.

L'IA ne doit susciter ni excès de pessimisme, ni excès d'optimisme : nous n'anticipons ni chômage de masse, ni accélération automatique de la croissance. Dans les prochaines années, l'IA ne remplacera pas l'humain, de même qu'elle ne sera pas la solution à tous les défis de notre temps. Nous ne devons ni surestimer l'impact à très court terme, ni le sous-estimer à long terme.

L'Europe et la France ont des atouts pour être des acteurs de cette révolution, en premier lieu du fait de l'excellence de nos talents. Cette richesse et le dynamisme exceptionnel de l'écosystème français dans l'IA ne doivent néanmoins pas masquer une réalité préoccupante.

Depuis plusieurs décennies, la tendance est celle d'un déclassement technologique et économique de notre continent, qui hypothèque sa prospérité et son indépendance.

Alors que les États-Unis et la Chine ont fait de la maîtrise de l'IA l'un des piliers de leur stratégie de puissance, nous devons relever le défi de l'IA, faute de quoi nous n'aurons pas la maîtrise de notre avenir. Il faut réformer nos institutions et nos politiques publiques, pour que l'IA puisse être pleinement un facteur de progrès.

Nous proposons six grandes lignes d'action :
 lancer immédiatement un plan de sensibilisation et de formation de la nation : animation de débats publics en continu sur les impacts économiques et sociétaux de l'IA au plus près des lieux du quotidien, structuration de l'offre de formation d'enseignement supérieur, massification de la formation continue aux outils d'IA, intégration de l'IA comme objet et outil du dialogue social ;
 réorienter structurellement l'épargne vers l'innovation et créer, à court terme, un fonds « France & IA » de 10 Md€, pour financer l'émergence de l'écosystème d'IA et la transformation du tissu économique français ;
 faire de la France un pôle majeur de la puissance de calcul : approvisionnement collectif sécurisé d'ampleur nationale et européenne, appel à projets d'implantation de centres de calcul avec garantie publique d'utilisation et simplification des procédures, crédit d'impôt IA pour l'entraînement de modèles ;

 faciliter l'accès aux données : en matière de données à caractère personnel, modernisation du mandat de la Commission nationale de l'informatique et des libertés (Cnil) et de son collège, suppression de certaines procédures d'autorisation préalable d'accès aux données de santé et réduction des délais de réponse ; en matière culturelle, mise en place de l'infrastructure technique favorisant l'entraînement des modèles d'IA dans le respect des droits de propriété intellectuelle ;
 assumer le principe d'une « exception IA » dans la recherche publique : libération des chercheurs des contraintes administratives, revalorisation de leur rémunération, doublement des moyens de la recherche publique spécialisée en IA ;
 promouvoir une gouvernance mondiale de l'IA : création d'une Organisation mondiale de l'IA pour évaluer et encadrer les systèmes d'IA, d'un Fonds international pour l'IA au service de l'intérêt général et d'un mécanisme de solidarité « 1 % IA » pour les pays en voie de développement.

Une mobilisation collective, massive, sans délai et au long cours est impérative. C'est dans cette perspective que notre Commission s'est attachée à élaborer un plan d'action aussi ambitieux que réaliste, au service des personnes, de nos besoins, de nos valeurs et de nos principes. Le plan représente un investissement public annuel de 5 Md€ pendant cinq ans. Il comprend des investissements technologiques mais aussi des investissements pour catalyser à la fois la diffusion de l'IA dans l'économie, son déploiement au service des citoyens et une appropriation et formation de toute la société.

Cet investissement est significatif mais il est nécessaire pour faire de la France un pays à la pointe dans l'intelligence artificielle et pour que notre société en tire tous les bénéfices. Cette ambition est atteignable, étant donné les atouts de la France et de l'Europe. Elle est également réaliste et accessible pour notre pays : le « plan IA » que nous proposons représenterait 0,3 % des dépenses publiques totales. Le coût de l'inaction serait, à l'inverse, très élevé. Nous renoncerions à des gains économiques et sociaux importants, et risquerions un déclassement historique. Il s'agit donc de choisir les dépenses qui permettront à la France d'assurer la maîtrise de son avenir.

<u>DOCUMENT 11</u> : G. Loiseau, « La personnalité juridique des robots, une monstruosité juridique »*, JCPG* 2018, p. 597

[...] Le 16 février 2017, le Parlement européen adoptait une résolution « contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique ». Ce texte comporte plusieurs propositions parmi lesquelles celle de reconnaître « la création, à terme, d'une personnalité juridique spécifique aux robots, pour qu'au moins les robots autonomes les plus sophistiqués puissent être considérés comme des personnes électroniques responsables, tenus de réparer tout dommage causé à un tiers ». La proposition est soutenue, en France, par quelques juristes qui verraient bien une personne robot prendre place dans l'ordre juridique. Mais elle fait aussi réagir, notamment plus de 200 spécialistes en intelligence artificielle issus de différents États de l'Union européenne qui ont adressé au mois d'avril dernier une lettre ouverte à la Commission européenne afin de s'opposer à la création d'une personnalité juridique pour les robots. La réplique en dit long sur les craintes que soulève le projet et le sérieux avec lequel il faut l'envisager. Il n'y aurait rien de plus dangereux que de le prendre à la légère – on voit pourtant certains sourire à l'évocation d'une idée fantaisiste ou

fictionnelle – car ceux qui le défendent sont des idéologues tenaces (et) en position d'être écoutés.

Impulsivement, l'idée d'une personnalité juridique procède d'une représentation des robots autonomes comme des créatures susceptibles d'agir, voire de se comporter, comme des personnes. C'est d'ailleurs la fonction des machines intelligentes d'être en capacité de réaliser des actions qui sont en principe exécutées par les humains. Créatures intelligentes et, le cas échéant, auto-apprenantes, les robots relèveraient en cela davantage de l'ordre des personnes que de celui des choses. Bien sûr, on nous assure que la personnalité juridique des robots ne serait que fonctionnelle et sans le moindre rapport avec celle des personnes humaines. C'est d'une personnalité technique qu'il s'agit, dans l'optique de régler des questions pratiques comme la responsabilité des dommages causés par les robots. N'est-elle pas ainsi décrite dans le texte adopté par le Parlement européen comme une personnalité « électronique » ? Nous avons déjà entendu pareil discours. C'est le discours de ceux qui défendent la reconnaissance d'une personnalité juridique aux animaux. Or, il y a en réalité, sous le propos qui se veut rassurant, une ambition mimétique de faire évoluer la condition animale sur le modèle de droits garantissant le respect de l'humain. Objecterait-on que le droit positif n'a pas bougé en ce sens, n'oublions pas que les personnes morales sont, quant à elles, effectivement parvenues à accéder à une situation juridique équivalente à celle des personnes humaines alors que c'est leur personnalité technique qui est prise en exemple pour en doter les robots.

Ouvrons alors les yeux : le projet d'une personnalité juridique des robots est celui de la conception d'un monstre (1) dont on ne peut attendre que des troubles graves dans l'ordre juridique et social (2).

1. La conception d'un monstre

Instituer un sujet de droit – puisque c'est là l'effet de l'attribution de la personnalité juridique – suppose d'identifier précisément l'entité élevée à la condition de personne. La difficulté commence par savoir de quoi on parle car le terme de robot est une appellation commode pour désigner toutes sortes de technologies faisant appel à l'intelligence artificielle. Celle-ci est cependant protéiforme et, si l'on peut raisonnablement penser qu'un algorithme ne peut être une personne, la perception de ce qui est susceptible d'être ainsi qualifié devient rapidement floue. Ce sujet de droit serait de surcroît institué avec une malformation juridique : celle d'être aussi un objet de droit. Aussi, avant de forcer la rationalité du droit, il faut s'interroger sur l'utilité de l'entreprise. Et l'on se convainc alors de l'inutilité de trafiquer l'appareil normatif.

A. – Quelle créature ?

Une chose est de lancer l'idée de « la création (…) d'une personnalité juridique spécifique aux robots », au moins s'agissant des « robots autonomes les plus sophistiqués ». La suggestion est cependant bien vague quant aux critères à appliquer. Serait-ce la corporéité comme le sous-tend l'emploi du terme de robot qui, dans l'esprit des auteurs de la résolution, renvoie à « l'existence d'une enveloppe physique, même réduite » ? Faut-il privilégier l'autonomie, mais à partir de quel degré de sophistication ?

Il ne s'agit pas de moquer le caractère approximatif ou immature de la proposition. L'attribution de la personnalité est, de manière générale, un choix de politique juridique. Des entités peuvent en être dépourvues malgré leur rôle économique ou social, comme les groupes de sociétés. Il faut en conséquence rationnellement peser les raisons et, corrélativement, déterminer les critères justifiant de reconnaître la personnalité juridique à certains types d'entités et pas à d'autres. Or, il ne fait pas vraiment de sens de considérer que la corporéité ou l'incorporéité de l'intelligence artificielle serait un critère sélectif de l'éligibilité à la personnalité juridique. L'autonomie ou le degré de capacités cognitives pourrait être une considération plus pertinente ; mais sa relativité ne permet pas d'en faire une donnée fiable pour décider de ce qui est ou n'est pas une personne juridique compte tenu, qui plus est, de l'évolution technologique.

Il n'y a là cependant rien d'insurmontable – pourrait-on rétorquer. On est en revanche plus perplexe face à une créature qui, attributaire de la personnalité juridique, serait un sujet de droit sans cesser a priori d'être un objet de droit. Le transformisme de la chose robot en personne robot ne ferait pas disparaître la propriété dont le robot est l'objet. Et, à moins de détraquer le droit, seule une chose peut être objet de droit. Il faut dès lors se rendre à l'évidence : la personnification des robots dérèglerait le construit juridique en donnant vie à une chimère, mi-personne mi-chose, qui pervertirait la summa divisio des personnes et des choses et l'ordre de valeur qui lui correspond. La summa divisio n'aurait-elle plus la radicalité qu'on lui prêtait ? Si l'on peut concevoir qu'un existant ne soit, ni une personne sujet de droit, ni une chose objet de droit – Carbonnier avait cette belle formule en évoquant à propos de l'enfant à naître un non-sujet de droit – il est plus difficile d'appréhender la mixité d'une entité qui serait à la fois sujet de droit et objet de droit. On pourrait tenter de contourner l'écueil en énonçant, un peu à la manière de l'article 515-17 du Code civil en ce qui concerne les animaux, que, sous réserve des droits dont ils sont investis, les robots sont soumis au régime des biens. Mais, sous le maquillage, le droit grimace à faire coexister l'incompatible que sont le statut de sujet de droit et celui d'objet de droit. Et pour quel profit, au demeurant ?

B. – Pour quelle utilité ?

Les promoteurs d'une personnalité juridique attribuée aux robots mettent en avant l'avantage qu'il y aurait en matière de responsabilité à ce que ces derniers supportent eux-mêmes la réparation des dommages qu'ils sont susceptibles de causer. Cette présentation suggère deux choses : l'une est que les régimes de responsabilité du droit positif actuel ne sont pas ou sont mal adaptés à la prise en charge de ces dommages ; l'autre est qu'un régime faisant peser directement la responsabilité sur la personne robot serait plus efficace ou répondrait mieux aux nouvelles situations à traiter. Rien, pourtant, ne vient accréditer ces deux points de vue. D'une part, la responsabilité du fait des produits défectueux constitue une base juridique éprouvée pour indemniser les dommages causés par des objets intelligents. Certes, ces objets ne sont pas des produits ordinaires et il faudra tenir compte, notamment pour la détermination de l'origine du défaut, du caractère complexe du bien agrégeant des éléments incorporels et le cas échéant corporels, éléments dont la production fait intervenir différents professionnels, du fabricant du robot aux concepteurs d'algorithmes et de programmes. Mais il n'y a là rien de vraiment nouveau. La conception large du producteur – qu'il s'agisse du fabricant du produit fini ou du fabricant d'une partie composante – et la responsabilité solidaire du fabricant de la partie composante et de celui qui en réalise l'intégration dans le produit pourvoient au traitement de la responsabilité sans qu'il soit besoin d'autres règles. Et si la preuve du lien de

causalité entre le défaut et le dommage sera probablement rendue plus délicate par l'autonomie de certaines machines intelligentes et leur capacité d'auto-apprentissage, la difficulté n'appelle pas non plus d'ajustements nouveaux et pourra être réglée en admettant la preuve du lien de causalité par des présomptions graves, précises et concordantes.

La responsabilité de droit commun du fait des choses pourrait être sollicitée en complément, en particulier lorsque le dommage est le résultat de l'action d'une machine non défectueuse. Il peut être le fait d'un robot en mouvement, entrant en contact avec une personne ou une chose, ou résulter du fonctionnement anormal d'un système intelligent. La responsabilité sera alors celle du gardien – propriétaire, utilisateur – investi des pouvoirs d'usage, de direction et de contrôle. De ce dernier point de vue, le contrôle est certainement compatible avec l'autonomie du système intelligent et sa capacité d'auto-apprentissage. Si des prises de décision automatique non-maîtrisées par l'utilisateur peuvent survenir dans l'exécution des tâches, elles n'excluent pas le contrôle au besoin largement entendu comme la capacité d'arrêter le fonctionnement de la machine. Quant à leur imprévisibilité, elle ne suffirait pas pour retenir la force majeure.

Bref, il n'y a aucune raison de s'inquiéter d'une impropriété du droit de la responsabilité à couvrir la réparation de dommages causés par des technologies intelligentes, incarnées ou incorporelles. Et l'on se demande bien, d'autre part, quelle plus-value attendre d'une responsabilité personnelle et autonome du robot pris en qualité de personne juridique. Si toute personne dispose d'un patrimoine, il faudrait en l'occurrence abonder celui de la personne robot pour l'exécution de la dette de réparation, ce qui ne ferait que reporter le poids de la dette sur : le fabricant, le propriétaire, l'utilisateur ? Le recours à l'assurance s'imposerait rapidement mais quel intérêt il y aurait alors à souscrire une assurance de personne plutôt qu'une assurance de chose ? L'inconvénient est en revanche visible car la responsabilité perdrait son effet prophylactique si le fabriquant ne devait plus assumer le risque de responsabilité qui serait transféré à la personne robot. En responsabilisant les robots, on déresponsabiliserait les fabricants et concepteurs de programmes alors que la sécurisation des objets intelligents et la réduction des risques de dommages est l'affaire de ces derniers. Question de sécurité, soyons d'ailleurs certains que l'on peut plus sûrement compter sur des normes imposées aux fabricants, aux concepteurs de programmes, voire aux utilisateurs de robots qu'en programmant des devoirs dont ces derniers seraient personnellement débiteurs.

Dans ce contexte, les prétendues insuffisances des règles du droit positif ne sont qu'un prétexte, un alibi de pacotille, pour servir une proposition en réalité idéologique : faire accéder les robots à une catégorie – celle des personnes – que le droit situe dans une hiérarchie par rapport à la catégorie des choses. On ne peut se défaire de l'idée que ce qui est convoité, sous couvert d'une personnalité technique, c'est la valeur symbolique du statut de personne et la prise en considération du rôle social que les robots seront probablement, pour certains, appelés à jouer. [...]

<u>DOCUMENT 12</u> : Directive (UE) 2024/2853 du Parlement européen et du Conseil du 23 octobre 2024 *relative à la responsabilité du fait des produits défectueux et abrogeant la directive 85/374/CEE du Conseil* (extraits)

Article 4

Définitions

Aux fins de la présente directive, on entend par :

1), « produit »: tout meuble, même s'il est incorporé dans un autre meuble ou dans un immeuble ou interconnecté avec celui-ci ; le terme comprend l'électricité, les fichiers de fabrication numériques, les matières premières et les logiciels ; [...]

Article 7

Défectuosité

1. Un produit est considéré comme défectueux lorsqu'il n'offre pas la sécurité à laquelle une personne peut légitimement s'attendre ou qui est requise par le droit de l'Union ou le droit national.

2. Pour évaluer la défectuosité d'un produit, toutes les circonstances doivent être prises en compte, y compris :

a) la présentation et les caractéristiques du produit, y compris son étiquetage, sa conception, ses caractéristiques techniques, sa composition, son emballage et les instructions d'assemblage, d'installation, d'utilisation et d'entretien ;

b) l'utilisation raisonnablement prévisible du produit ;

c) l'effet sur le produit de toute capacité à poursuivre son apprentissage ou à acquérir de nouvelles caractéristiques après sa mise sur le marché ou sa mise en service ;

d) l'effet raisonnablement prévisible sur le produit d'autres produits dont on peut s'attendre à ce qu'ils soient utilisés conjointement avec le produit, notamment au moyen d'interconnexion ;

e) le moment où le produit a été mis sur le marché ou mis en service ou, lorsque le fabricant conserve le contrôle du produit après ce moment, le moment où le produit a quitté le contrôle du fabricant ;

f) les exigences pertinentes en matière de sécurité des produits, y compris les exigences de cybersécurité pertinentes pour la sécurité ; [...]

Article 10

Charge de la preuve

1. Les États membres veillent à ce que le demandeur soit tenu de prouver la défectuosité du produit, le dommage subi et le lien de causalité entre cette défectuosité et ce dommage.

2. La défectuosité du produit est présumée lorsque l'une des conditions suivantes est remplie:

a) le défendeur ne divulgue pas les éléments de preuve pertinents conformément à l'article 9, paragraphe 1 ;

b) le demandeur démontre que le produit n'est pas conforme aux exigences obligatoires en matière de sécurité des produits prévues par le droit de l'Union

ou le droit national qui sont destinées à protéger contre le risque de survenance du dommage subi par la personne lésée ; ou

c) le demandeur démontre que le dommage a été causé par un dysfonctionnement manifeste du produit lors d'une utilisation raisonnablement prévisible ou dans des circonstances ordinaires.

3. Le lien de causalité entre la défectuosité du produit et le dommage est présumé lorsqu'il a été établi que le produit est défectueux et que le dommage causé est d'une nature généralement compatible avec le défaut en question.

4. Une juridiction nationale présume la défectuosité du produit ou le lien de causalité entre la défectuosité du produit et le dommage, ou les deux, lorsque, malgré la production d'éléments de preuve conformément à l'article 9 et compte tenu de toutes les circonstances pertinentes du cas d'espèce :

a) le demandeur fait face à des difficultés excessives, notamment en raison de la complexité technique ou scientifique, pour prouver la défectuosité du produit ou le lien de causalité entre cette défectuosité et le dommage, ou les deux ; et

b), le demandeur démontre qu'il est probable que le produit est défectueux ou qu'il existe un lien de causalité entre la défectuosité du produit et le dommage, ou les deux.

[...]

Article 11

Exonération de responsabilité

1. Un opérateur économique visé à l'article 8 n'est pas responsable du dommage causé par un produit défectueux s'il prouve l'une des situations suivantes :

[...]

c), qu'il est probable que la défectuosité ayant causé le dommage n'existait pas au moment de la mise sur le marché, de la mise en service ou, dans le cas d'un distributeur, de la mise à disposition sur le marché du produit, ou que cette défectuosité est apparue après ce moment ;

[...]

2. Par dérogation au paragraphe 1, point c), un opérateur économique n'est pas exonéré de responsabilité lorsque la défectuosité d'un produit est due à l'un des éléments suivants, à condition qu'il soit sous le contrôle du fabricant :

a) un service connexe ;
b) des logiciels, y compris des mises à jour ou mises à niveau logicielles ;
c) une absence de mises à jour ou de mises à niveau logicielles nécessaires au maintien de la sécurité ;
d) une modification substantielle du produit.

<u>DOCUMENT 13</u> : CE, 30 janvier 2026, *Commune de Nice*, n°506370

Considérant ce qui suit :

1. A la suite d'un contrôle effectué le 5 avril 2023 dans les locaux de la commune de Nice, la présidente de la Commission nationale de l'informatique et des libertés (CNIL) a mis en

demeure cette commune le 13 novembre 2024, sur le fondement de l'article 20 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, de lui remettre une analyse d'impact relative à la protection des données (AIPD) sur les traitements algorithmiques d'images de vidéosurveillance dénommés " franchissement de ligne " et " zone d'intrusion ", et de saisir la Commission pour avis sur ces projets de traitement en application de l'article 90 de la même loi. Par sa délibération n° 2025-032 du 15 mai 2025 portant avis sur les conditions de mise en œuvre de ces traitements, la CNIL a estimé, aux points 9 à 13 de cet avis, que la mise en œuvre du traitement algorithmique de données à caractère personnel dénommé " zone intrusion entrées des écoles " n'était pas permise en l'état actuel de la législation. Dans cette mesure, la commune de Nice demande l'annulation pour excès de pouvoir de cette délibération.
[...]
Sur la légalité interne :

5. Aux termes de l'article L. 251-1 du code de la sécurité intérieure : " Les systèmes de vidéoprotection remplissant les conditions fixées à l'article L. 251-2 sont des traitements de données à caractère personnel régis par le présent titre, par le 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) et par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. " Aux termes de l'article L. 251-2 du même code : " Des systèmes de vidéoprotection peuvent être mis en œuvre sur la voie publique par les autorités publiques compétentes aux fins d'assurer : / 1° La protection des bâtiments et installations publics et de leurs abords ; / (...) / 4° La constatation des infractions aux règles de la circulation ; / 5° La prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés à des risques d'agression (...) / 6° La prévention d'actes de terrorisme, dans les conditions prévues au chapitre III du titre II du présent livre ; / (...) ".

6. Il ressort des pièces du dossier que le traitement de données à caractère personnel dénommé " zone d'intrusion entrées des écoles " consiste, d'une part, à détecter en temps réel, de manière continue et automatisée, au moyen d'un algorithme, dans les images issues d'un système de vidéosurveillance des voies publiques mis en œuvre en application des dispositions précitées de l'article L. 251-2 du code de la sécurité intérieure, la présence de véhicules stationnant irrégulièrement devant les entrées des écoles pendant leurs horaires d'ouverture et, d'autre part, à alerter, par le même moyen, les services de police municipale de la survenance d'un tel événement, dans le but de prévenir des troubles à l'ordre public et, en particulier, d'assurer la sécurité de ces établissements.

7. Contrairement à ce que soutient la commune, les dispositions précitées de l'article L. 251- 2 du code de la sécurité intérieure, si elles permettent la mise en œuvre de systèmes de vidéosurveillance des voies publiques, ne sauraient, dans leur silence, être interprétées comme autorisant la mise en œuvre de traitements algorithmiques permettant une analyse systématique et automatisée des images collectées dans des espaces publics au moyen de tels systèmes. Aucune autre disposition n'autorise, par ailleurs, la mise en œuvre de tels traitements. Par suite, et alors même que le traitement envisagé ne serait, ainsi que le soutient la commune, pas qualifiable de système d'intelligence artificielle (IA) à " haut risque " au sens de l'article 6 du règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle, la CNIL a pu, sans commettre d'erreur droit ni excéder sa compétence, estimer qu'il ne pouvait être mis en œuvre en l'état actuel de la législation nationale.

8. Il résulte de tout ce qui précède que la commune de Nice n'est pas fondée à demander l'annulation de la délibération de la CNIL qu'elle attaque. Sa requête doit ainsi être rejetée, y compris ses conclusions tendant à l'application des dispositions de l'article L. 761-1 du code de justice administrative.

<u>DOCUMENT 14</u> : Comité national pilote d'éthique du numérique, Avis n° 7, *Systèmes d'intelligence artificielle générative : enjeux d'éthique*, 30 juin 2023 (extraits)

3.4. PROJECTION DE QUALITÉS HUMAINES

Le simple fait de manier le langage, qui est le moyen de la pensée consciente et du jugement, provoque une projection de traits humains sur la machine. Cette projection ne permet pas de délester la charge morale des mots, en séparant complètement le langage généré des significations, associations et jugements. Implicites dans le langage, les significations littérales des mots surgissent spontanément dans nos têtes. Se soustraire à ces projections immédiates de sens exige un entraînement particulier que tous les utilisateurs n'ont pas. Le sens qu'on attribue au langage généré ne relève que d'une projection à partir de dialogues entre les êtres humains, mais elles suffisent pour attribuer à la machine une intention et des connaissances.

On peut distinguer, entre autres, trois types de transfert entre les êtres humains et les LLM. Le premier relève de la projection de connaissances : à la suite de son apprentissage, un modèle de langue paraît « savoir » beaucoup de choses. Les « connaissances » d'un LLM ne sont que des illusions, mais l'utilisateur croit que la machine les possède réellement. Le deuxième type de transfert est celui des états émotionnels et des affects.

À travers le contenu généré, la machine peut induire chez l'utilisateur une impression qu'elle possède des émotions ou des états d'âme, même si l'utilisateur sait qu'il s'agit d'un programme informatique. Le troisième type de transfert est celui des qualités morales. Qu'un système d'IA générative soit perçu comme « bienveillant », « attentionné » ou « donneur de leçons », ces perceptions n'existent qu'au travers des projections. Le LLM ne devient en aucun cas un agent moral, ni une personne au sens juridique du terme.

Or, les projections de qualités morales peuvent aller loin, jusqu'à attribuer une responsabilité à une machine qui ne peut, par son essence, en porter aucune.

Le CNPEN souhaite rappeler certains arguments exprimés dans son avis sur les enjeux éthiques des agents conversationnels en les étendant à l'utilisation des LLM. « Les agents conversationnels sont de plus en plus intégrés dans différents aspects de la vie humaine. Leur utilisation soulève des tensions éthiques, ce qui pose la question de la responsabilité au sens de la réglementation comme au sens de la philosophie morale. La question de la responsabilité est posée dans toutes ses formes : responsabilité légale et morale, individuelle et collective, celle du concepteur, du fabricant, de l'utilisateur et du décideur politique, celle relative aux éventuels dysfonctionnements et celle liée aux conséquences de ces technologies à long terme. »

Les projections d'états de connaissance sur les systèmes d'IA peuvent présenter des avantages pratiques, tels que faciliter un dialogue ou donner l'impression de posséder une base solide pour des conseils médicaux. Cependant, ils peuvent également causer des dommages, par exemple, lorsque le chatbot fournit une information erronée ou lorsqu'il suggère une action nuisible à l'utilisateur. De plus, ils peuvent tromper les utilisateurs inexpérimentés ou mal préparés. Étant donné que l'anthropomorphisme peut survenir même si l'utilisateur est conscient que le texte provient d'une machine, la responsabilité est – et doit être – du ressort des êtres humains car la machine n'est pas un agent moral et ne doit en aucun cas être considérée comme une personne. La responsabilité est ainsi partagée entre l'utilisateur et les acteurs tout au long de la chaîne de valeurs du produit. Ce partage s'effectue au cas par cas, en fonction des aspects techniques et de l'implication de chaque partie prenante dans chacune des situations qui provoquent des tensions éthiques.

PRÉCONISATION C7 : RÉDUIRE LA PROJECTION DES QUALITÉS HUMAINES SUR LES SYSTÈMES D'IA GÉNÉRATIVE

Pour réduire la projection spontanée des qualités humaines sur les systèmes d'IA générative et l'attribution d'une intériorité aux modèles de fondation, le fournisseur des modèles doit mettre en œuvre des mécanismes de contrôle et de filtrage spécifiques. Il doit également informer l'utilisateur des biais éventuels de l'anthropomorphisation.

<u>DOCUMENT 15</u> : Défenseur des droits, *Algorithmes, systèmes d'IA et services publics : quels droits pour les usagers ? Points de vigilance et recommandations*, 2024 (extraits)

L'intervention humaine au moment de prendre, sur la base du résultat d'algorithmes ou de systèmes d'IA, la décision administrative individuelle.

Aujourd'hui, le droit en vigueur distingue deux types de décisions administratives individuelles selon leur degré d'automatisation ou d'automaticité :

- D'une part, les décisions administratives individuelles partiellement automatisées : c'est-à-dire des décisions dans lesquelles un algorithme ou un système d'IA est intervenu à un moment donné, pour une finalité précise, mais où le résultat de ces systèmes n'a été qu'un élément dans la prise de décision, qui a pris en compte d'autres dimensions. L'intervention humaine est notamment requise lorsque le traitement de données personnelles mobilisé contient des données sensibles au sens du RGPD, d'où l'importance que le périmètre de ce qui relève ou non de cette catégorie soit clair.

  > Par exemple, pour déterminer le montant attribué de la prestation de compensation du handicap (PCH), gérée par un département.

- D'autre part, les décisions administratives individuelles entièrement automatisées : c'est-à-dire les décisions qui sont prises par l'administration mais sans autre considération que le seul résultat de l'algorithme ou du système d'IA, qui à lui seul constitue la décision. Il n'y a donc pas, ici, d'intervention humaine au moment de la

prise de décision individuelle. Pour autant, la décision reste bien juridiquement celle de l'administration ou de la collectivité.

> Par exemple, le calcul de la somme à payer au titre de l'impôt sur le revenu. Le critère de répartition entre ces deux catégories de décision est l'intervention humaine. Pour être qualifiée comme telle, elle doit être consistante et avoir une influence réelle sur le résultat.

L'intervention humaine obligatoire en cas de recours administratif contre la décision individuelle.

En cas de recours administratif contre une décision individuelle (au sens des articles L. 410-1 et suivants du CRPA), une intervention humaine est requise. Ce recours appelle une attention particulière de la part de l'administration.

Ce type d'intervention ne concerne donc pas un traitement « de masse » et, au regard des garanties déjà prévues au titre Ier du livre IV du CRPA, n'appelle pas à ce stade d'observations particulières.

2. La substance de l'intervention humaine au moment de la prise de décision individuelle – recommandations pour la garantir

Pour caractériser une décision administrative individuelle comme seulement partiellement automatisée, l'intervention humaine ne peut se limiter à un « simple geste symbolique ». Cette intervention peut en particulier se traduire par l'exigence d'une étape supplémentaire : l'agent effectue une action positive, concrète et significative à partir ou à côté du résultat généré par l'algorithme. L'agent peut par exemple se voir confier la même tâche que l'algorithme, et doit ensuite, en cas de résultat différent (ex : calcul, identification), arbitrer entre les deux résultats celui qu'il convient de retenir.

Ainsi, le fait qu'un agent applique de façon systématique, par exemple en appuyant sur un bouton « valider », les résultats générés par l'algorithme ou le système d'IA, sans opération intellectuelle de vérification, ne saurait être considéré comme une intervention humaine de nature à faire de cette décision une décision partiellement automatisée. Il y a près de dix ans, le Conseil d'État insistait déjà sur la nécessité d'éviter que « les systèmes présentés comme relevant de "l'aide à la décision" soient en réalité presque toujours suivis et commandent la décision, l'intervention humaine n'étant alors qu'apparente ». Une marge de manœuvre significative du côté des agents est donc requise pour considérer que le traitement automatisé n'a qu'une place partielle dans la prise de décision.

<u>DOCUMENT 16</u> : CJUE, 27 février 2025, *Dun & Bradstreet Austria*, aff. C-203/22 (extraits)

16 CK s'est vu refuser, par un opérateur de téléphonie mobile, la conclusion ou la prolongation d'un contrat de téléphonie mobile, qui aurait impliqué le paiement mensuel d'une somme de dix euros, au motif que, selon une évaluation de son crédit par voie automatisée, à laquelle a procédé D & B, elle ne présentait pas une solvabilité financière suffisante.

17 CK a saisi l'autorité autrichienne de protection des données, laquelle a enjoint à D & B de communiquer à CK des informations utiles sur la logique sous-jacente à la prise de décision automatisée fondée sur les données à caractère personnel relatives à CK.

18 D & B a formé un recours contre la décision de cette autorité [...] en faisant valoir, en substance, que, en raison d'un secret d'affaires protégé, elle n'avait pas à communiquer à CK d'informations supplémentaires [...].

[...]

55 En particulier, dans le contexte spécifique de l'adoption d'une décision fondée exclusivement sur un traitement automatisé, la finalité principale du droit de la personne concernée à obtenir les informations prévues à l'article 15, paragraphe 1, sous h), du RGPD consiste à lui permettre d'exercer de manière efficace les droits qui lui sont reconnus par l'article 22, paragraphe 3, de ce règlement, à savoir celui d'exprimer son point de vue sur cette décision et celui de contester celle-ci.

56 En effet, si les personnes affectées par une décision automatisée, y compris un profilage, n'étaient pas en mesure de comprendre les raisons ayant conduit à cette décision avant d'exprimer leur point de vue ou de contester celle-ci, ces droits ne sauraient [...] pleinement remplir leur finalité de protéger ces personnes contre les risques particuliers pour leurs droits et libertés que présente le traitement automatisé de leurs données à caractère personnel.

57 [...] il y a donc lieu de considérer que l'article 15, paragraphe 1, sous h), du RGPD offre à la personne concernée un véritable droit à l'explication sur le fonctionnement du mécanisme qui sous-tend une prise de décision automatisée dont cette personne a fait l'objet et sur le résultat auquel cette décision a abouti.

58 [...] le droit d'obtenir des « informations utiles concernant la logique sous-jacente » à une prise de décision automatisée [...] doit être compris comme un droit à l'explication de la procédure et des principes concrètement appliqués pour exploiter, par la voie automatisée, les données à caractère personnel de la personne concernée aux fins d'en obtenir un résultat déterminé, tel un profil de solvabilité. [...]

59 Ne saurait satisfaire à ces exigences ni la simple communication d'une formule mathématique complexe, telle qu'un algorithme, ni la description détaillée de toutes les étapes d'une prise de décision automatisée, dans la mesure où aucune de ces modalités ne constituerait une explication suffisamment concise et compréhensible.

61 Ainsi, les « informations utiles concernant la logique sous-jacente » à une prise de décision automatisée [...] doivent décrire la procédure et les principes concrètement appliqués de telle manière que la personne concernée puisse comprendre lesquelles de ses données à caractère personnel ont été utilisées de quelle manière lors de la prise de décision automatisée en cause, sans que la complexité des opérations à réaliser [...] puisse libérer le responsable de traitement de son devoir d'explication.

Par ces motifs, la Cour dit pour droit :
1) L'article 15, paragraphe 1, sous h), du RGPD [...] doit être interprété en ce sens que : en cas de prise de décision automatisée, y compris un profilage [...], la personne concernée peut exiger du responsable du traitement [...] que celui-ci lui explique, au moyen d'informations pertinentes et d'une façon concise, transparente, compréhensible et aisément accessible, la

procédure et les principes concrètement appliqués pour exploiter, par la voie automatisée, les données à caractère personnel relatives à cette personne aux fins d'en obtenir un résultat déterminé, tel un profil de solvabilité.

2) [...] dans l'hypothèse où le responsable du traitement considère que les informations à fournir [...] comportent des données de tiers [...] ou des secrets d'affaires [...], ce responsable est tenu de communiquer ces informations prétendument protégées à l'autorité de contrôle ou à la juridiction compétentes, auxquelles il incombe de pondérer les droits et les intérêts en cause aux fins de déterminer l'étendue du droit d'accès de la personne concernée [...].

DOCUMENT 17 : Articles 121-1, 121-2 et 121-3 du code pénal

Article 121-1

Nul n'est responsable pénalement que de son propre fait.

Article 121-2

Les personnes morales, à l'exclusion de l'État, sont responsables pénalement [...] des infractions commises, pour leur compte, par leurs organes ou représentants. [...]

La responsabilité pénale des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits [...]

Article 121-3

Il n'y a point de crime ou de délit sans intention de le commettre.

Toutefois, lorsque la loi le prévoit, il y a délit en cas de mise en danger délibérée de la personne d'autrui.

Il y a également délit, lorsque la loi le prévoit, en cas de faute d'imprudence, de négligence ou de manquement à une obligation de prudence ou de sécurité prévue par la loi ou le règlement [...]

DOCUMENT 18 : A. Seveno, « Chatbots, campagnes « augmentées »… l'IA s'immisce dans la politique française », *Le Monde*, 5 février 2026 (extraits)

Mohamed Tlamsi, candidat à la tête d'une liste Europe Egalité Ecologie pour les municipales des 15 et 22 mars à Périgny-sur-Yerres (Val-de-Marne), a entièrement réalisé ses affiches de campagne avec l'intelligence artificielle (IA). Et il l'assume. Sur son compte Instagram, quelques internautes critiquent la démarche en raison de son impact écologique. Le jeune homme se défend : *« L'enjeu* (…) *est de mettre l'intelligence, humaine comme artificielle, au service de l'intérêt général. »*

Il n'est pas le seul à penser ainsi. Le 7 janvier, le parti Renaissance annonçait investir dans le déploiement d'une stratégie numérique s'appuyant sur l'IA, avec, en ligne de mire, la présidentielle de 2027. Un directeur chargé d'un pôle *«* technologies et innovations » a été

nommé : Victor Cohen, ancien responsable des outils numériques du parti. Renaissance a d'ores et déjà conclu un accord avec une entreprise spécialisée dans l'intelligence artificielle, dont il refuse de communiquer le nom.

Dès juin 2024, Reconquête ! s'était aussi emparé de l'outil, à l'occasion des législatives anticipées. Le président du parti d'extrême droite, Eric Zemmour, se vantait alors sur X d'avoir créé la *« première vidéo de politique française entièrement réalisée par l'intelligence artificielle »*. Les images ainsi générées illustrent ses obsessions : immigration, sécurité et déclin économique. Dans une enquête publiée le 4 juillet 2024, les chercheurs de l'ONG AIForensics relevaient que l'usage de l'IA générative lors de la campagne des législatives était très largement le fait des partis d'extrême droite.

Stratégie militante

Quelques mois plus tard, l'IA semble s'être généralisée. Défendant une *« IA positive »*, Renaissance investit donc dans l'intelligence artificielle générative. *« Les algorithmes favorisent les contenus extrêmes, il faut pouvoir investir massivement sur ce point-là »*, assume le directeur chargé du numérique.

Cette stratégie ne fait pas l'unanimité au sein des appareils politiques français, notamment à gauche. Le Parti socialiste, par exemple, refuse catégoriquement d'utiliser l'IA pour la création de visuels ou de vidéos. *« Pour nous, le geste créatif* (…) *ne peut pas être substituable aux machines »*, explique Floran Vadillo, directeur général du Parti socialiste. *« Quand on produit des visuels, soit on les produit en interne, soit nous faisons appel à des artistes. »* Au risque de prendre du retard face à la stratégie des autres partis ? *« Parfois, il est possible de prendre de l'avance dans la faillite »*, assène-t-il. En 2025, une affiche créée par La France insoumise (LFI) à l'aide du logiciel d'IA Grok, appartenant à Elon Musk, avait fait polémique. La mise en scène caricaturale de l'animateur Cyril Hanouna a valu au mouvement des accusations d'antisémitisme. A la suite de cela, Paul Vannier, député (LFI) du Val-d'Oise et cadre du parti, assurait en mars 2025 que des mesures seraient prises en interne à propos de l'utilisation de l'IA. LFI n'a pas répondu aux sollicitations du *Monde*.

L'introduction de l'intelligence artificielle par les partis politiques ne se résume toutefois pas à la création de visuels ou de vidéos à destination des réseaux sociaux. Renaissance explique vouloir se servir de l'IA pour appuyer sa stratégie militante, à savoir renforcer le maillage territorial et la coordination entre les échelles locales et nationale, mais aussi étendre les outils d'aide aux militants sur le terrain. *« On veut trouver notre voie et créer le NationBuilder de notre génération »*, ajoute le cadre du parti, en référence au logiciel américain de ciblage électoral créé en 2009. Depuis, tous les partis politiques se sont munis de ces outils qui collectent des données et aident à rationaliser le travail de terrain lors des campagnes présidentielles. Résultat escompté : déterminer *« à la rue près »* quels sujets aborder avec les habitants en fonction de leurs préoccupations.

Autre ustensile : les chatbots. Ces assistants virtuels, conçus avec l'intelligence artificielle, ont pour fonction d'interagir avec les utilisateurs à partir d'une base de données créée. En mai 2023, Samuel Lafont, alors chargé du numérique chez Reconquête!, annonce la création de ChatZ, un chatbot pour promouvoir les idées du parti. Celui-ci a suscité quelques déceptions pour les commanditaires : le logiciel admettait que la théorie raciste du « grand remplacement», pensée par Renaud Camus en 2010 et récupérée par le parti d'extrême droite, relevait bien du complotisme.

Jusqu'ici, aucun autre parti n'a affiché publiquement avoir repris cet outil. Mais, en interne, certains ont déjà développé un assistant virtuel. C'est le cas du parti Les Républicains (LR). *« Dans notre application réservée aux adhérents, il y a un chatbot dans lequel vous pouvez poser vos questions pour en savoir plus sur notre programme ou vous renseigner sur les dernières déclarations faites par le parti »*, explique Jonas Haddad, vice-président (LR) de la région Normandie. Si l'usage de l'outil reste interne, le parti souhaite *« à moyen terme »* en élargir l'accès.

« Beaucoup de dérives »

« Etre capable d'avoir réponse à tout, c'est très puissant, et ça permet d'avoir un cerveau partagé hyperperformant », admet Florian Gauthier, fondateur de Vera, une IA qui vise à contrer la désinformation, ainsi que du « chatbotsecondtour ». Ce dernier, élaboré dans l'entre-deux-tours des législatives de 2024, avait pour but de fournir des arguments en faveur du programme du Nouveau Front populaire, l'alliance de la gauche. Peu après sa mise en ligne, beaucoup de militants s'en sont emparés. *« Je ne sais pas si c'est bien, parce que ça casse l'humain, et ce ne sont pas des logiciels pour débattre. C'est tentant, mais il y a beaucoup de dérives »*, admet, avec du recul, le jeune entrepreneur. *« Je ne tire pas un trait définitif* [sur l'idée] *d'offrir un accès condensé aux militants de notre programme, mais ça ne remplacera jamais la relation humaine »*, pense le directeur général du Parti socialiste.

« Je ne crois pas qu'un parti se privera de l'intelligence artificielle aujourd'hui », estime néanmoins Michaël Bardin, chercheur en droit public et numérique à l'université d'Avignon. Pour l'universitaire, une forme d'équilibre se crée une fois que tout le monde possède les mêmes instruments. *« Je ne pense pas que certaines forces politiques vont véritablement prendre plus d'importance que d'autres grâce à l'IA. »* L'émergence de ces outils pose toutefois des questions d'encadrement juridique des pratiques. En vertu de l'adoption du règlement européen sur l'intelligence artificielle (AI Act), en juin 2024, les IA destinées à influencer des élections sont reconnues comme étant à haut risque. *« La définition est assez souple pour pouvoir s'appliquer à des situations différentes »*, affirme Brice Héritier, avocat en droit public au sein du cabinet Fidal. Pour lui, les campagnes *« augmentées »* des élections municipales seront une *« forme de galop d'essai »*, avant la campagne pour la présidentielle.

Au-delà des partis et des militants, les électeurs aussi commencent à utiliser l'IA. Un sondage mené du 10 au 12 décembre 2025 par l'institut Ipsos BVA auprès de 1 000 personnes, publié jeudi 5 février, en partenariat avec la Fondation Jean Jaurès, signale un large usage de la part d'électeurs en quête de renseignements susceptibles d'orienter leur vote. De quoi poser des questions importantes sur la « neutralité » de ces outils et leur protection vis-à-vis des entreprises d'influence politique. Si deux tiers des sondés ont déjà utilisé un outil d'intelligence artificielle générative, un quart seulement l'a fait pour se renseigner sur une personnalité ou un parti politique et 23 % ne l'ont pas encore fait sur ce sujet, mais seraient prêts à le faire. Pour les élections municipales des 15 et 22 mars, 27 % des sondés envisagent d'utiliser l'IA pour se renseigner sur les programmes des candidats. Une proportion similaire envisage de le faire lors de la campagne présidentielle de 2027, faisant de ces outils un enjeu de premier plan.