IA et RGPD : les recommandations de la CNIL à l'épreuve du droit

INFORMATIQUE

Publié le 24/09/2025

Guillaume Fricker

avocat au barreau de Saint Malo-Dinan, administrateur de l'AAPPE



Alwie99d/AdobeStock

Comment la CNIL encadre le développement de l'intelligence artificielle à la lumière du RGPD, à travers ses recommandations pratiques et ses exigences de conformité pour les acteurs du numérique. Décryptage des enjeux de gouvernance, d'explicabilité et de respect des droits des personnes dans les projets IA, à partir de ses dernières publications officielles du 22 juillet 2025.

L'essor de l'intelligence artificielle (IA) bouleverse en profondeur le traitement des données à caractère personnel. L'introduction d'algorithmes d'apprentissage automatique dans la sphère économique, sociale et administrative pose d'innombrables défis, tant sur le plan technique que juridique. La multiplication des usages de l'IA dans des domaines sensibles – comme la santé, la justice, la sécurité ou encore les ressources humaines – accroît la nécessité d'un encadrement strict du traitement des données personnelles.

Dans ce contexte, la Commission nationale de l'informatique et des libertés (CNIL) s'impose en France comme l'autorité référente pour accompagner la transition numérique dans le respect des droits fondamentaux. Ses recommandations du 22 juillet 2025 offrent une grille de lecture pertinente pour les acteurs souhaitant se conformer aux exigences du RGPD tout en innovant dans le domaine de l'IA. Ces recommandations, à la fois techniques et juridiques, visent à répondre aux attentes croissantes de la société civile en matière de transparence, de loyauté et de maîtrise des risques liés à l'intelligence artificielle.

I – Les principes fondamentaux du RGPD applicables à l'IA

La CNIL rappelle que le RGPD s'applique pleinement aux traitements de données à caractère personnel opérés dans le cadre des systèmes d'IA, sans exception liée à la nature innovante ou complexe de ces technologies. Les principes cardinaux énoncés à l'article 5 du RGPD structurent l'ensemble des obligations pesant sur les responsables de traitement, qu'ils s'appuient ou non sur des systèmes d'IA :

Licéité, loyauté et transparence : les traitements doivent être « licites, loyaux et transparents » vis-à-vis des personnes concernées. L'article 5 du RGPD énonce l'ensemble des principes de base réalisant la protection des données : principes de licéité, loyauté et transparence ; limitation des finalités ; minimisation des données ; exactitude ; limitation de la conservation ; intégrité et confidentialité ; et responsabilité. La loi du 6 janvier 1978 (art. 4) et le RGPD (art. 5, 1-a à f) énoncent dans des termes analogues une série de six principes. Les données personnelles doivent être traitées de manière licite et loyale au regard de la personne concernée, ainsi que de manière transparente si le traitement relève du RGPD (« licéité, loyauté, transparence ») ;

Limitation des finalités : les données doivent être collectées à des fins déterminées, explicites et légitimes, sans traitement ultérieur incompatible avec ces finalités. Ce principe implique que la collecte et l'utilisation des données à des fins d'IA soient strictement encadrées : « Collectées à des fins déterminées, explicites et légitimes » ;

Minimisation des données : seules les données adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités doivent être collectées et traitées. « Seules doivent être traitées les informations adéquates, pertinentes et nécessaires au regard des objectifs poursuivis (c'est ce que l'on appelle la minimisation des données) »[1]. Le règlement général sur la protection des données ne retient pas le terme de « non-excessives » et introduit le principe de minimisation des données aux termes duquel les données doivent être « limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées » ;

Exactitude et mise à jour : les données doivent être exactes et, si nécessaire, tenues à jour. « Les données collectées doivent être non seulement exactes mais aussi, si nécessaires, tenues à jour »[2]. Toutes les mesures « raisonnables » doivent être prises pour que des données personnelles inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder ;

Limitation de la conservation : les données ne peuvent être conservées que pour une durée n'excédant pas celle nécessaire, au regard des finalités. « Le temps de la présence du salarié s'agissant d'une application de gestion des carrières, cinq ans pour un fichier de paie, deux ans après le dernier contact avec le candidat à un emploi pour un fichier de recrutement »[3]. Un principe repris dans le RGPD qui dispose qu'un employeur ne doit conserver les données personnelles de ses salariés que sur une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ;

Intégrité et confidentialité : les traitements doivent garantir la sécurité des données contre tout accès non autorisé ou illicite. Les données doivent être « traitées de façon à garantir une sécurité appropriée, en assurant notamment leur protection contre les traitements non autorisés ou illicites, ainsi que contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques et organisationnelles appropriées ».

Ces principes structurent l'approche de la CNIL, qui insiste sur leur nécessaire adaptation dans le contexte particulier de l'IA, caractérisé par la massification, l'automatisation et la complexité des traitements.

II – Les spécificités des traitements de données par l'IA : enjeux identifiés

Les systèmes d'IA présentent des particularités qui accentuent les risques pour les droits et libertés des personnes concernées :

Volume et diversité des données traitées : les modèles d'IA nécessitent souvent de vastes jeux de données, posant la question de la minimisation et de la pertinence des données collectées. « Ce terme à lui seul justifie une interprétation stricte du texte (...) qui ne manque pas d'interroger les politiques favorables au *Big Data*, comme celles relatives à la création d'un marché unique du numérique lorsqu'elle implique la création d'espaces européens des données » ;

Difficulté d'information et de transparence : la complexité technique des algorithmes et des processus d'apprentissage automatique rend difficile l'explication du traitement aux personnes concernées, ce qui peut nuire au respect du principe de transparence et à l'exercice effectif des droits. « Le principe de loyauté prévoit notamment la reconnaissance des attentes raisonnables des personnes concernées, l'examen des éventuelles conséquences négatives que le traitement pourrait avoir sur celles-ci, et la prise en compte de la relation et des effets potentiels du déséquilibre entre les personnes concernées et le responsable du traitement » ;

Prise de décisions automatisées : les traitements algorithmiques entraînent la multiplication des prises de décisions automatisées ayant des effets juridiques ou significatifs sur les personnes, ce qui implique des garanties particulières au titre du RGPD (articles 22 et 35). « Le règlement liste trois traitements susceptibles d'engendrer des risques élevés pour les droits et les libertés des personnes physiques (Règl. UE 2016/679 du 27-4-2016 art. 35) : l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire... ». L'analyse d'impact est obligatoire dans trois hypothèses : en cas d'évaluation systématique et approfondie d'aspects personnels fondée sur un traitement automatisé ; le traitement à grande échelle de données sensibles ou de données relatives à des condamnations pénales et à des infractions ; la surveillance systématique à grande échelle d'une zone accessible au public[4] ;

Risques accrus pour les droits et libertés : la CNIL souligne l'impératif d'analyser et de maîtriser les risques spécifiques liés à l'IA, notamment en matière de biais algorithmiques, de discrimination et d'opacité des décisions. « Le RGPD est fondé sur une logique de rendre compte auprès de l'autorité de contrôle, en particulier par le calcul des risques, réalisé par le responsable du traitement. L'étude des risques conditionne ainsi les mesures techniques et organisationnelles que ce dernier va décider de prendre ».

III – Les principales recommandations de la CNIL pour la conformité RGPD des systèmes d'IA

A – Gouvernance, *accountability* et *privacyby design*

La CNIL met en avant la nécessité d'intégrer la protection des données dès la conception (*privacy by design*) et par défaut (*privacyby default*) des systèmes d'IA. Le responsable du traitement doit être en mesure de démontrer à tout moment sa conformité aux principes du RGPD, ce qui implique une documentation rigoureuse (registre de traitements, études d'impact, mentions informatives, audits) et la mobilisation du *Data ProtectionOfficer* (DPO).

« Le DPO doit assurer cette interface nécessaire entre le responsable de traitement, les agents et la CNIL dans la perspective d'une mise en conformité aux principes posés par le RGPD et notamment le principe d'*accountability* (...) obligation du responsable de traitement de démontrer le respect des principes de licéité, de loyauté, de transparence des traitements de données à caractère personnel, de limitation des finalités des traitements, de minimisation des données traitées, d'exactitude des données, de limitation de la conservation des données et d'intégrité et la confidentialité des données. Ce principe suppose de rendre compte des démarches entreprises pour se mettre en conformité ».

Le respect du principe de *privacyby design* implique la prise en compte, en amont des projets d'IA, de mesures techniques et organisationnelles visant à limiter les risques pour les personnes concernées.

Le principe de *privacyby design* est également visé par l'article 25 du RGPD. Pour la CNIL, ce principe « implique de protéger les données personnelles dès la conception. Cela signifie que les entreprises ont désormais l'obligation d'intégrer ce principe de protection des données à caractère personnel dès la mise en œuvre de projets impliquant un traitement de données au sein d'une structure »

B – Analyse d'impact (DPIA/AIPD) : un outil central

La réalisation d'une analyse d'impact relative à la protection des données (AIPD/DPIA) est un passage obligé pour nombre de projets d'IA présentant un risque élevé pour les droits et libertés.

La CNIL rappelle les critères dégagés par le G29 (devenu CEPD) pour juger de la nécessité d'une analyse d'impact, notamment le recours à de nouvelles technologies, la prise de décisions automatisées, le traitement à grande échelle de données sensibles, la surveillance systématique, ou encore le traitement de données concernant des personnes vulnérables.

« Le G29 a pu sur cette base établir neuf indices qu'il convient de prendre en compte pour évaluer l'opportunité de la réalisation d'une analyse d'impact, à savoir (...) l'existence d'une évaluation, notation ou d'un profilage ; l'existence d'une prise de décision automatisée avec effet juridique ou effet similaire significatif ; l'existence d'un dispositif de surveillance systématique ; le fait que les données visées soient des données sensibles ou à caractère hautement personnel ; le fait que les données soient traitées à grande échelle ; le fait que les données concernent des personnes vulnérables ; l'utilisation d'une technologie innovante, ou l'application de nouvelles solutions technologiques ou organisationnelles ; le fait que le traitement en lui-même empêche la personne concernée d'exercer un droit ou de bénéficier d'un service ou d'un contrat (Règl. UE 2016/679 du 27-4-2016 art. 35, 3-a et art. 22) ».

Dans la plupart des cas, une analyse d'impact s'impose si deux de ces critères, au moins, sont réunis.

La CNIL insiste sur la nécessité d'une actualisation permanente de l'analyse d'impact, afin d'adapter le contenu à l'évolution des risques éventuellement créés par le traitement, notamment en cas de mise à jour des modèles ou de changement de finalités.

« Bien que le RGPD ne l'ait pas prévu, la jurisprudence administrative souligne la nécessité d'une actualisation permanente de l'analyse d'impact afin d'en adapter le contenu à l'évolution des risques éventuellement créés par le traitement (CE 6-11-2019 n° 434376 : RJDA 2/20 n° 126). Cette exigence figure dans les lignes directrices du "G29" ».

C – Transparence, information et explicabilité

La CNIL rappelle l'obligation d'informer les personnes concernées, dès la collecte, des opérations de traitement, des finalités poursuivies, de la logique sous-jacente aux traitements automatisés et des droits dont elles disposent.

« Le responsable de traitement doit informer les personnes concernées par les traitements de données, en l'espèce les salariés et les candidats à l'embauche, des opérations de traitement, dès la collecte des données (RGPD, art. 13). Il est préférable de procéder à une information écrite et individuelle des salariés ».

L'explicabilité des systèmes d'IA est ainsi érigée en exigence fondamentale, bien que la CNIL reconnaisse la difficulté d'expliquer certains traitements algorithmiques complexes.

D – Respect effectif des droits des personnes concernées

L'exercice des droits d'accès, de rectification, d'effacement, d'opposition et de limitation du traitement doit être garanti dans le cadre des systèmes d'IA, ce qui suppose une organisation technique et humaine adaptée pour répondre aux demandes dans les délais prévus par le RGPD.

« Aussi longtemps qu'il conserve des données à caractère personnel relatives à une personne concernée, le responsable de traitement sera tenu de répondre, en principe "dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande" art. 12.3 du RGPD, aux demandes d'exercice de ses droits par cette personne ».

Les droits des personnes concernées qui doivent être garantis, en matière de gestion des ressources humaines, sont les suivants : droit d'opposition au traitement (...) droits d'accès, de rectification, d'effacement (dans des conditions particulières) ; droit à la limitation du traitement, par exemple lorsque la personne conteste l'exactitude des données ; droit à la portabilité.

À cet égard, la CNIL recommande la mise en œuvre de procédures spécifiques pour le traitement des demandes de droits, notamment pour garantir le droit à la portabilité des données et le gel temporaire des traitements en cas d'exercice du droit à la limitation.

« Le droit à la limitation du traitement est également une nouveauté. Il permet de demander au responsable de traitement qu'il procède à la limitation du traitement des données dans certains cas, par exemple la contestation de l'exactitude des données, l'attente de la vérification du motif légitime du responsable de traitement après exercice par la personne concernée de son droit d'opposition au traitement. La limitation entraîne le gel temporaire des données, qui ne peuvent plus faire l'objet d'opérations de traitement ni être modifiées ».

IV – Portée et perspectives des recommandations de la CNIL dans le paysage juridique français et européen

Les recommandations de la CNIL s'inscrivent dans une dynamique européenne d'encadrement de l'IA, en articulation avec les travaux du Comité européen de la protection des données (CEPD) et la future adoption du règlement européen sur l'IA (*AIAct*). Elles offrent un cadre opérationnel pour la mise en conformité des systèmes d'IA, tout en laissant subsister des zones d'incertitude, notamment sur la question de l'explicabilité, la gestion des biais, ou la conciliation entre innovation technologique et protection des libertés.

En France, la CNIL joue un rôle moteur en matière d'accompagnement et de régulation, à travers ses référentiels, sa doctrine et ses contrôles. Sur le plan européen, ses recommandations contribuent à l'harmonisation des pratiques et à la consolidation d'un socle commun de garanties pour les personnes concernées.

Toutefois, l'évolution rapide des technologies d'IA et la complexification des modèles algorithmiques appellent une vigilance accrue, tant du côté des responsables de traitement que des autorités de contrôle.

Conclusion. Si la CNIL pose avec force les principes devant guider le développement de l'intelligence artificielle, rien ne garantit aujourd'hui que ces recommandations seront réellement suivies d'effets. Bien que la Commission multiplie les alertes sur la nécessité de concilier innovation et respect des droits fondamentaux, il subsiste un écart manifeste entre les exigences posées par le RGPD et la réalité des pratiques des acteurs de l'IA, souvent portés par des logiques de marché ou de performance technologique.

La question demeure : la voix de la CNIL sera-t-elle véritablement entendue par des entreprises ou des institutions parfois réticentes à intégrer des contraintes perçues comme des freins à l'innovation ? L'absence de moyens de contrôle renforcés et de sanctions dissuasives risque de reléguer ces recommandations à de simples vœux pieux, surtout face à la pression internationale et à la rapidité des évolutions technologiques. Dès lors, la construction d'une IA de confiance ne pourra reposer uniquement sur la bonne volonté des acteurs mais exigera une mobilisation concrète du régulateur, une volonté politique affirmée et une vigilance citoyenne accrue. Ce n'est qu'à ce prix que l'équilibre entre innovation et protection des droits pourra, peut-être, être atteint.

Notes de bas de pages

1.

PE et Cons. UE, règl. n° 2016/679, 27 avr. 2016, art. 5, § 1 – L. n° 78-17, 6 janv. 1978, art. 6.

2.

PE et Cons. UE, règl. n° 2016/679, 27 avr. 2016, art. 5, § 1, d.

3.

https://lext.so/xd956p.

4.

RGPD, art. 35, § 3.

Référence : AJU017u3