LE POUVOIR SUR LE CODE

Norme de droit public numérique

INSTITUTE FOR DIGITAL SOCIETY & FUTURE PUBLIC LAW

PROJET SOUMIS À CONSULTATION V1.0 — 28 SEPTEMBRE 2026

PROJET

STATUT DU PRÉSENT DOCUMENT

Stade. Projet soumis à consultation, version 1.0, daté du 28 septembre 2026. Référence au registre : à attribuer à l'ouverture de la consultation.

Organisme émetteur. Émis par l'Institute for Digital Society and Future Public Law de l'EPLO.

Effet juridique. La Norme relève du droit souple. Elle n'est pas juridiquement contraignante, sauf si une autorité compétente lui donne effet par son propre instrument.

Consultation. Consultation publique d'au moins soixante (60) jours. Les institutions publiques, les organes de contrôle, les juridictions et les institutions de médiation, les chercheurs, la société civile et les fournisseurs sont invités à présenter des observations. Les observations sont présentées sous le nom de leur auteur et publiées avec ce nom ; les observations anonymes ou confidentielles ne sont pas acceptées.

Introduction

La puissance publique s'exerce désormais couramment au moyen de systèmes numériques : des modèles de notation qui sélectionnent les personnes sur lesquelles une administration enquête, des portefeuilles numériques qui conditionnent l'accès à des services transfrontières, des plateformes de données qui déterminent la manière dont les hôpitaux répartissent leurs capacités. Le droit sectoriel examine chaque système de manière fragmentaire. Le droit de la protection des données demande si les données à caractère personnel sont traitées de manière licite, le droit de l'IA si un modèle satisfait aux exigences fondées sur les risques qui lui sont applicables, et le droit de la cybersécurité si les incidents sont gérés et signalés. Aucun régime sectoriel ne pose la question d'ensemble dont traite la présente Norme : l'institution publique responsable conserve-t-elle la capacité, en droit comme en pratique, de comprendre, de diriger, d'inspecter, de corriger et, si nécessaire, de faire cesser le dispositif numérique par lequel elle exerce la puissance publique ?

L'État ne conserve pas le pouvoir sur le code du seul fait qu'il est titulaire d'un contrat, d'une politique ou d'une plateforme. Il ne le conserve que lorsque l'autorité publique légalement investie demeure, de manière démontrable, capable de comprendre, de diriger, d'inspecter, de corriger, de réparer, de maintenir et, si nécessaire, de sortir des dispositifs techniques et sociotechniques par lesquels une mission publique est exercée. Le pouvoir sur le code se démontre ; il ne se proclame pas.

La Norme est organisée en quatre parties. La partie I (Noyau normatif) énonce l'exigence fondamentale, les onze principes, les dix capacités conservées ainsi que les tests et concepts fondamentaux. La partie II (Méthode) expose l'analyse d'impact de droit public numérique, méthode de référence de la Norme pour vérifier si le Noyau normatif est respecté dans chaque mission publique. La partie III (Application) expose la manière dont la Norme est utilisée : les modes d'utilisation, le Dossier de la mission publique numérique, les trois niveaux d'examen et leurs relevés de constatations, les formes sous lesquelles une autorité compétente peut donner effet à la Norme, et ses rapports avec d'autres instruments. La partie IV (Gestion de la Norme et mise en œuvre par le droit souple) explique comment la Norme est soumise à consultation, adoptée, modifiée et mise en œuvre.

PROJET

Partie I — Noyau normatif

I.1 Objet et nature

I.1.1 Le pouvoir sur le code (Power over Code) : Norme de droit public numérique (la « Norme ») énonce les conditions minimales qui doivent rester remplies chaque fois qu'une mission publique est exercée au moyen ou par l'intermédiaire de systèmes numériques, ou que ceux-ci la contraignent, la hiérarchisent ou la façonnent substantiellement.

I.1.2 La Norme est une norme juridique : un ensemble cohérent d'exigences normatives, assorti d'une méthode de référence pour leur application, destiné à assurer une application uniforme d'une institution et d'un ordre juridique à l'autre. Elle tire son contenu du droit constitutionnel, du droit administratif, du droit des droits de l'homme et du droit sectoriel qui régissent déjà la puissance publique. Elle ne crée pas de nouveaux droits substantiels et ne se substitue pas au droit applicable, lequel détermine le contenu et la force contraignante de chaque exigence dans chaque ordre juridique.

I.1.3 La Norme s'applique aux missions publiques à médiation numérique qui satisfont au test du champ d'application fonctionnel (I.8.1), que la mission soit exercée par un organisme public ou par un acteur privé agissant pour son compte.

I.2 Langage normatif

I.2.1 « **Doit** » désigne soit une condition méthodologique préalable à toute conclusion défendable au regard de la Norme, soit une obligation établie par le droit applicable. Chaque Dossier de la mission publique numérique précise lequel de ces fondements s'applique. Le non-respect d'une exigence formulée par « doit » fait obstacle à la catégorie de décision correspondante.

I.2.2 « **Devrait** » exprime une attente forte de la Norme, dont une institution ne peut s'écarter que moyennant une justification circonstanciée et consignée.

I.2.3 « **Peut** » exprime une faculté.

I.2.4 Un manquement méthodologique au regard de la Norme ne constitue pas en soi une constatation judiciaire d'illégalité. De même, la décision de ne pas appliquer la Norme ne supprime aucune obligation juridique existante d'une institution.

I.3 Définitions

I.3.1 **Le droit public numérique** est le domaine du droit qui a pour objet la constitution juridique, l'exercice, la médiation et le contrôle de la puissance publique dans des environnements dépendants du numérique.

I.3.2 « **Code** » désigne les dispositifs techniquement formalisés et opérationnellement effectifs par lesquels un système numérique exerce une mission publique, en assure la médiation, la contraint, la hiérarchise ou la façonne substantiellement de toute autre manière. Il comprend le code source et le code exécutable des logiciels ; les algorithmes, les règles de calcul, les modèles de décision et les modèles d'intelligence artificielle ; les configurations des systèmes, les seuils, les pondérations, les paramètres et les réglages par défaut ; les

PROJET

modèles de données, les schémas, les classifications et les jeux de données d'entraînement, de test, de référence ou d'exploitation ; les moteurs de flux de travail, les règles de décision automatisée et les règles d'escalade ; les interfaces de programmation d'applications et les mécanismes d'interopérabilité et d'échange de données ; les mécanismes d'identité, d'authentification, d'autorisation, d'attestation et de contrôle d'accès ; les systèmes de journalisation, de surveillance, de classement, de filtrage, d'appariement, de recommandation et de notification ; l'architecture des plateformes, les configurations en nuage et les contrôles de sécurité intégrés ; les spécifications techniques, les exigences des documents de marché, les conditions de licence et les fonctions du système placées sous la maîtrise du fournisseur ; ainsi que les protocoles d'interaction homme-machine lorsqu'ils structurent, limitent, canalisent ou orientent l'exercice de la puissance publique.

I.3.3 Le droit, les politiques, les instructions administratives, les contrats et le pouvoir d'appréciation humain ne constituent pas en eux-mêmes du code du seul fait qu'ils sont écrits ou formalisés. Ils ne relèvent de la définition que dans la mesure où ils sont traduits dans un système numérique, y sont intégrés ou sont rendus opérationnels par lui.

I.3.4 « Pouvoir sur le code » désigne la capacité, juridiquement fondée et institutionnellement effective, des autorités publiques de comprendre, de diriger, de contraindre, d'inspecter, de tester, de contester, de corriger, d'écarter, de suspendre, de remplacer et, si nécessaire, de faire cesser les systèmes techniques par lesquels les missions publiques sont exercées. Il exige que l'institution responsable conserve la responsabilité juridique de la mission ; une connaissance institutionnelle et une compétence technique suffisantes ; l'accès aux preuves, documents, données, modèles, configurations, journaux et informations d'audit pertinents ; la maîtrise effective des modifications substantielles du système ; la capacité d'assurer l'information, les explications, le réexamen, la contestation, la correction et les recours ; la continuité opérationnelle lorsqu'un fournisseur, une plateforme, un modèle ou un composant d'infrastructure est défaillant ou devient indisponible ; ainsi que l'autorité et la capacité pratique d'intervenir lorsque le système produit des résultats illégaux, constitutionnellement viciés, dangereux, discriminatoires, peu fiables ou institutionnellement inacceptables.

I.3.5 Le pouvoir sur le code n'exige pas qu'une institution publique soit propriétaire de ses logiciels ou les développe elle-même. L'externalisation, la commande publique, les licences, la dépendance à l'égard de l'informatique en nuage, les systèmes propriétaires et la participation du secteur privé sont compatibles avec le pouvoir sur le code, à condition de ne pas priver l'institution responsable de la capacité pratique de s'acquitter de ses obligations juridiques.

I.3.6 L'analyse d'impact de droit public numérique (DPLIA) est la méthode de référence de la Norme, exposée dans la partie II, pour recenser, analyser, documenter et réexaminer les implications de droit public d'une mission publique à médiation numérique et pour statuer sur celles-ci. La DPLIA fait partie de la Norme ; elle n'est pas un instrument distinct.

I.3.7 Le Dossier de la mission publique numérique (le « Dossier ») est le support documentaire unique et faisant foi d'une évaluation menée au titre de la Norme (III.2).

I.3.8 « Institution responsable » désigne l'institution publique juridiquement responsable de la mission publique évaluée.

PROJET

I.3.9 « **Autorité compétente** » désigne un organisme public juridiquement habilité à donner effet à la Norme dans son domaine de compétence ; et « **instrument d'adoption** » désigne l'instrument par lequel elle le fait (III.5).

I.3.10 « **Relevé de constatations au regard de la Norme** » désigne le résultat d'une évaluation, quel que soit le niveau d'examen (III.4). Il ne constitue ni un certificat, ni une marque de conformité, ni une déclaration de légalité.

I.4 L'exigence fondamentale

> **Exigence fondamentale**
>
> Toute institution juridiquement responsable d'une mission publique à médiation numérique conserve l'autorité, la connaissance, l'accès, les preuves, la capacité et les moyens pratiques nécessaires pour comprendre, diriger, contraindre, inspecter, contester, corriger, écarter, suspendre, remplacer et, s'il y a lieu, faire cesser les dispositifs techniques et sociotechniques par lesquels cette mission est exercée.

I.4.1 L'exigence fondamentale est vérifiée au moyen des dix capacités conservées (I.6) et des six points de contrôle (II.3). Les clauses de propriété et les déclarations de principe sont pertinentes, mais ne constituent pas une preuve. Dans chaque cas, la question est de savoir si les droits, l'accès, l'autorité, les preuves et les capacités opérationnelles existent, sont attribués, sont utilisables et ont été testés dans des conditions réalistes.

I.5 Principes

Les onze principes ci-après énoncent les conditions minimales d'une médiation numérique des missions publiques qui soit légale, constitutionnellement continue, institutionnellement responsable et résiliente.

Principe 1. Identification de la mission publique. Toute activité à médiation numérique doit être appréciée selon la mission qu'elle remplit et ses effets pratiques, et non selon sa qualification institutionnelle, sa forme contractuelle, son modèle de propriété ou sa description technologique.

Principe 2. Habilitation légale et continuité constitutionnelle. La transformation numérique ne doit pas interrompre l'application continue de la légalité, de la compétence, de l'équité procédurale, de l'égalité, de la proportionnalité, de la motivation, de l'obligation de rendre compte, de la protection juridictionnelle et du recours effectif.

Principe 3. Responsabilité publique non délégable. L'institution publique responsable doit conserver la responsabilité juridique et institutionnelle de la mission publique, y compris lorsque le développement technique, l'exploitation, l'infrastructure, le traitement des données ou l'aide à la décision sont fournis par un acteur privé.

Principe 4. Pouvoir institutionnel sur le code. L'institution responsable doit conserver des pouvoirs juridiques, un accès technique, des connaissances, des droits contractuels, une capacité organisationnelle et une aptitude opérationnelle suffisants pour comprendre, superviser, tester, corriger, écarter, suspendre,

remplacer ou faire cesser le système concerné. Les preuves de cette capacité sont organisées selon les quatre domaines de preuve (I.7).

Principe 5. Traçabilité et intégrité des preuves. Le système doit produire et conserver des preuves suffisantes de sa base juridique, de ses hypothèses de conception, de ses sources de données, de ses règles de fonctionnement, de ses modifications substantielles, ainsi que des décisions, des interventions, des erreurs et des résultats.

Principe 6. Contestabilité et recours. Les personnes concernées doivent bénéficier d'une information, d'explications, d'un réexamen, d'une correction, d'une possibilité de contestation et d'un recours effectifs, adaptés à la nature et aux conséquences de la mission publique à médiation numérique.

Principe 7. Gouvernance sur l'ensemble des six couches. Le respect du droit applicable ne peut être établi par le seul examen de l'algorithme ou du composant technique. Les couches juridique, institutionnelle, technique, des données, opérationnelle et sociétale sont évaluées ensemble.

Principe 8. Maîtrise des acteurs privés et des dépendances. Les contrats, les licences, les modalités de passation de marchés, les restrictions liées à la propriété intellectuelle, les dépendances à l'égard de l'informatique en nuage, les règles des plateformes et les systèmes propriétaires ne doivent pas empêcher l'autorité publique de s'acquitter de ses obligations juridiques ni d'exercer une maîtrise effective.

Principe 9. Sécurité, résilience et continuité. Le système numérique doit être conçu et gouverné de manière à préserver la continuité, l'intégrité, la disponibilité, la capacité de rétablissement et le fonctionnement légal de la mission publique en cas de perturbation, de défaillance, d'attaque, de retrait d'un fournisseur ou d'évolution technologique prévisibles.

Principe 10. Vérification tout au long du cycle de vie. L'évaluation doit se poursuivre après le déploiement. Toute modification substantielle du droit, de la finalité, des données, des modèles, de la configuration du système, des fournisseurs, de l'infrastructure, du risque ou de la capacité institutionnelle doit déclencher une réévaluation proportionnée.

Principe 11. Appréciation institutionnelle intégrée. La décision finale ne doit pas être réduite à un score technique ni à un résultat automatisé de conformité. L'institution responsable doit adopter et consigner une appréciation de droit public motivée, fondée sur les six points de contrôle, l'analyse des six couches, la synthèse causale, la confiance dans les preuves, les risques résiduels et les conditions de la poursuite de l'exploitation.

I.6 Les dix capacités conservées

I.6.1 L'exigence fondamentale reçoit un contenu opérationnel au moyen de dix capacités conservées. Dans l'ordre canonique, ce sont : Comprendre → Diriger → Documenter → Auditer → Expliquer → Corriger → Intervenir → Conserver les preuves → Continuer → Sortir.

I.6.2 Les capacités sont cumulatives et non facultatives. La solidité de l'une ne peut compenser l'absence d'une autre capacité nécessaire à l'exécution des obligations juridiques attachées à la mission, et les dix sont examinées ensemble.

PROJET

I.6.3 La propriété du code source n'est pas le facteur déterminant. Selon la portée constitutionnelle de la mission et la nature d'une éventuelle dépendance à l'égard d'un acteur privé, l'accès au code source peut être indispensable, utile sans être indispensable, ou inutile. La question est fonctionnelle et non patrimoniale.

I.6.4 Le degré d'approfondissement requis pour chaque capacité est fonction de la portée constitutionnelle de la mission, de la gravité et de la réversibilité des effets potentiels, du degré de dépendance à l'égard d'acteurs privés et de la difficulté qu'aurait une personne concernée à obtenir des preuves de ce qui s'est produit. La Norme n'institue pas une responsabilité sans faute pour toute défaillance d'un système et n'exige pas que chaque autorité publique dispose en interne d'une capacité d'ingénierie logicielle.

N°	Capacité	Aptitude institutionnelle requise	Exemples de preuves	Domaine de preuve
1	Comprendre	Décrire la manière dont le dispositif affecte substantiellement la mission, ainsi que les limites opérationnelles et les modes de défaillance connus de ce dispositif.	Cartographie de la mission; description de l'architecture; analyse des limites; registre des compétences du personnel; explication technique indépendante.	Connaître
2	Diriger	Maîtriser les finalités licites, la politique applicable, les seuils appliqués, la population concernée et toute modification substantielle de ces éléments.	Registre des droits de décision; approbation des modifications; clauses de contrôle des modifications opposables au fournisseur; journal des approbations.	Gouverner
3	Documenter	Reconstituer les données, les règles, les versions et les interventions pertinentes, ainsi que le cheminement ayant conduit à toute décision.	Traçabilité des données; historique des configurations et des versions; documents administratifs et techniques.	Connaître
4	Auditer	Permettre un examen qualifié, présentant l'indépendance appropriée, des performances, des journaux, des contrôles et des preuves détenues par le fournisseur. Exercer le droit d'audit, et non se borner à le détenir.	Droits d'accès effectivement exerçables; audits réalisés; résultats de tests; registres d'accès.	Répondre
5	Expliquer	Fournir des motifs intelligibles et propres à chaque cas, suffisants pour que la personne concernée comprenne une décision et, le cas échéant, la conteste.	Tests d'explication menés auprès d'usagers; décisions motivées; modèles de motivation; procédures de communication.	Connaître
6	Corriger	Détecter et corriger les erreurs affectant les données, la logique et les résultats, et répercuter la correction sur toutes les décisions affectées par l'erreur.	Tests de correction et de propagation; identification des cas affectés; registres de réouverture.	Répondre

N°	Capacité	Aptitude institutionnelle requise	Exemples de preuves	Domaine de preuve
7	Intervenir	Écarter le résultat du système, en restreindre ou en suspendre le fonctionnement, ou revenir en toute sécurité à un état antérieur, par une action autorisée.	Procédures d'intervention testées; agents formés; autorité d'escalade et journaux correspondants.	Gouverner
8	Conserver les preuves	Maintenir les preuves utilisables aux fins des réclamations, du réexamen, du contentieux, des enquêtes et du retour d'expérience, dans le respect des règles légales de conservation.	Tableau des durées de conservation; gel des preuves à des fins contentieuses; journaux protégés; contrôles d'accès.	Répondre
9	Continuer	Satisfaire aux obligations juridiques essentielles pendant une panne, une attaque ou la défaillance d'un fournisseur.	Solution de repli testée; canal de substitution; exercices de reprise; ressources de continuité.	Maintenir
10	Sortir	Migrer, remplacer ou faire cesser un système ou une relation avec un fournisseur, tout en préservant l'obligation juridique sous-jacente.	Plan de transition assorti d'une estimation des coûts; tests de portabilité; droits à assistance; préservation des demandes en cours; exercice de sortie réalisé.	Maintenir

Tableau I.1. Les dix capacités conservées dans l'ordre canonique, avec le domaine de preuve auquel chacune appartient.

I.6.5 Les documents conservés doivent être suffisants pour permettre la reconstitution et le recours, dans le respect des exigences légales de minimisation des données, de confidentialité et de limitation de la conservation. La correction doit identifier chaque décision affectée et prévoir une voie légale pour y remédier, en consignant les éventuelles limites à la réouverture et leurs conséquences.

I.7 Les quatre domaines de preuve

I.7.1 Les quatre domaines de preuve regroupent les dix capacités selon le type de preuve que chacune requiert. Ils constituent une aide à l'organisation des preuves, non une seconde série d'éléments notés, et ne modifient pas l'ordre canonique des capacités.

Domaine de preuve	Capacités	Question	Preuves types
Connaître	Comprendre · Documenter · Expliquer	L'institution peut-elle décrire comment la mission fonctionne, où se situent ses limites et pourquoi un résultat donné s'est produit ?	Architecture, traçabilité des données, cartographie des dépendances, preuves des compétences du personnel, motifs propres à chaque cas.

Domaine de preuve	Capacités	Question	Preuves types
Gouverner	Diriger · Intervenir	L'institution peut-elle diriger les choix et les modifications substantiels et interrompre le fonctionnement ?	Droits contractuels et droits d'accès, registres de contrôle des modifications, droits d'intervention exercés (et non simplement détenus).
Répondre	Auditer · Corriger · Conserver les preuves	L'institution peut-elle se soumettre à un examen, corriger les erreurs et conserver les preuves aux fins du réexamen ?	Audits réalisés, registres de correction et de propagation, registres de conservation et de gel des preuves.
Maintenir	Continuer · Sortir	L'institution peut-elle continuer à s'acquitter de ses obligations juridiques et sortir d'une dépendance ?	Résultats d'exercices, tests indépendants, réponse aux incidents, exercices de sortie.

Tableau I.2. Les quatre domaines de preuve.

I.8 Tests et concepts fondamentaux

I.8.1 Test du champ d'application fonctionnel

I.8.1.1 La Norme s'applique lorsque trois conditions cumulatives sont remplies : a) la puissance publique est exercée — la question porte sur l'exercice, l'organisation, le contrôle ou la continuité d'une mission publique d'importance constitutionnelle, qu'elle soit exercée directement par un organisme public ou par un acteur privé agissant pour son compte ; b) un système numérique influence substantiellement cet exercice, dont il façonne le fond, la procédure ou le résultat de telle sorte qu'ils seraient différents en l'absence du système ; et c) cette influence a une portée constitutionnelle, en ce qu'elle affecte la légalité, l'obligation de rendre compte, les droits, la gouvernance démocratique ou la résilience institutionnelle.

I.8.1.2 L'influence substantielle peut s'exercer par des recommandations, des réglages par défaut, des registres faisant foi ou les effets cumulés de l'orientation des usagers entre services. L'examen porte sur le fonctionnement réel et non sur la qualification donnée au système : un outil présenté comme une aide à la décision peut déterminer les résultats avec une intervention humaine purement nominale.

I.8.1.3 Si l'une des conditions n'est pas remplie, la question sort du champ d'application de la Norme. La simple commodité numérique courante, dépourvue de portée substantielle en droit public, n'entre pas dans ce champ ; un système de faible ampleur peut néanmoins en relever lorsqu'il affecte les droits ou le contrôle. L'incertitude ne prouve pas qu'une mission se situe hors du champ : un périmètre incertain appelle des preuves et une appréciation provisoire consignée, et ce périmètre est réexaminé lorsque la mission ou ses dépendances changent substantiellement.

I.8.2 Test de l'acteur privé

I.8.2.1 Lorsqu'un acteur privé participe à une mission qui satisfait au test du champ d'application fonctionnel, le test de l'acteur privé consiste à déterminer si cette participation met en jeu la responsabilité publique non délégable et appelle des contrôles renforcés. Ses branches sont les suivantes : a) la substitution fonctionnelle

PROJET

— l'acteur accomplit une tâche que l'institution publique devrait autrement accomplir elle-même ; b) le caractère indispensable en pratique — apprécié au regard de la documentation, des droits d'audit, de la maîtrise des modifications, de la conservation des preuves et de la capacité de sortie ; et c) le déplacement de l'obligation de rendre compte — l'obligation de rendre compte ordinaire de droit public (motivation, contrôle, recours) ne peut atteindre directement l'acteur.

I.8.2.2 Lorsqu'il est satisfait à toutes les branches, le comportement de l'acteur est soumis à la même rigueur que celui d'un organisme entièrement public exerçant la même mission, et des contrôles renforcés sont requis ; une dépendance grave prise isolément peut justifier des garanties ciblées. Le test met en évidence des besoins de gouvernance. L'imputation à l'État, la responsabilité directe du fournisseur et la soumission au contrôle juridictionnel demeurent des questions régies par le droit applicable.

I.8.2.3 Le test du champ d'application fonctionnel et le test de l'acteur privé répondent successivement à des questions différentes et ne sont pas fusionnés : le premier identifie la question de droit public ; le second détermine si un participant privé donné à cette mission est soumis à des obligations de droit public.

I.8.3 Architecture de gouvernance à six couches

Couche	Question centrale
1. Constitutionnelle, légale et réglementaire	Quels pouvoirs, droits, obligations et règles sectorielles constituent la mission, et le mandat satisfait-il aux exigences de légalité et de proportionnalité ?
2. Responsabilité institutionnelle	Qui est responsable de la mission, la finance, en assure le fonctionnement, la supervise et la modifie, et cette responsabilité peut-elle être retracée tout au long des délégations et des relations avec les fournisseurs ?
3. Données et infrastructure	De quels registres, modèles, interfaces, services en nuage et dispositifs d'interopérabilité, et de quelle architecture de sécurité, la mission dépend-elle ?
4. Décision et prestation de service	Comment la mission est-elle exercée au moment de la décision : par des algorithmes, par l'automatisation ou par une structure d'exercice du pouvoir d'appréciation ?
5. Obligation de rendre compte et contrôle	La motivation, l'audit, les réclamations, les recours et le contrôle juridictionnel atteignent-ils les enregistrements produits par la couche décisionnelle ?
6. Résilience et continuité	Qu'advient-il de la mission en cas de panne, de retrait d'un fournisseur, d'attaque, de crise ou de transition ?

Tableau I.3. L'architecture de gouvernance à six couches.

I.8.3.1 Les couches sont distinctes sur le plan analytique, mais interdépendantes sur le plan institutionnel. Un défaut à une couche se manifeste généralement à une autre : une responsabilité impossible à retracer (couche 2) apparaît lorsque l'obligation de rendre compte est mise à l'épreuve (couche 5) ; une dépendance non examinée (couche 3) devient une crise de continuité au moment du renouvellement (couche 6). L'architecture est une carte causale, non un septième point de contrôle ni une liste de vérification parallèle.

I.8.4 Infrastructure constitutionnelle

I.8.4.1 On entend par infrastructure constitutionnelle les systèmes numériques — systèmes d'identité, registres, dispositifs en nuage, couches d'interopérabilité — qui font désormais partie des fondations

institutionnelles par lesquelles les personnes exercent leurs droits et les organismes publics remplissent des missions constitutionnelles, de sorte que leur défaillance interrompt la vie constitutionnelle au lieu de causer un simple désagrément opérationnel. Une infrastructure est critique sur le plan constitutionnel lorsque sa défaillance ou la perte de sa maîtrise rendrait impossible l'exercice de droits essentiels ou le fonctionnement régulier des pouvoirs publics.

I.8.5 Responsabilité publique non délégable

I.8.5.1 Une autorité publique peut déléguer une tâche sans déléguer l'obligation d'en répondre qui s'y attache : cette obligation ne se transmet pas avec la tâche elle-même. L'externalisation technique ne saurait laisser une personne concernée sans institution tenue de répondre ni sans voie utilisable de correction. « Le fournisseur est responsable » ne tient pas légalement lieu d'obligation institutionnelle de répondre.

PROJET

Partie II — Méthode : analyse d'impact de droit public numérique

II.1 Nature de la méthode

II.1.1 La Norme énonce ce qui doit rester vrai ; la DPLIA est la méthode de référence de la Norme pour vérifier si tel est le cas dans une mission publique donnée. La DPLIA ne remplace pas les évaluations spécialisées, qu'elles soient juridiques, techniques ou relatives aux risques ou aux droits, lorsque celles-ci demeurent légalement requises. Elle lit ensemble leurs résultats, en tant que preuves, au regard du Noyau normatif.

II.1.2 La méthode doit pouvoir aboutir à une conclusion favorable lorsque les preuves l'étayent. Sa valeur tient à la qualité des motifs, des décisions et des garanties, non au nombre de constatations défavorables ni au volume de documentation produit.

II.1.3 Les points de contrôle donnent lieu à des constatations, non à des scores. Aucun score global n'est calculé, et la légalité ne peut être établie en additionnant des cotations de capacité favorables ni en mettant en balance une conception illégale et l'efficacité attendue.

II.2 Les six étapes

II.2.1 La DPLIA se déroule en six étapes. La numérotation des étapes organise le travail ; elle ne permet pas de franchir définitivement un point de contrôle avant que les preuves dont il dépend aient été vérifiées. Les preuves recueillies à une étape ultérieure peuvent modifier toute constatation antérieure, et une modification substantielle peut ramener l'évaluation à l'étape 1. Les constatations initiales sont provisoires lorsqu'elles dépendent de preuves recueillies ultérieurement ; la Décision institutionnelle exige qu'elles soient mises en cohérence.

Étape	Intitulé	Travaux	Résultat versé au Dossier
1	Champ d'application	Ouvrir le Dossier lors de la conception de la politique, de la passation du marché, du renouvellement, d'une modification substantielle ou d'un incident ; déterminer le responsable, le résultat recherché et la décision à prendre ; appliquer le test du champ d'application fonctionnel ; fixer le niveau d'examen (III.3).	Conclusion de l'examen préalable ; responsable ; périmètre ; niveau d'examen ; élément déclencheur de réexamen.
2	Cartographie de la mission	Définir le périmètre et les dépendances de la mission ; cartographier les six couches ; appliquer le test de l'acteur privé ; identifier les personnes concernées ; répertorier les preuves spécialisées importées.	Cartographie de la mission ; répertoire des dépendances et des preuves ; analyse des personnes concernées.
3	Six points de contrôle	Vérifier la mission au regard de chaque point de contrôle et coter les dix capacités, en consignant pour chaque constatation la source des preuves et le degré de confiance.	Constatations par point de contrôle, avec sous-constatations ; cotations des capacités.

PROJET

Étape	Intitulé	Travaux	Résultat versé au Dossier
4	Synthèse causale	Lire ensemble, sous forme de chaînes causales, les constatations relatives aux points de contrôle, aux capacités et aux couches ; énoncer séparément le risque, la confiance dans les preuves et l'intégrité de la mise en œuvre.	Synthèse causale ; risques résiduels ; opinions divergentes.
5	Décision institutionnelle	Adopter une décision motivée relevant de l'une des huit catégories, assortie de conditions, de responsables, d'échéances et de conséquences.	Décision signée ; registre des conditions ; relevé de constatations.
6	Réexamen au cours du cycle de vie	Suivre le fonctionnement, l'information et la réparation ; réévaluer selon le calendrier ou en cas de modification substantielle ; gérer la transition ou la sortie.	Calendrier de réexamen ; journal des éléments déclencheurs ; constatations mises à jour.

Tableau II.1. Les six étapes de la DPLIA.

Étape 1 — Champ d'application

II.2.2 L'évaluation s'ouvre lorsqu'une mission est conçue, fait l'objet d'un marché, est renouvelée, est substantiellement modifiée ou est mise en cause dans un incident. L'institution responsable ouvre le Dossier, désigne le responsable tenu de rendre compte de la mission et consigne le résultat public recherché ainsi que la décision que l'évaluation doit éclairer. Elle applique le test du champ d'application fonctionnel (I.8.1) une seule fois, avant l'examen de tout point de contrôle ; ce test n'est pas lui-même un point de contrôle.

II.2.3 Une mission jugée hors du champ d'application fait l'objet d'une fiche d'examen préalable motivée, qui désigne le responsable et un élément déclencheur de réexamen. Les obligations juridiques et administratives ordinaires continuent de s'appliquer. Pour une mission relevant du champ d'application, l'institution fixe le niveau d'examen conformément à la section III.3 et en consigne les motifs.

Étape 2 — Cartographie de la mission

II.2.4 La Cartographie de la mission définit le périmètre et les dépendances de la mission : les acteurs, les données, les systèmes, les fournisseurs, les voies de recours et les solutions de repli sur lesquels elle repose. Elle cartographie la mission au regard des six couches (I.8.3), applique le test de l'acteur privé (I.8.2) à chaque participant privé important et identifie les personnes concernées, leurs vulnérabilités et les intérêts en jeu.

II.2.5 Les preuves spécialisées — une analyse d'impact relative à la protection des données, une analyse d'impact sur les droits fondamentaux, un test de sécurité — sont répertoriées par renvoi, avec mention de leur source, de leur version, de leur dépositaire, de leur portée juridique et de leur état de vérification. Un rapport spécialisé achevé est une preuve à apprécier, non une réponse faisant autorité sur chaque question relevant de son domaine. La question pertinente est de savoir ce qu'il établit au sujet de la mission considérée et ce qui reste non résolu aux interfaces.

PROJET

Étape 3 — Les six points de contrôle

II.2.6 Les six points de contrôle de droit public (les « six points de contrôle ») traduisent en constatations explicites les exigences juridiques et constitutionnelles applicables à la mission. Chaque point de contrôle énonce une question déterminante, les éléments qu'il couvre et une règle de blocage. Une évaluation complète traite les six points de contrôle; toute sous-question considérée comme sans objet appelle un motif consigné.

Point de contrôle	Question déterminante	Éléments couverts	Règle de blocage
1. Mandat légal	L'institution dispose-t-elle d'une compétence juridique précise et poursuit-elle un but public légitime pour cette mission ?	Compétence matérielle et territoriale; précision de l'habilitation; finalité publique et population concernée; limitation des finalités; cohérence entre la règle codée et la règle de droit.	La mission ne doit pas être mise en œuvre sans une base juridique identifiable, en vigueur et suffisamment précise quant à sa finalité et à la population visée.
2. Conception justifiée au regard des droits	La conception est-elle nécessaire, proportionnée, non discriminatoire et accessible, compte tenu des solutions de substitution disponibles ?	Preuves du problème et solutions de substitution; moyens moins intrusifs; avantages, charges et réversibilité; effets sur les groupes et effets distributifs; accessibilité; vulnérabilité.	Une conception ne doit pas être mise en œuvre lorsqu'un moyen moins intrusif permet d'atteindre le même but, ou lorsque les effets sur les groupes n'ont pas été évalués pour une mission relevant du niveau d'examen 2 ou 3. L'établissement de rapports ne peut remédier à une discrimination illégale ni à une ingérence disproportionnée.
3. Responsabilité publique	Une institution publique unique, dotée d'un responsable de la décision nommément désigné, est-elle identifiable et tenue de répondre de la mission ?	Répartition légale des responsabilités entre acteurs publics, privés et décentralisés; modalités de délégation, de passation de marchés et d'utilisation des données; voies d'escalade.	La mission doit avoir un responsable public de la décision nommément désigné avant tout engagement dans une procédure de passation de marché.
4. Maîtrise opérationnelle	L'institution peut-elle légalement et effectivement gouverner les données, le code, les fournisseurs, les modifications et les interventions qui façonnent substantiellement la mission ?	Accès légal aux données et correction de celles-ci; maîtrise contractuelle des dépendances importantes; contrôle des modifications, gestion des versions, accès aux journaux et tests indépendants; capacité d'auditer, de corriger, de restreindre et de réorienter.	Pour les missions ayant une incidence significative sur les droits, l'incapacité d'auditer un effet substantiel, d'intervenir à son égard ou de le corriger doit faire obstacle au déploiement jusqu'à ce que la maîtrise soit démontrée. Une stipulation contractuelle jamais mise en œuvre ne suffit pas à elle seule.

Point de contrôle	Question déterminante	Éléments couverts	Règle de blocage
5. Preuves, contrôle et recours	L'institution et une personne concernée peuvent-elles reconstituer, comprendre, contester et corriger un résultat ou une défaillance d'importance ?	Preuves administratives et techniques ; motifs intelligibles ; réexamen humain ou institutionnel effectif ; préparation aux réclamations, aux recours, à la saisine du médiateur ou du régulateur et au contrôle juridictionnel ; correction des erreurs individuelles et systémiques, y compris la propagation de la correction.	Pour les missions ayant une incidence significative sur les droits, l'absence de preuves suffisantes, de possibilité réelle de contestation ou de correction effective doit faire obstacle au déploiement ordinaire. Une description publiée ou une présence humaine nominale n'établit pas l'existence d'un recours.
6. Continuité et sortie	L'institution peut-elle continuer à s'acquitter de ses obligations juridiques en cas de panne, d'attaque, de défaillance d'un fournisseur, de modification, de renouvellement ou de résiliation, et sortir du dispositif sans abandonner les droits, les preuves ou le service ?	Continuité et solution de repli non numérique testées ; conduite des opérations en cas d'incident et dégradation maîtrisée ; portabilité, changement de fournisseur et assistance à la transition ; préservation des preuves, des procédures en cours et des corrections pendant la transition.	La continuité et la sortie doivent être testées avant qu'une décision de renouvellement ou de rupture du contrat ne devienne inévitable, et non après que la dépendance est devenue irréversible.

Tableau II.2. Les six points de contrôle de droit public

II.2.7 Le point de contrôle 4 n'est pas un score générique de cybersécurité et ne tranche pas la question de savoir si une personne concernée dispose d'un recours effectif ; cette question relève du point de contrôle 5. Le point de contrôle 1 établit une habilitation qu'aucune capacité technique ne peut fournir.

Étape 4 — Synthèse causale

II.2.8 Le respect du droit applicable ne peut être établi en examinant isolément l'algorithme ou le composant technique. La synthèse causale lit ensemble, sous forme de chaînes, les constatations relatives aux points de contrôle, aux capacités et aux couches, en posant pour chaque constatation importante les questions suivantes : a) quelle est la condition déclenchante ; b) par quelle couche se propage-t-elle ; c) quelle garantie est censée interrompre la propagation, et cette garantie a-t-elle été effectivement mise en œuvre ou seulement documentée ; et d) quel risque résiduel subsiste une fois pris en compte l'effet réel, et non nominal, de la garantie. Une évaluation favorable de chaque composant pris séparément ne peut remplacer cette analyse de leur fonctionnement combiné.

II.2.9 Trois appréciations relatives aux preuves sont consignées séparément et ne sont jamais fusionnées :

- **Le risque** — le préjudice potentiel : gravité, probabilité, ampleur, durée, vulnérabilité, réversibilité et propagation.

- **La confiance dans les preuves** — l'appui dont bénéficie une constatation : élevée lorsque les preuves actuelles sont vérifiées et dûment corroborées; moyenne lorsque l'accès ou les tests sont limités; faible lorsque les preuves sont manquantes, présumées ou sérieusement contestées.
- **L'intégrité de la mise en œuvre** — la question de savoir si les garanties sont attribuées, dotées de ressources, suivies et susceptibles d'être imposées en pratique.

II.2.10 Une faible probabilité estimée ne peut pallier l'absence de preuves de l'habilitation légale ou du recours. Un droit contractuel ne démontre ni l'existence d'effectifs suffisants ni un usage effectif.

Étape 5 — Décision institutionnelle

II.2.11 L'institution responsable adopte et consigne une appréciation de droit public motivée relevant de l'une des huit catégories.

Catégorie de décision	Cas d'application	Élément déclencheur type
Mettre en œuvre	Tous les points de contrôle sont « Satisfait » ou « Sans objet »; les capacités sont démontrées avec une confiance élevée dans les preuves.	Aucune lacune de capacité relevée.
Mettre en œuvre sous conditions contraignantes	Les points de contrôle sont « Satisfait » ou « Conditionnel »; une ou plusieurs garanties sont faibles mais peuvent être corrigées, avec un responsable nommément désigné et une échéance.	Un droit d'audit qui existe mais n'a pas été testé.
Expérimenter dans des conditions contrôlées	Application nouvelle pour laquelle les preuves restent prospectives.	La capacité existe au stade de la conception, mais n'a pas encore fait ses preuves en exploitation.
Reconcevoir et soumettre à nouveau	Un point de contrôle n'est pas satisfait, mais la mission reste légale dans son principe moyennant une nouvelle conception.	Aucun droit d'accès aux données ou d'audit n'a été obtenu.
Suspendre	Une défaillance de capacité continue d'exposer les droits à une atteinte pendant que la nouvelle conception est en cours.	Risque de préjudice actuel.
Abandonner	La mission ne peut être exercée légalement, quelle que soit la conception réalisable.	Non-satisfaction irrémédiable d'un point de contrôle.
Solliciter une habilitation légale supplémentaire	La mission est bien conçue, mais ne dispose pas d'une base juridique suffisante.	Non-satisfaction du point de contrôle 1 sans lien avec la maîtrise opérationnelle.
Renvoyer pour décision indépendante	La confiance dans les preuves est trop faible pour que l'évaluateur puisse conclure.	Preuves sous la maîtrise du fournisseur ou inaccessibles.

Tableau II.3. Les huit catégories de décision institutionnelle.

II.2.12 Chaque décision consigne ses motifs, les éventuelles opinions divergentes, les garanties, les conditions, les responsables nommément désignés, les échéances et la conséquence qui s'applique automatiquement si

une condition n'est pas remplie à l'échéance. Une condition dépourvue de responsable ou d'échéance n'est pas une condition. « Poursuivre le suivi » ou « à suivre » n'est pas une condition suffisante.

II.2.13 Les conditions peuvent régir les améliorations à apporter au cours d'une exploitation légale, mais les prérequis doivent être vérifiés avant que l'activité qui en dépend ne commence. Une constatation « Conditionnel » n'autorise pas un déploiement ordinaire complet lorsqu'une exigence bloquante n'est pas remplie.

II.2.14 Une expérimentation suppose une base juridique existante, des participants protégés, un périmètre limité et un mécanisme d'arrêt. Elle ne peut servir d'exception à une interdiction ni tenir lieu de mandat légal.

II.2.15 L'institution tenue de rendre compte signe la décision, désigne la personne chargée de vérifier les conditions et consigne la date du prochain réexamen. La validation par le fournisseur ne peut remplacer la décision publique. Des preuves d'un préjudice actuel appellent sans tarder des mesures de protection conformes au droit, alors même qu'une évaluation plus complète est en cours.

Étape 6 — Réexamen au cours du cycle de vie

II.2.16 L'évaluation ne prend pas fin avec l'autorisation ou le déploiement. Toute modification substantielle du droit, de la finalité, des données, des modèles, de la configuration du système, des fournisseurs, de l'infrastructure, du risque ou de la capacité institutionnelle rouvre les points de contrôle concernés. Une mission approuvée à titre expérimental ne doit pas étendre sa population, sa finalité, ses données ou sa portée institutionnelle sans une réévaluation consignée : il n'y a pas d'extension tacite. Une décision ne demeure valable que dans les limites du périmètre et des conditions évalués; les conditions non remplies entraînent la conséquence prévue par la décision, y compris la restriction ou la suspension lorsque cela se justifie.

II.2.17 À chaque réexamen, l'institution confirme que :

- un calendrier de réévaluation et un journal des éléments déclencheurs sont tenus à jour;
- chaque constatation « Conditionnel » est assortie d'un responsable, d'une échéance, d'une méthode de vérification et d'une conséquence;
- la continuité et la sortie ont été testées avant qu'une décision de renouvellement ou de rupture du contrat ne devienne inévitable;
- le réexamen postérieur au déploiement a porté sur les incidents, les dérives, les réclamations, les corrections et les effets différenciés.

II.2.18 La planification de la sortie commence dès la conception et la passation du marché, même si son exécution est consignée à l'étape 6. La transition ou la cessation préserve les obligations de service, les preuves, les demandes en cours et l'obligation de rendre compte.

PROJET

II.3 Constatations relatives aux points de contrôle et cotations des capacités

II.3.1 Constatations relatives aux points de contrôle. Chaque point de contrôle donne lieu à une constatation motivée :

Constatation	Signification
Satisfait	Une habilitation et des garanties suffisantes sont démontrées.
Conditionnel	L'exigence peut être remplie au moyen d'une condition contraignante et assortie d'un délai, avant ou pendant un déploiement contrôlé. La condition est assortie d'un responsable, d'une échéance, d'une méthode de vérification et d'une conséquence en cas de non-respect.
Non satisfait	Le dispositif ne peut légalement être mis en œuvre sans nouvelle conception, habilitation supplémentaire ou abandon.
Indéterminé	La confiance dans les preuves est trop faible pour une conclusion responsable ; des preuves supplémentaires ou une décision indépendante sont nécessaires.
Sans objet	Le point de contrôle n'est pas mis en jeu par la mission telle que son périmètre a été défini, pour des motifs consignés.

Tableau II.4. Les cinq constatations relatives aux points de contrôle.

II.3.2 Chaque constatation précise si les preuves sur lesquelles elle repose sont directes, importées d'une évaluation spécialisée ou déduites. « Partiel » n'est pas une constatation relative à un point de contrôle.

II.3.3 L'absence d'habilitation suffisante, d'institution tenue de rendre compte, de preuves essentielles au contrôle ou de recours effectif fait obstacle au déploiement ordinaire d'une mission ayant une incidence significative sur les droits. Un usage interdit ou illégalement discriminatoire ne peut être justifié par une mise en balance. Une constatation « Indéterminé » portant sur une exigence non compensable, due à des preuves manquantes et non à des preuves défavorables, emporte la même conséquence pour le déploiement qu'une constatation « Non satisfait » jusqu'à l'obtention de preuves suffisantes. Les défauts critiques en matière de continuité ou de sortie font de même obstacle à un dispositif dont la défaillance rendrait impossible l'exécution d'obligations juridiques.

II.3.4 Cotations des capacités. Chacune des dix capacités est cotée « Oui », « Partiel » ou « Non ». Pour chaque capacité, l'évaluateur distingue trois questions, une réponse positive aux deux premières étant compatible avec une réponse négative à la troisième : a) l'institution détient-elle le pouvoir ou le titre juridique — un mandat légal, une clause contractuelle d'audit, un pouvoir documenté d'écarter le résultat du système ; b) dispose-t-elle de la capacité pratique et des ressources pour l'exercer — personnel formé, accès technique, temps institutionnel ; et c) la capacité a-t-elle été démontrée dans des conditions réalistes ? Les tests peuvent être simulés ou scénarisés lorsqu'un test en conditions réelles mettrait en péril les droits ou la continuité du service.

II.3.5 Une affirmation du fournisseur non étayée par des preuves de l'institution plafonne la cotation à « Partiel ». Un contrat promettant la portabilité des données ne démontre pas, à lui seul, la capacité « Sortir » ; une politique permettant à un agent d'écarter le résultat du système ne démontre pas la capacité « Intervenir » si les agents habilités à le faire ne disposent pas du temps, des informations ou de l'autorité

PROJ

nécessaires; un registre public de transparence ne démontre pas la capacité « Expliquer » au degré de précision qu'exige une contestation individuelle; un droit d'audit n'est coté « Oui » que lorsqu'il a été exercé, et non simplement détenu.

II.3.6 Niveaux de preuve. Les preuves d'une garantie sont classées « Documenté » (la garantie existe sur le papier), « Opérationnel » (elle a été mise en œuvre au moins une fois) ou « Testé » (elle a été testée dans des conditions réalistes). Le niveau de preuve minimal requis dépend du niveau d'examen (III.3).

II.4 Liens indicatifs entre capacités et points de contrôle

II.4.1 Chaque évaluation explique quelles cotations de capacité étayent ou fragilisent chaque constatation relative à un point de contrôle. Les liens ci-dessous sont indicatifs et se recoupent; ils ne regroupent pas les capacités et ne remplacent pas les domaines de preuve.

Point de contrôle	Capacités qui fournissent généralement des preuves
1. Mandat légal	Aucune ne peut fournir l'habilitation légale; Comprendre et Documenter attestent la cohérence entre la règle codée et la règle de droit.
2. Conception justifiée au regard des droits	Comprendre, Diriger, Documenter.
3. Responsabilité publique	Diriger, Documenter.
4. Maîtrise opérationnelle	Diriger, Auditer, Corriger, Intervenir.
5. Preuves, contrôle et recours	Documenter, Auditer, Expliquer, Corriger, Conserver les preuves.
6. Continuité et sortie	Intervenir, Conserver les preuves, Continuer, Sortir.

Tableau II.5. Liens probatoires indicatifs.

II.5 Le cycle de vie du système

II.5.1 Les six étapes de la DPLIA sont distinctes des six phases du cycle de vie du système auquel la DPLIA s'applique : 1) cadrage stratégique; 2) conception et passation des marchés; 3) développement et déploiement; 4) gouvernance opérationnelle; 5) réexamen et adaptation; et 6) cessation ou transition. La DPLIA peut être appliquée, intégralement ou au degré d'approfondissement qu'exige le niveau d'examen, à n'importe quelle phase. Les modes d'utilisation prévus à la section III.1 correspondent à ces phases.

PROJET

Partie III — Application

III.1 Six modes d'utilisation

III.1.1 La Norme et la DPLIA sont utilisées selon six modes liés entre eux. Les quatre premiers sont des utilisations ordinaires au cours du cycle de vie; les deux autres étendent la Norme aux événements exceptionnels et à l'analyse à l'échelle du système. Dans chaque mode, le Noyau normatif fournit la référence, et la DPLIA la méthode par laquelle sont examinées les insuffisances, les incertitudes, les interactions causales, les garanties nécessaires et les conséquences institutionnelles.

Mode	Ce qu'il vérifie
1. Évaluation prospective	Avant la conception, la passation du marché ou l'autorisation législative : si une mission à médiation numérique envisagée peut, dans son principe même, être légalement mise en place.
2. Examen de la conception et du développement	Pendant la conception et la réalisation : si l'architecture qui se dessine satisfait aux points de contrôle avant que les engagements ne deviennent difficiles à remettre en cause.
3. Évaluation préalable au déploiement	Avant l'approbation, l'autorisation ou la mise en service : si la mission telle qu'elle a été réalisée — et non telle qu'elle avait été proposée à l'origine — satisfait à la Norme.
4. Examen opérationnel et réexamen au cours du cycle de vie	Pendant l'exploitation ordinaire : si la mission continue de satisfaire à la Norme et si une modification substantielle appelle une réévaluation.
5. Examen à la suite d'un incident, d'une défaillance, d'une réclamation, d'un contentieux ou d'une controverse	En réponse à un événement précis : quel point de contrôle ou quelle couche l'événement met en cause et quelle correction il appelle.
6. Examen systémique, comparé, législatif ou institutionnel	À l'échelle de plusieurs missions, de plusieurs ordres juridiques ou d'un secteur : les schémas récurrents que l'évaluation d'une seule mission ne peut faire apparaître.

Tableau III.1. Les six modes d'utilisation.

III.1.2 Chaque utilisation suppose une conséquence décisionnelle identifiée et un réexamen continu. L'évaluation d'un système envisagé peut conduire à une nouvelle conception ou à un non-déploiement; l'évaluation d'une mission existante peut exiger des mesures de protection immédiates parallèlement à des mesures correctives de plus long terme. C'est le réexamen au cours du cycle de vie (étape 6) qui rend chaque mode opérant : un réexamen qui ne modifie rien dans le Dossier n'a pas produit de décision institutionnelle.

III.2 Le Dossier de la mission publique numérique

III.2.1 Chaque évaluation tient un Dossier de la mission publique numérique unique et faisant foi. Le Dossier est la mémoire institutionnelle et l'armature probatoire de l'évaluation, non une annexe facultative. Il

constitue un dossier de décision cohérent, non un entrepôt de documents : il relie les preuves spécialisées par renvoi, en mentionnant leur source, leur version, leur dépositaire et leur état de vérification, au lieu de reproduire les contrats, jeux de données ou journaux sous-jacents. Il constitue un document administratif officiel et est conservé comme tel.

III.2.2 Le Dossier est organisé en six sections :

Section du Dossier	Contenu essentiel
1. Examen préalable et niveau d'examen	Mission, responsable, élément déclencheur, constatations relatives au champ d'application, niveau d'examen et motifs, périmètre, date de réexamen.
2. Mission et base juridique	Mandat, finalité, cheminement décisionnel, dépendances, description faisant foi du système ; institution responsable et décideur tenu de rendre compte ; systèmes, fournisseurs et acteurs privés.
3. Gouvernance et personnes concernées	Cartographie des six couches ; test de l'acteur privé ; répartition des responsabilités ; personnes concernées, intérêts et vulnérabilités ; participation.
4. Points de contrôle et synthèse	Constatations et sous-constatations relatives aux points de contrôle, avec la source des preuves ; risque, confiance dans les preuves et intégrité de la mise en œuvre ; solutions de substitution ; synthèse causale ; opinions divergentes.
5. Capacités et décision	Cotations des dix capacités avec les niveaux de preuve ; garanties ; Décision institutionnelle ; conditions, responsables, échéances et conséquences ; modalités de suivi, de réparation, de continuité et de sortie.
6. Obligation de rendre compte au public et cycle de vie	Relevé de constatations ; résumé public ; réponses à la consultation ; inscription au registre ; voies d'information et de contestation ; dates de réexamen, éléments déclencheurs, incidents, modifications et décisions ultérieures.

Tableau III.2. Les six sections du Dossier de la mission publique numérique.

III.2.3 Les documents de marché devraient exiger, à titre de conditions préalables à l'attribution du marché, les droits d'audit, d'accès aux preuves, de contrôle des modifications et de sortie que vérifient les points de contrôle 3, 4 et 6. Un droit invoqué pour la première fois après la signature révèle une lacune du Dossier ; il n'y remédie pas.

III.3 Niveaux d'examen

III.3.1 Une évaluation est menée à l'un des trois niveaux d'examen. Le niveau d'examen détermine qui évalue, la quantité de preuves requise et l'indépendance que doit présenter l'examen. Il s'agit d'une appréciation de proportionnalité, arrêtée à l'étape 1 et revue chaque fois que la mission change substantiellement ; elle ne remplace pas les constatations de fond auxquelles aboutissent les points de contrôle.

	Niveau 1 — Auto-évaluation	Niveau 2 — Évaluation vérifiée	Niveau 3 — Évaluation indépendante
Qui évalue	L'institution responsable.	L'institution responsable, avec validation par un vérificateur nommément désigné, indépendant de la mission évaluée.	Une partie indépendante de l'institution responsable.
Missions types	Portée limitée en droit public; appui réversible; aucune automatisation ayant une incidence significative sur les droits.	Effet substantiel sur les droits, les services ou la confiance du public; irréversibilité modérée.	Portée constitutionnelle élevée ou forte irréversibilité; forte dépendance à l'égard d'acteurs privés; groupes vulnérables à grande échelle; constatations bloquantes ou preuves contestées.
Dossier minimal	Dossier concis; responsable nommément désigné; preuves pertinentes; suivi proportionné. Les points de contrôle peuvent être consignés comme « Satisfait » ou « Sans objet » sur la base de preuves minimales lorsque les motifs sont exposés.	Dossier complet; analyse intégrale des six points de contrôle; résumé public; annexes spécialisées requises par la mission.	Répertoire complet des preuves; association des personnes concernées; autorisation à un niveau hiérarchique élevé.
Niveau de preuve minimal	Documenté.	Opérationnel pour chaque garantie importante.	Testé pour les capacités essentielles à la légalité, au recours, à la continuité et à la sortie.
Résultat	Relevé de constatations au regard de la Norme.	Relevé de constatations au regard de la Norme.	Relevé de constatations au regard de la Norme.

Tableau III.3. Les trois niveaux d'examen.

III.3.2 Choix du niveau. Le niveau est fonction de l'incidence de la mission, de la vulnérabilité des personnes concernées, de l'ampleur, de la réversibilité, de la dépendance à l'égard d'acteurs privés, de la nouveauté et de l'asymétrie des preuves. Des qualifications telles que justice, identité ou protection sociale ne déterminent pas à elles seules le niveau : la mission, ses conséquences et ses dépendances doivent être analysées.

III.3.3 Missions critiques sur le plan constitutionnel. Une mission qui assure le fonctionnement d'une infrastructure critique sur le plan constitutionnel (I.8.4) est évaluée au niveau 3 et exige en outre des tests renforcés de continuité et de sortie, des exercices d'incident, un examen indépendant périodique, une inscription au registre public et une responsabilité exercée à un niveau hiérarchique élevé pour la continuité des obligations publiques essentielles.

III.3.4 Contexte de l'évaluation. Des conditions propres aux bailleurs de fonds, aux situations transfrontières, aux situations d'urgence, aux domaines sensibles en matière de sécurité ou à un secteur donné peuvent

ajouter des exigences. Elles n'abaissent jamais le niveau d'examen ni ne réduisent la profondeur de l'évaluation de fond. Une même mission n'est pas soumise à des exigences de droit public moindres au motif qu'une évaluation est commandée à des fins de financement.

III.3.5 Hors champ d'application. Une mission qui ne satisfait pas au test du champ d'application fonctionnel ne se voit pas attribuer de niveau d'examen. Elle fait l'objet de la fiche d'examen préalable décrite au point II.2.3.

III.4 Relevé de constatations

III.4.1 À chaque niveau d'examen, le résultat d'une évaluation est un relevé de constatations au regard de la Norme. Il indique : la mission et l'institution responsable; le niveau d'examen ainsi que l'identité et l'indépendance de l'évaluateur ou du vérificateur; le périmètre, les critères et les preuves retenus, ainsi que la date à laquelle les preuves ont été vérifiées; chaque constatation relative à un point de contrôle; les cotations des dix capacités et les niveaux de preuve; la confiance dans les preuves; la Décision institutionnelle adoptée par l'institution responsable, lorsqu'une telle décision a été adoptée; et la date du prochain réexamen.

III.4.2 Un relevé de constatations ne constitue ni un certificat, ni une marque de conformité, ni une déclaration de légalité, ni une déclaration de conformité d'un système. Ses constatations étayent la décision de l'institution compétente et ne la remplacent pas. L'achèvement d'une évaluation ne crée jamais de présomption de légalité. Un relevé n'est valable que pour le périmètre, la version et la date qui y sont consignés; la Norme ne reconnaît pas un relevé fondé sur une évaluation qui n'a jamais été consignée dans un Dossier à jour.

III.5 Formes d'adoption et effet juridique

III.5.1 Une autorité compétente peut donner effet à la Norme sous la forme d'une obligation légale; d'une instruction ministérielle ou administrative; d'une norme applicable au service public ou à l'administration de la justice; d'une exigence en matière de marchés publics; d'une méthode d'un régulateur; d'un référentiel d'un médiateur ou d'une institution d'audit; d'une exigence de sauvegarde d'un bailleur de fonds; ou d'une politique volontaire. Son effet juridique dépend de l'instrument d'adoption.

III.5.2 Un instrument d'adoption devrait indiquer l'organisme qui adopte la Norme et sa compétence, la version de la Norme adoptée, les missions couvertes et les conséquences internes du non-respect. Il distingue les obligations juridiques existantes des engagements supplémentaires pris au titre de la politique de l'institution.

III.5.3 Un instrument d'adoption devrait prévoir au minimum que :

- toute mission publique à médiation numérique envisagée ou substantiellement modifiée fait l'objet d'un examen préalable avant la passation du marché, le déploiement ou tout engagement de conception irréversible;
- l'autorité publique responsable est nommément désignée et ne peut transférer par contrat la responsabilité finale de droit public;

PROJET

- les missions relevant du niveau d'examen 3 et les missions critiques sur le plan constitutionnel font l'objet d'une évaluation indépendante ;
- les constatations relatives aux points de contrôle sont tenues distinctes des scores de risque et des avantages ;
- les évaluations spécialisées sont incorporées par renvoi et mises en cohérence dans une conclusion d'ensemble unique ;
- l'institution maintient les dix capacités conservées à un degré proportionné à l'incidence ;
- des résumés publics et des motifs individuels sont fournis, sous réserve des dérogations prévues par la loi ;
- le suivi, la réévaluation, la réponse aux incidents et la sortie sont des éléments obligatoires du cycle de vie ;
- le Dossier de la mission publique numérique constitue un document administratif officiel et est conservé comme tel.

III.5.4 La commande publique devrait garantir les dispositions en matière d'audit, de documentation, de contrôle des modifications, d'intervention, de continuité et de sortie qu'exigent les capacités. Les institutions de petite taille peuvent recourir à une expertise partagée ou cumuler des rôles, à condition que les conflits d'intérêts soient déclarés et qu'un examen critique indépendant soit préservé. Une institution devrait documenter la manière dont elle financera le personnel, l'examen, la participation et les tests, plutôt que de souscrire des obligations qu'elle n'a pas la capacité d'exécuter.

III.5.5 Une institution qui adopte la Norme devrait tenir un registre public indiquant, pour chaque mission évaluée, l'institution responsable, la date de l'évaluation, la version de la Norme appliquée, le niveau d'examen, la décision, le prochain réexamen et une voie de contestation accessible. Une structure de publication à deux niveaux peut protéger les éléments sensibles tout en servant l'obligation de rendre compte ; toute restriction à la divulgation exige un fondement légal et motivé ainsi qu'un accès approprié pour les contrôleurs indépendants compétents.

III.5.6 La DPLIA devrait être intégrée à la gouvernance existante plutôt que confiée à un bureau d'éthique isolé. La fonction de coordination peut être placée auprès d'un ministère de la justice, des services du chef du gouvernement, d'un service numérique de l'État, d'une institution supérieure de contrôle des finances publiques ou d'une unité interministérielle d'audit et de vérification ; la responsabilité opérationnelle demeure celle de l'autorité qui exerce la mission.

III.6 Participation et transparence

III.6.1 La participation commence avant que les choix importants ne soient arrêtés. Le Dossier indique qui a été entendu, de qui l'expérience fait encore défaut, ce qui a changé en conséquence et pourquoi les solutions de substitution ont été écartées. Les résumés publics permettent de repérer l'existence du dispositif ; les motifs propres à chaque cas et des voies de réclamation utilisables permettent le recours. La transparence opère à trois niveaux — registre, système et cas individuel — et une mention au niveau du registre ne satisfait pas à elle seule aux exigences de motivation ou de recours au niveau du cas individuel.

PROJET

III.7 Rapports avec d'autres instruments

III.7.1 Un organisme public peut satisfaire individuellement à chaque obligation sectorielle alors que la mission d'ensemble sur laquelle elles portent conjointement reste non évaluée. La Norme est conçue pour combler cette lacune, non pour concurrencer les instruments qui lui fournissent des preuves. Elle s'utilise parallèlement à ces instruments, comme suit.

Instrument	Preuves qu'il fournit	Ce que la Norme ajoute
Convention-cadre du Conseil de l'Europe sur l'intelligence artificielle et méthodologie HUDERIA	Contexte, participation, effets sur les droits de l'homme, la démocratie et l'État de droit, et mesures d'atténuation tout au long du cycle de vie de l'IA.	La couche de la légalité constitutionnelle et de la maîtrise institutionnelle : constatations relatives aux points de contrôle propres à chaque ordre juridique, capacités conservées et décision institutionnelle assortie de l'obligation de rendre compte, y compris pour les composants ne relevant pas de l'IA.
Analyse d'impact sur les droits fondamentaux au titre du règlement de l'UE sur l'IA (art. 27)	Groupes concernés, risques spécifiques de préjudice, contrôle humain, gouvernance et mécanismes de plainte, dans les limites de son champ d'application légal.	Responsabilités et dépendances à l'échelle de l'ensemble de la mission publique. La Norme ne remplace pas cette analyse d'impact.
Exigences du règlement de l'UE sur l'IA applicables aux systèmes d'IA à haut risque	Preuves relatives aux exigences techniques et organisationnelles propres au système d'IA.	Évaluation de la mission publique d'ensemble plutôt que du système pris isolément.
Analyse d'impact relative à la protection des données au titre du RGPD (art. 35)	Finalités du traitement, nécessité, risques, garanties et réexamen.	Habilitation institutionnelle, dépendances sans lien avec le traitement, recours d'ensemble, continuité et sortie.
ISO/IEC 42001	Preuves de la gouvernance de l'IA au sein de l'organisation.	Les deux répondent à des questions différentes. La certification ISO/IEC 42001 est un élément de preuve pertinent, non la démonstration de la légalité.
Gestion des risques en matière de cybersécurité au titre de la directive SRI 2 (NIS 2)	Résilience des réseaux et des systèmes d'information.	Légalité, droits et obligation de rendre compte pour la mission que ces systèmes soutiennent.
Évaluation de l'interopérabilité au titre du règlement pour une Europe interopérable	Effets juridiques, organisationnels, sémantiques et techniques sur l'interopérabilité transfrontière.	La question de savoir si une personne concernée peut exercer un droit dans des conditions d'égalité une fois que les systèmes échangent des données ; responsabilité d'ensemble et continuité.

Instrument	Preuves qu'il fournit	Ce que la Norme ajoute
Directive sur la prise de décisions automatisée (Canada) et évaluation de l'incidence algorithmique (EIA)	Niveaux d'incidence, consultation juridique, tests, examen et recours.	Preuves à l'échelle de la mission lorsque la médiation numérique dépasse le champ institutionnel ou le champ des systèmes couverts par la Directive.
Cadre de gestion des risques liés à l'IA du NIST (AI RMF)	Preuves et pratiques volontaires de gestion des risques liés à l'IA.	Obligations de droit public applicables et leurs conséquences pour la décision institutionnelle.

Tableau III.4. Rapports avec d'autres instruments.

III.7.2 Les instruments existants favorisent déjà l'intégration : une analyse d'impact relative à la protection des données (AIPD) peut porter sur un ensemble d'opérations de traitement similaires, et le règlement sur l'IA prévoit expressément que l'analyse d'impact sur les droits fondamentaux complète l'AIPD.

III.7.3 L'approche large de la méthodologie HUDERIA en matière de droits et d'État de droit est une source d'analyse de fond compatible, et son caractère non contraignant ne diminue en rien la valeur de sa méthodologie. L'évaluation de l'incidence algorithmique du Canada intègre déjà un examen tout au long du cycle de vie du système. La DPLIA s'appuie sur ces travaux et ne revendique pas l'analyse du cycle de vie comme une contribution exclusive.

PROJET

Partie IV — Gestion de la Norme et mise en œuvre par le droit souple

IV.1 Gestionnaire et dénomination

IV.1.1 La gestion de la Norme est assurée par l'Institute for Digital Society and Future Public Law (l'« Institut ») conformément au Règlement de l'Institut. Jusqu'à l'approbation visée au point IV.1.2, la Norme est désignée comme « Le pouvoir sur le code : Norme de droit public numérique de l'Institut », avec la mention « projet soumis à consultation » jusqu'à son adoption.

IV.1.2 La Norme ne peut être désignée comme norme de l'EPLO ou norme provisoire de l'EPLO, ou comme approuvée par l'EPLO, qu'après son approbation par le Comité exécutif de l'EPLO conformément au Règlement relatif aux normes de l'EPLO. L'approbation ne modifie pas le texte de la Norme.

IV.2 Consultation, adoption et modification

IV.2.1 L'adoption et la modification sont régies par l'article IV, paragraphe 3, point f), du Règlement de l'Institut, en vertu duquel le Conseil scientifique adopte les normes et méthodologies de l'Institut sur proposition du Directeur, ainsi que par la Décision du Conseil scientifique relative à la procédure d'élaboration et d'adoption des normes de l'Institut ; le Règlement relatif aux normes de l'EPLO s'applique également. En vertu de ces dispositions :

- une nouvelle version est soumise à une consultation publique d'au moins soixante (60) jours, et toute autre modification de fond à une consultation publique d'au moins trente (30) jours, et la suite donnée à chaque observation est publiée ;
- la Norme, ainsi que toute modification de celle-ci, est adoptée par le Conseil scientifique sur proposition du Directeur, sans la participation des membres qui y ont un intérêt, y compris ses auteurs ;
- chaque version adoptée porte un numéro de version et une date et est inscrite dans un registre public tenu par l'Institut.

IV.2.2 Chaque modification est publiée avec ses motifs et un état des exigences modifiées. Elle précise son effet sur les évaluations déjà achevées ou en cours ainsi que toute disposition transitoire. Les relevés de constatations indiquent la version de la Norme appliquée.

IV.2.3 Le gestionnaire de la Norme publie ses responsabilités, ses procédures de participation, ses règles en matière de conflits d'intérêts et l'historique des versions. La gestion de la Norme associe des institutions publiques, des spécialistes du droit et de la technique, les communautés concernées et des chercheurs indépendants.

IV.3 Outils de mise en œuvre relevant du droit souple

IV.3.1 La Norme est mise en œuvre au moyen d'outils de droit souple : principes directeurs ; clauses types et dispositions réglementaires types ; avis consultatifs de l'Institut ; appels à observations ; commentaires et

PROJET

notes interprétatives; guides de formation et de pratique; et déclarations d'interopérabilité avec les instruments d'organisations intergouvernementales.

IV.4 Évaluation, audit et validation de la conformité

IV.4.1 Les évaluations, audits et validations de la conformité réalisés par l'Institut ou pour son compte reposent sur un périmètre convenu, des critères définis et des preuves vérifiables. L'Institut présente ses constatations sous la forme de relevés au regard de la Norme (III.4). Ceux-ci étayent la décision de l'institution compétente, mais ne la remplacent pas.

IV.4.2 Toute attestation publique de résultats à l'initiative de l'Institut requiert une décision distincte du Comité exécutif de l'EPLO.

IV.5 Effet juridique et statut public

IV.5.1 La Norme n'est pas juridiquement contraignante, sauf si une autorité compétente lui donne effet par son propre instrument (III.5). Ni la Norme ni aucun relevé de constatations ne confère de pouvoir juridique, ne crée de présomption de légalité, ni ne donne à l'Institut ou à un évaluateur un statut public réservé.

IV.6 Certification de personnes

IV.6.1 Lorsqu'un organisme de certification des compétences des personnes sera créé, la certification s'exercera dans le respect d'un cloisonnement garantissant l'impartialité entre la formation, l'évaluation et la certification, fixé par la décision portant création de cet organisme.

PROJET