

« Sovereignty is your alpha »

Palantir ou la « souveraineté »
hémiplogique

PAR FRANCE CHARRUYER



Annette Messager, Chaos, 2008. Illustration de la chronique originale.

Le livre blanc publié par Palantir début juillet 2026, *Institutional Sovereignty in the Age of AI*, nous offre une démonstration de souveraineté hémiplogique : une thèse pour se protéger des fournisseurs de modèles, zéro ligne sur le droit qui oblige ces fournisseurs. L'analyse de Palantir relative aux couches technique et contractuelle est robuste (rétention des données, poids des modèles, matériel), mais singulièrement amnésique sur la couche juridictionnelle (portée des lois extraterritoriales de type FISA ou Cloud Act, réquisitions et autres immunités). La carte analytique que nous livre Palantir (le risque vient des fournisseurs de modèles) et la nôtre (le risque vient aussi du droit d'accès étatique) sont hélas deux cartes du même territoire ; chacune éclaire ce que l'autre masque.

De quoi la souveraineté est-elle le nom ?

Avant d'ouvrir le manifeste, reprenons le mot au sérieux. La souveraineté n'est pas un mot-valise pour vendre des services : c'est une catégorie du droit politique, et elle a un contenu précis. Bodin la définit en 1576 comme la « puissance absolue et perpétuelle d'une République », dont la première marque est de donner la loi à tous sans le consentement de personne. Carl Schmitt en livre en 1922 le critère resté canonique : est souverain celui qui décide de la situation exceptionnelle (*Théologie politique*). Marc Sztulman, dans sa chronique « La mort du souverain », en tire la version opérationnelle pour notre temps : est souverain celui qui détient la possibilité de déroger à la règle de droit ; celui qui peut suspendre la norme, le contrat, le service, et à qui nul ne peut l'opposer.

Le test de souveraineté n'est donc pas « qui administre ? » mais « qui peut déroger ? ». Qui détient le pouvoir d'exception. Retenons ce critère : il servira de pierre de touche à chaque page du manifeste de Palantir. Car une « souveraineté » qui laisse à autrui le pouvoir d'exception n'est pas amputée d'un détail ; elle est amputée de sa définition.

La souveraineté en étendard US

Il fallait s'y attendre : le mot « souveraineté », longtemps moqué comme une lubie continentale, est devenu un argument de vente à Denver. Début juillet 2026, Palantir a publié un manifeste appelant gouvernements et entreprises à protéger leur « alpha » face aux laboratoires d'IA. Ce texte formalise la critique portée publiquement par Alexander Karp contre OpenAI et Anthropic, accusés de bâtir les modèles de fondation et de siphonner la chaîne de valeur.

Disons-le sans détour : ce texte mérite d'être lu, et pris au sérieux. Il nomme avec une précision rare des mécanismes que cette chronique décrit depuis des mois sous d'autres noms. L'écosystème prédateur des LLM est tout entier tourné vers l'extraction (*Extraction-Prone Model*). Pour rappel, tout modèle de frontière utilisé sans accord de non-rétention (le fameux ZDR), cousin industriel de ce que nous appelons le droit à la

non-distillation, génère un risque de dépossession des savoir-faire de l'organisation. La migration du « savoir tribal » vers les poids des modèles est une description opérationnelle de ce transfert de valeur. Et le texte a pour mérite de livrer trois réflexes immédiatement utiles au praticien.

Premier réflexe : la faille des métadonnées dans les accords de non-rétention (*Zero Data Retention*). Un accord ZDR garantit que ni les requêtes ni les sorties ne sont conservées ; mais, relève Palantir, les journaux des classifieurs de sécurité — ceux-là mêmes qui lisent vos entrées et sorties pour en dériver des scores — échappent souvent au périmètre contractuel du « contenu client » et peuvent persister, selon le livre blanc, jusqu'à deux ans (sic). Si la donnée est bien effacée, sa trace dérivée, elle, demeure. Toute clause de confidentialité IA devrait désormais couvrir explicitement ces vecteurs auxiliaires — pour autant que les utilisateurs se posent les bonnes questions.

Deuxième réflexe : la hiérarchie des garanties. La garantie *structurelle* (isolement physique, enclaves attestées par le matériel) en vient à primer la garantie *contractuelle* (la promesse d'un fournisseur). Cela reste une grille d'audit que tout responsable de traitement peut transposer : classer chaque flux de travail selon le niveau de garantie qu'exige la sensibilité des données.

Troisième réflexe : la « réversibilité » des modèles. Pouvoir changer de fournisseur sans friction n'est pas une commodité d'achat, c'est un levier de négociation permanent — et la condition pour que les engagements contractuels restent crédibles.

Le « flywheel » en boucle de rétroaction

Le concept central du manifeste est le *flywheel* : l'usage génère du signal, le signal structuré devient savoir-faire, le savoir-faire améliore le système, le système génère plus d'usage. Le diagnostic est juste : celui qui capte la boucle capte la valeur ; si la capture s'opère chez le fournisseur de modèles, l'organisation offre son avantage compétitif à un tiers qui le revendra, y compris à ses concurrents.

La structure de ce manifeste est limpide : la « couche de contrôle » que le texte érige en siège de la souveraineté (ontologie, permissions granulaires, journaux d'audit, orchestration) est la description exacte du produit Palantir. Le texte prêche le *zero trust* envers les laboratoires d'IA et demande, dans le même mouvement, une confiance entière envers l'éditeur de la couche où résident précisément le jumeau numérique de l'organisation, ses flux de travail et son savoir tribal. C'est déplacer la dépendance d'un étage, non la supprimer. Jacques Ellul l'aurait reconnu au premier regard : la technique qui pose problème appelle une solution technique, qui appelle à son tour sa propre couche de garantie ; l'auto-accroissement du système technicien, ici vendu comme son remède.

Et le texte le concède presque : l'auditabilité de ce que le fournisseur fait de vos données se réduit, admet-il, à un simple rapport SOC 2 remis sous accord de confidentialité, qui n'atteste rien de l'entrée éventuelle de vos données dans un pipeline d'entraînement. La reddition de comptes — et, modestement, le fait de pouvoir rendre compte de sa gestion (C. civ., art. 1993) ; est hélas ici structurellement impossible... Qui peut répondre de ses actes, de ses manquements, de ses erreurs ou de ses incidents, avec une auditabilité en peau de chagrin ?

La loi qui oblige ?

Dans un manifeste entièrement consacré à empêcher des tiers d'accéder à vos données, deux mots n'apparaissent jamais : *Cloud Act* et *FISA* et autres friandises extraterritoriales en mode patriote.

Le CLOUD Act du 23 mars 2018 permet aux autorités américaines d'exiger d'un fournisseur soumis à la juridiction des États-Unis la remise de données qu'il contrôle, où qu'elles soient stockées dans le monde. La Section 702 du *Foreign Intelligence Surveillance Act* autorise la collecte, sans mandat individualisé, des communications de personnes non américaines situées hors des États-Unis, avec le concours obligé des fournisseurs de services américains.

L'actualité de l'été 2026 rend ce silence assourdissant. Reconduite en avril 2024 par le *Reforming Intelligence and Securing America Act* avec une clause d'extinction au 20 avril 2026, la Section 702 a expiré en juin 2026, le Congrès n'ayant pas trouvé d'accord malgré deux prolongations techniques. Et pourtant c'est le point que tout juriste européen doit méditer, la surveillance continue. Les certifications programmatiques approuvées par la Cour FISA en mars 2026 restent valides jusqu'à leur terme, vers mars 2027, en vertu des dispositions transitoires ; les injonctions adressées aux fournisseurs demeurent contraignantes, sous peine d'astreintes pouvant atteindre 250 000 dollars par jour.

Relisons l'épisode avec le critère du préambule : une loi expire, la surveillance qu'elle fondait se poursuit, et les acteurs privés restent tenus d'y concourir. Qui a dérogé à la règle ? Qui a décidé de l'exception ? Ni le fournisseur, ni son client : l'État qui a juridiction sur eux. Voilà le souverain, au sens propre ; et il n'est pas dans le livre blanc.

Méditons la leçon. **Une loi de surveillance américaine expirée continue de produire ses effets ; un contrat de non-rétention en vigueur cesse de produire les siens dès qu'une loi le lui ordonne.** Le ZDR promet que rien n'est conservé *par le fournisseur pour ses propres fins* ; il ne promet rien et d'ailleurs il ne peut rien promettre contre une injonction fondée sur le droit américain, à laquelle le fournisseur est tenu de déférer. L'assurance contractuelle dont Palantir démontre brillamment la faiblesse face aux fournisseurs de modèles souffre exactement de la même faiblesse face à l'État qui a juridiction sur... Palantir. Le *zero trust* s'arrête à Denver.

Le dernier chapitre du manifeste lève toute ambiguïté sur sa grille de lecture : après moult thèses sur l'autonomie institutionnelle, le texte s'achève sur un appel aux armes // *a call to arms* // en faveur de modèles à poids ouverts *américains*. La souveraineté qu'on vous propose est celle d'un locataire : libre de réaménager les pièces, jamais de choisir la loi du bailleur.

Comment compléter l'hémisphère manquant

La réponse n'est pas de jeter le manifeste, c'est peut-être de le compléter. Ses outils sont bons ; sa carte est amputée. À la grille de Palantir (rétention, poids, matériel), le lecteur européen doit superposer une seconde grille, faite de critères fonctionnels objectifs et vérifiables : sous quelle juridiction le fournisseur peut-il être contraint de remettre ou d'intercepter des données ? Quelles immunités juridictionnelles l'architecture garantit-elle réellement — chiffrement dont les clés échappent au fournisseur, hébergement qualifié, séparation des systèmes d'information ? Quelle réversibilité effective, mesurée en jours et en coûts de sortie ? Quelle auditabilité par un tiers indépendant, au-delà du rapport SOC 2 sous NDA ?

Ce ne sont pas des préférences d'origine ; ce sont des exigences de preuve. Elles s'appliquent à tout fournisseur, de toute nationalité , y compris, du reste, à Palantir, dont l'offre isolée sur site répond mieux à certains de ces critères que le « nuage » de bien des concurrents. La souveraineté ne se décrète pas par le drapeau ; elle se démontre par l'architecture et par le droit applicable.

Reste la question du telos, qu'Aristote nous oblige à poser : souveraineté *pour quoi* ? Le manifeste répond « alpha » : la souveraineté comme rendement, l'autonomie comme avantage compétitif. C'est la colonisation du monde vécu diagnostiquée par Habermas, appliquée à la souveraineté elle-même : une catégorie politique, soit la capacité d'un corps collectif à se donner sa propre loi reformatée, pour la bonne cause, en catégorie financière. Or la souveraineté d'une entreprise , d'une institution de santé, d'un département, d'un cabinet d'avocats ne se mesure pas en points de base : elle se mesure à la capacité de continuer à décider, à protéger le secret qui lui est confié, à répondre de ses actes. L'alpha est un sous-produit ; l'imputabilité est la fin.

La souveraineté hémiplegique protège vos données de tout le monde, sauf de la loi de celui qui les héberge. Compléter l'hémisphère manquant , juridictionnel, probatoire, politique ,

n'est pas un luxe doctrinal européen : c'est la moitié du corps sans laquelle l'autre ne tient pas debout.

Un monde où rien n'est retenu (notamment par la *discovery*), dont le manifeste se félicite qu'elle ne puisse atteindre la donnée jamais stockée est aussi un monde où rien ne peut être prouvé.

La souveraineté par l'effacement dissout la traçabilité, deuxième maillon du fil de cette série de chroniques sur le chaos numérique ambiant, et avec elle la possibilité même de l'imputabilité. Le manifeste Palantir le reconnaît sans le vouloir : sans traçabilité robuste, écrit-il, aucun lien de causalité ne pourra jamais être établi entre vos données et les capacités d'un modèle de frontière. Identifiabilité, traçabilité, imputabilité : le chaos numérique n'est pas l'absence de protection, c'est l'abondance de protections qui, chacune, déplace la preuve hors de portée.

Quand le pouvoir d'exception migre dans la loi d'un autre, le souverain ne s'affaiblit pas, il meurt. Ce que Palantir vend sous ce nom en est le masque mortuaire, techniquement admirable. La souveraineté qui compte n'est pas celle qui efface les traces ; c'est celle qui décide, en pleine lumière, de la règle, de son exception et de qui répond de quoi.

France Charruyer, avocat associé fondateur Altij Avocats, présidente de l'association Data Ring

Sources : Palantir, Institutional Sovereignty in the Age of AI (juill. 2026) ; M. Sztulman, « La mort du souverain » ; J. Bodin, Les Six Livres de la République; C. Schmitt, Théologie politique; Brennan Center (avr. 2026) ; Cato Institute (11 juin 2026) .

SOURCE ORIGINALE

france-charruyer.fr · Lire la chronique en ligne