

# Palantir Technologies

L'entreprise qui veut voir tout, partout, toujours

Stéphane FOSSE

[fosse.fr](http://fosse.fr)

15 mai 2026

Copyright : cette œuvre est libre, vous pouvez la copier, la diffuser et la modifier  
selon les termes de la [Licence Art Libre](#)

Palantir Technologies est une entreprise américaine de logiciels d'analyse de données et d'intelligence artificielle fondée en 2003 à Palo Alto par Peter Thiel, Alex Karp, Joe Lonsdale, Stephen Cohen et Nathan Gettings. Son nom est emprunté aux pierres de vision du légendaire de Tolkien : des objets qui permettent de tout voir, loin. En vingt ans, Palantir est passée d'une startup financée par la CIA à une société cotée au New York Stock Exchange valorisée à plus de 300 milliards de dollars en 2026, avec des revenus qui dépassent 4 milliards de dollars annuels en 2025. C'est aussi l'entreprise que l'ACLU, Amnesty International et l'Electronic Frontier Foundation désignent comme l'infrastructure centrale de la surveillance d'État américaine.

## 1 Quelles sont les origines de Palantir et son lien avec la CIA ?

L'histoire commence après le 11 septembre 2001. Peter Thiel, cofondateur de PayPal, observe que les algorithmes de détection de fraude qu'il avait développés pour les transactions financières pourraient s'appliquer à la détection de réseaux terroristes. L'idée est simple : si on peut identifier une transaction frauduleuse dans un flux de millions d'opérations, on peut identifier un individu dangereux dans un flux de millions de données. Ce raisonnement, aussi séduisant qu'il est contestable, est à l'origine de Palantir.

La société est formellement constituée le 6 mai 2003. Thiel y investit une trentaine de millions de dollars de ses propres fonds. Mais le véritable tournant arrive en 2004-2005, quand In-Q-Tel, le fonds de capital-risque de la CIA, injecte 2 millions de dollars dans la startup. Ce montant est modeste, mais le signal est décisif : les ingénieurs de Palantir passent les années suivantes à travailler directement avec des analystes de la CIA pour affiner leur premier produit, Gotham, un système de visualisation de réseaux de données. Les premières grandes agences clientes sont le FBI, la NSA et le Département de la Défense. Palantir ne vend pas un logiciel sur étagère : elle embauche des ingénieurs déployés directement chez ses clients, les Forward Deployed Engineers (FDE), qui vivent dans les organisations pour construire des workflows sur mesure et s'y rendre indispensables.

Cette stratégie mérite qu'on s'y arrête. Elle ressemble moins à du SaaS qu'à une implantation chirurgicale. L'organisation cliente ne s'abonne pas à un outil : elle laisse des ingénieurs Palantir construire, dans ses propres murs, une couche d'abstraction de toutes ses données. Une fois l'ontologie en place, les coûts de migration deviennent prohibitifs. Le New York City Police Department l'a appris à ses dépens en 2017, quand il a tenté de rompre son contrat et s'est retrouvé face à Palantir qui refusait de livrer ses données dans un format standard.

## 2 Comment fonctionnent les plateformes Palantir ?

Palantir opère aujourd'hui avec quatre plateformes intégrées. Gotham est le produit originel, conçu pour les services de renseignement et les forces de l'ordre : il cartographie les connexions entre personnes, lieux, événements et objets, en agrégeant des données issues de bases hétérogènes. Foundry, la plateforme commerciale, fait la même chose pour les grandes entreprises — logistique, santé, finance — en unifiant des systèmes de données fragmentés. Apollo est le système de déploiement continu qui permet à Palantir d'opérer dans n'importe quel environnement : cloud public, infrastructure sur site, edge computing embarqué sur un drone ou un sous-marin. C'est Apollo qui permet à Palantir de déployer ses logiciels dans des environnements classifiés sans jamais perdre le contrôle des mises à jour.

En avril 2023, Palantir lance AIP, l'Artificial Intelligence Platform, qui intègre les grands modèles de langage — dont les modèles d'Anthropic — dans des environnements classifiés de niveau Impact Level 6. C'est la brique qui permet à un analyste militaire d'interroger en langage naturel des masses de données satellitaires ou d'imagerie

de drones, et d'obtenir en retour des synthèses, des recommandations de cibles, des options de frappe. AIP a valu à Palantir une croissance de ses revenus commerciaux américains de plus de 80 % en 2025.

Au centre de tout cela se trouve l'ontologie — le concept le plus important pour comprendre ce que Palantir vend vraiment. Ce n'est pas du data warehouse, ce n'est pas de la BI classique. L'ontologie est une couche sémantique qui transforme des données brutes en objets métier cohérents : un employé, un aéronef, un suspect, un patient. Elle crée un jumeau numérique de l'organisation cliente et connecte automatiquement « John Smith » dans les fichiers RH à « jsmith » dans les logs d'accès et à l'identifiant fiscal correspondant. Une fois que l'ontologie d'une organisation est construite dans Palantir, elle contient la logique opérationnelle de toute l'organisation. En sortir coûte plus cher que d'y rester.

### 3 Quels sont les contrats militaires de Palantir avec le Pentagone et l'OTAN ?

Maven Smart System (MSS) est la plateforme de ciblage militaire développée par Palantir pour le Pentagone, héritière du projet Maven lancé en 2017 — celui que Google avait abandonné en 2018 après la révolte interne de ses ingénieurs. Palantir a comblé le vide. Maven agrège des données satellitaires, des flux de drones, des radars, des capteurs et des rapports de renseignement, puis utilise l'apprentissage automatique pour identifier des cibles potentielles — véhicules, bâtiments, dépôts d'armes — en quasi-temps réel.

En mai 2024, le Pentagone signe un contrat Maven à 480 millions de dollars avec Palantir. Le plafond est rehaussé à 1,3 milliard de dollars en mai 2025. En juillet 2025, l'US Army fusionne 75 contrats existants en un accord-cadre de 10 milliards de dollars sur dix ans. En mars 2026, le sous-secrétaire à la Défense Steve Feinberg signe une lettre classant Maven comme programme officiel du Département de la Défense, garantissant des financements pluriannuels et forçant son adoption dans toutes les branches militaires. Dans une présentation publique, un responsable du bureau IA du Pentagone annonce que d'ici juin 2026, Maven transmettra « 100 % d'intelligence générée par machine » aux commandants militaires, sans intervention humaine dans la boucle de dissémination.

Le 25 mars 2025, l'OTAN signe avec Palantir un accord pour déployer MSS NATO dans ses opérations — l'une des acquisitions technologiques les plus rapides de l'alliance, six mois de l'idée à la signature. Le Royaume-Uni s'engage de son côté en décembre 2025 avec un contrat de 240 millions de livres sterling au Ministère de la Défense, sans appel d'offres compétitif. Le PDG Alex Karp a déclaré publiquement en 2023 que Palantir était « responsable de la majorité du ciblage en Ukraine ». Ses logiciels sont intégrés dans plus d'une demi-douzaine d'agences ukrainiennes depuis l'invasion russe de 2022, agrégeant imagerie satellitaire, données open source et rapports de terrain pour présenter aux commandants des options de frappe.

Des experts des Nations Unies ont mis en garde contre les risques éthiques et juridiques d'un ciblage automatisé sans supervision humaine réelle. Les biais des données d'entraînement peuvent avoir des conséquences létales sur le terrain. Palantir maintient que ses logiciels ne prennent jamais de décision de mise à mort et que des humains approuvent chaque cible. Mais quand un système identifie 1 000 cibles en 24 heures — comme lors des frappes contre l'Iran en 2026 — il est légitime de s'interroger sur la profondeur réelle de cette supervision.

### 4 Comment Palantir est-il utilisé pour surveiller et expulser des migrants aux États-Unis ?

ICE, l'agence américaine d'immigration, est un client de Palantir depuis 2011. La relation s'est considérablement approfondie sous l'administration Trump. En 2026, quatre produits Palantir forment l'épine dorsale de la machine d'expulsion américaine.

ELITE (Enhanced Leads Identification and Targeting for Enforcement) affiche sur une carte les cibles potentielles pour la déportation, avec leur adresse, un score de confiance de localisation, leur photo et leur numéro d'étranger. Selon un guide utilisateur obtenu par 404 Media, le système permet aussi d'identifier des zones « riches en cibles » où les agents peuvent le plus efficacement remplir leurs quotas d'arrestation. Un témoignage sous serment en Oregon révèle qu'ICE utilise ELITE pour planifier des opérations de rafle, en s'appuyant notamment sur des données du Département de la Santé, y compris des données Medicaid. Le guide opérateur contient une instruction qui désactive les filtres pour « afficher toutes les cibles dans un jeu de données d'opérations spéciales » — une fonctionnalité que Palantir décrit comme marginale dans ses communications publiques.

ICM (Investigative Case Management), géré par Palantir depuis 2014, est le système de gestion de cas d'ICE. Il agrège, pour chaque individu dans le système d'immigration américain, la scolarité, les relations familiales, l'employeur, les relevés téléphoniques, l'historique d'immigration, les données biométriques, le casier judiciaire et les adresses. Un document de financement précise que les citoyens américains sont également inclus dans

l'ICM, dès lors qu'ils font l'objet d'une procédure pénale. En 2017, cette technologie a servi à arrêter des parents d'enfants non accompagnés. En août 2019, elle a planifié les raids du Mississippi qui ont séparé des enfants de leurs familles.

En avril 2025, ICE signe avec Palantir un contrat de 30 millions de dollars pour ImmigrationOS, une augmentation de l'ICM articulée autour de trois fonctions : prioriser les arrestations, tracer en quasi-temps réel les « auto-déportations », et gérer l'ensemble du cycle de vie d'une expulsion de l'identification au renvoi. Le CTO de Palantir a envoyé un message Slack interne décrivant comment l'entreprise avait « prototypé un nouvel ensemble d'intégrations de données et de flux de travail avec ICE » en quelques semaines. La révélation que Stephen Miller, architecte en chef de la politique d'immigration de l'administration Trump, détient une participation financière substantielle dans Palantir ajoute une couche de conflit d'intérêts rarement documentée.

Le quatrième produit, un système de traitement des dénonciations par IA générative, analyse et traduit automatiquement les signalements reçus par ICE. C'est probablement une évolution de FALCON, utilisé depuis 2012.

L'ACLU, l'EFF et Amnesty International ont toutes documenté cet arsenal. Amnesty a conclu que les capacités d'ImmigrationOS correspondent au système décrit sous le nom « Catch and Revoke » — surveillance des réseaux sociaux, suivi du statut de visa et évaluation automatisée des menaces conduisant à des révocations arbitraires. L'EFF a adressé une lettre formelle à Palantir, en demandant comment ses engagements en matière de droits humains s'appliquaient à ces pratiques. La réponse de Palantir est restée dans le vague, insistant sur la conformité légale plutôt que sur les résultats concrets. La conformité légale n'est pas un standard en matière de droits humains : c'est le plancher minimum, pas le plafond.

## 5 Qu'est-il arrivé avec la police prédictive à La Nouvelle-Orléans ?

En 2012, Palantir approche la ville de La Nouvelle-Orléans via James Carville, consultant politique, en utilisant comme intermédiaire l'initiative philanthropique NOLA for Life du maire Mitch Landrieu. Sans appel d'offres, sans vote du conseil municipal, sans information du public, Palantir déploie un système de police prédictive qui reste opérationnel jusqu'en 2018. L'histoire ne sera rendue publique que par une investigation de The Verge en 2018.

Le système repose sur une analyse de réseau social : il croise casiers judiciaires, activités sur les réseaux sociaux, affiliations supposées à des gangs, et établit des connexions entre individus pour attribuer des scores de risque. Des études ont montré qu'un tel modèle, entraîné sur des données policières historiquement biaisées, reproduit et amplifie ces biais : les quartiers noirs et pauvres sont surreprésentés dans les données d'entrée, donc surciblés en sortie. Une étude de 2016 a démontré qu'un algorithme comparable ciblait les quartiers à majorité noire à deux fois le taux des quartiers blancs pour des infractions liées aux drogues, alors que les enquêtes de santé publique ne montrent aucune différence significative dans les taux de consommation réels.

La Harvard Civil Rights-Civil Liberties Law Review a pointé la contradiction fondamentale de l'affaire : Palantir, en tant qu'entreprise privée, n'est soumise à aucune obligation de transparence comparable à celle d'un service de police public. L'algorithme est propriétaire. Les paramètres sont confidentiels. Les recours légaux pour un individu ciblé à tort sont quasi inexistants. Des structures comparables sont en place dans Los Angeles — où elles ont aussi été abandonnées après une protestation publique — et en 2024, Palantir fournit des outils d'investigation IA à onze forces de police britanniques.

## 6 Pourquoi l'expansion de Palantir dans le NHS britannique suscite-t-elle une résistance ?

Palantir entre dans le NHS en mars 2020 avec un contrat à 1 livre sterling pour gérer les données Covid-19. Cette entrée à prix symbolique est précisément ce que les critiques appellent la stratégie « land and expand » : décrocher un pied dans la porte, rendre le produit indispensable, puis facturer. En novembre 2023, NHS England lui attribue un contrat de 330 millions de livres sterling sur sept ans pour la Federated Data Platform (FDP), une plateforme unifiée de données de santé. Le contrat est lourdement caviardé — 200 pages entièrement noircies dans les sections relatives à la protection des données personnelles.

Une investigation publiée en janvier 2026 par The Nerve recense au moins 34 contrats passés entre Palantir et des entités publiques britanniques : NHS, Met Police, GCHQ, Ministère de la Défense, Home Office, conseils locaux. La valeur totale dépasse 670 millions de livres. Le réseau d'influence inclut Peter Mandelson, ancien ambassadeur du Royaume-Uni aux États-Unis, dont le cabinet de conseil Global Counsel est client de Palantir, et qui aurait facilité le contrat de 240 millions de livres du MoD signé sans appel d'offres.

Les inquiétudes sont concrètes. La technologie de Palantir est conçue pour traverser les silos de données. Ce qui est légalement séparé aujourd'hui peut devenir techniquement interconnectable demain si le cadre légal change. Le parti Reform UK a déjà proposé une législation pour permettre le partage automatique de données

entre le Home Office, le NHS, le HMRC et la police, explicitement dans le but de faciliter des expulsions massives. Le vice-président UK de Palantir a déclaré devant l'Enquête Covid en mars 2025 que les ministres devraient investir dans un système capable « d'intégrer les multiples systèmes sources à travers les administrations locales et centrales, les soins de santé et les autres organismes d'importance stratégique nationale ». C'est précisément ce qu'il vend.

L'Association Médicale Britannique a voté en 2025 contre le déploiement de la FDP. En février 2026, elle demande aux médecins de limiter leur engagement avec la plateforme. Cinquante mille patients ont écrit à leurs conseils de santé locaux pour s'y opposer. Moins d'un quart des 215 hôpitaux anglais utilisaient activement la FDP fin 2024, largement à cause de lacunes fonctionnelles reconnues.

## 7 Quelle est l'idéologie de Peter Thiel et comment influence-t-elle Palantir ?

Pour comprendre Palantir, il faut comprendre Peter Thiel. Il est co-fondateur de PayPal avec Elon Musk, fondateur de Founders Fund, premier investisseur institutionnel dans Facebook, et principal bailleur de fonds de Donald Trump en 2016 (1,25 million de dollars) puis de J.D. Vance. Il a déclaré en 2009 dans un essai pour le Cato Institute : « Je ne crois plus que liberté et démocratie sont compatibles. » Ce n'était pas une provocation : c'était un programme.

Thiel se réclame du libertarianisme mais construit des outils de surveillance d'État à grande échelle. La contradiction n'en est pas une, selon l'analyse du politologue Christopher Marquis : Thiel ne s'oppose pas à l'État concentré, il s'oppose à un État dont lui et ses alliés ne contrôlent pas les leviers. Ce que Palantir incarne dans cette lecture n'est pas la liberté individuelle, mais un transfert de la souveraineté de l'État vers une élite technique privée — des ingénieurs qui codent, pas des fonctionnaires élus, décident qui est suspect, qui est ciblé, qui est expulsé.

Patrick Eddington, ancien analyste de la CIA aujourd'hui au Cato Institute, a résumé la filiation idéologique avec une clarté qui mérite d'être citée : « Total Information Awareness, c'est ce qu'est Palantir maintenant. Ce qu'ils essayaient littéralement de faire, c'est concevoir la capacité d'ingérer des données de pratiquement n'importe quelle source et de les confronter à leur liste de cibles. » Total Information Awareness était le programme de surveillance de masse de la DARPA lancé après le 11 septembre 2001 — et que le Congrès américain avait supprimé en 2003 précisément pour des raisons de libertés civiles. Palantir a été fondée la même année par des personnes qui avaient rencontré John Poindexter, le directeur licencié du programme TIA, et qui trouvaient l'idée intéressante.

Alex Karp, le PDG, se décrit comme un « patriote américain ». Il a publiquement déclaré que Palantir « est responsable de la majorité du ciblage en Ukraine », et que les logiciels sont « en guerre, en Europe et dans le monde entier ». Il a présenté le travail de Palantir comme une obligation morale envers l'Occident. Cette rhétorique — le logiciel comme vecteur de valeurs civilisationnelles — mérite d'être examinée avec soin : quand le code devient politique étrangère, la question de la gouvernance démocratique de ce code devient urgente.

## 8 Quels sont les risques structurels posés par Palantir pour les sociétés démocratiques ?

Palantir construit des couches d'ontologie dans les organisations étatiques. Ces couches survivent aux changements d'administration, aux alternances politiques, aux scandales. Quand une agence déclare qu'elle ne peut pas rompre son contrat parce que « Palantir reste le seul fournisseur capable de satisfaire les besoins spécifiques d'ICE » — formulation utilisée pour justifier un contrat sans appel d'offres — elle décrit une dépendance architecturale. L'État n'est plus propriétaire de sa propre infrastructure de décision.

Le deuxième risque est algorithmique. Un système comme ImmigrationOS ou ELITE prend des décisions sur des individus à partir de données agrégées dont la véracité n'est jamais garantie. L'American Immigration Council rappelle que l'algorithme COMPAS, utilisé dans le système judiciaire américain, identifiait les accusés noirs comme deux fois plus à risque de récidive que les accusés blancs à profil comparable. Ce n'étaient pas des erreurs techniques : c'étaient des choix de conception. Chez Palantir, le code est propriétaire. L'audit est impossible. Le recours pour l'individu ciblé à tort est quasi inexistant.

Le troisième risque est politique. Palantir ne choisit pas ses clients — elle déclare avoir des politiques de droits humains, mais aucun mécanisme externe ne les fait respecter. L'EFF a documenté l'écart entre les engagements publics de Palantir (Principes directeurs des Nations Unies sur les entreprises et les droits de l'Homme, Déclaration universelle, lignes directrices de l'OCDE) et ses pratiques réelles. La réponse de Palantir à des questions précises reste systématiquement générique : conformité légale, processus internes, disponibilité au

dialogue. Des logs d’audit ne sont pas des garanties de droits humains, comme l’a relevé l’EFF — les régimes autoritaires tiennent eux aussi des registres méticuleux de leurs abus.

D’anciens employés de Palantir, treize d’entre eux signataires d’une lettre ouverte en 2025, ont écrit : « Les premiers Palantirians comprenaient le poids éthique de la construction de ces technologies. Ces principes ont maintenant été violés. » Quand ceux qui ont construit la machine commencent à douter de ce qu’ils ont fait, c’est un signal qu’il serait imprudent d’ignorer.

## 9 Conclusion

Palantir est une entreprise remarquable par sa cohérence. Depuis vingt ans, elle fait exactement ce qu’elle a annoncé vouloir faire : rendre visible ce qui est caché, connecter ce qui est séparé, accélérer la prise de décision. Le problème n’est pas dans la technologie en tant que telle — l’analyse de données et la visualisation de réseaux ont des applications légitimes. Le problème est dans la concentration de cette capacité dans une seule entité privée, non élue, non auditable, dont les fondateurs ont explicitement dit ne plus croire que liberté et démocratie sont compatibles, et dont les contrats les plus récents servent des politiques que plusieurs organisations internationales qualifient de violations des droits humains.

La question n’est pas de savoir si Palantir est une bonne ou une mauvaise entreprise. C’est une question mal posée. La bonne question est structurelle : peut-on déléguer l’infrastructure de la décision souveraine — qui est suspect, qui est expulsé, qui est ciblé par une frappe — à une entreprise privée dont le code est opaque, dont les contrats sont sans appel d’offres, et dont les dirigeants considèrent qu’ils défendent la civilisation ? Et si l’on accepte de le faire, quels mécanismes réels, pas seulement déclaratifs, garantissent que cette puissance ne sera pas utilisée contre ceux qu’elle prétend protéger ?

Pour l’Europe, la question se pose concrètement aujourd’hui : le NHS, la police britannique, le MoD, et demain peut-être d’autres services publics européens, sont en train d’accueillir dans leurs infrastructures une ontologie construite par une entreprise américaine dont les actionnaires, les fondateurs et les contrats les plus significatifs sont intimement liés à une administration américaine dont les priorités en matière de droits humains sont documentées. Ce n’est pas un argument pour l’isolationnisme technologique. C’est un argument pour une gouvernance sérieuse de l’infrastructure numérique souveraine — celle qui devrait être, dans une démocratie, la condition sine qua non de tout contrat de ce type.

## Références

- [1] AMERICAN IMMIGRATION COUNCIL. [ICE to Use ImmigrationOS by Palantir, a New AI System, to Track Immigrants’ Movements](#). Anglais. American Immigration Council, août 2025.
- [2] AMNESTY INTERNATIONAL. [Failing to Do Right: Palantir and ICE — Amnesty International Briefing on ImmigrationOS](#). Anglais. AMR5102112025. Amnesty International, 2025.
- [3] AMNESTY INTERNATIONAL. [USA/Global: Tech made by Palantir and Babel Street pose surveillance threats to pro-Palestine student protestors & migrants](#). Anglais. Amnesty International, août 2025.
- [4] AMNESTY INTERNATIONAL USA. [Palantir Technologies Contracts Raise Human Rights Concerns before NYSE Direct Listing](#). Anglais. Amnesty International USA, sept. 2020.
- [5] Cindy COHN et Betty GEDLU. [Palantir Has a Human Rights Policy. Its ICE Work Tells a Different Story](#). Anglais. Electronic Frontier Foundation, avr. 2026.
- [6] CYBERNEWS. [NATO bets big on AI from Trump-aligned company](#). Anglais. Cybernews, avr. 2025.
- [7] Sophie FENG et Jay STANLEY. [All the Ways Palantir is Assisting Trump’s Abusive Removal Campaign](#). Anglais. American Civil Liberties Union, mars 2026.
- [8] HARVARD CIVIL RIGHTS-CIVIL LIBERTIES LAW REVIEW. [Minority Report: Why We Should Question Predictive Policing](#). Anglais. Harvard Law School, mars 2018.
- [9] Makena KELLY. [Palantir: Peter Thiel’s Data-Mining Firm Helps DOGE Build Master Database to Surveil, Track Immigrants](#). Anglais. Democracy Now!, juin 2025.
- [10] Christopher MARQUIS. [Peter Thiel, Would-Be Philosopher King, Takes on Democracy](#). Anglais. Jacobin, oct. 2025.
- [11] NHS SUPPORT FEDERATION. [Palantir, the controversy, the contracts and the campaign against the FDP](#). Anglais. The Lowdown, avr. 2026.
- [12] Vytautas VALINSKAS. [Pentagon Adopts Palantir AI as Core Military System](#). Anglais. Technology.org, mars 2026.

- [13] Ali WINSTON. [Did Palantir Secretly Use New Orleans to Test its Predictive Policing Technology?](#) Anglais. Type Investigations, fév. 2018.