© Tribunal de Paris

OPCP

On-Prem Cloud Platform

Stabilité. Souveraineté. Performance.

Un cloud de dernière génération performant, maitrisé et industrialisé au service des missions régaliennes et de la performance des institutions.

Au cœur de l'État : les institutions portent, protègent et transforment la puissance publique.

Les services centraux des États, aussi bien les ministères, les administrations centrales ou les agences nationales, forment **le socle opérationnel de la gouvernance publique dans chaque pays d'Europe.**

Ils portent la responsabilité de concevoir, de coordonner et de mettre en œuvre les politiques publiques qui structurent le fonctionnement des sociétés et soutiennent le développement des pays.

Qu'il s'agisse de finances publiques, de santé, de justice, de sécurité, de transition écologique, d'infrastructures critiques ou encore d'innovation et de recherche, ces institutions interviennent sur des champs essentiels, souvent interdépendants, où **la fiabilité de l'action publique est déterminante.**

Leur mission s'étend de la conception stratégique jusqu'à l'exécution opérationnelle, avec un objectif commun : garantir la stabilité institutionnelle, la continuité et la performance du service public ainsi que de la protection des citoyens.

De ce fait, ces institutions gèrent quotidiennement :

- → **des processus administratifs complexes,**
- → **des volumes considérables de données,**
- → **des services essentiels qui doivent rester accessibles en permanence,**
- → **des opérations critiques où la sécurité et la fiabilité sont impératives,**
- → **une coordination multisite et multi-acteurs à l'échelle nationale et européenne.**

Au-delà de leurs missions institutionnelles, **elles soutiennent directement la performance économique.** Un État moderne, stable et numériquement avancé renforce son attractivité, facilite l'innovation, fluidifie l'activité des entreprises et consolide la confiance des acteurs économiques nationaux et étrangers.

Avoir un service public numériquement performant devient ainsi un levier essentiel à la réussite d'une politique moderne et prospère.

Les nouvelles technologies ouvrent de nouvelles capacités à l'action publique.

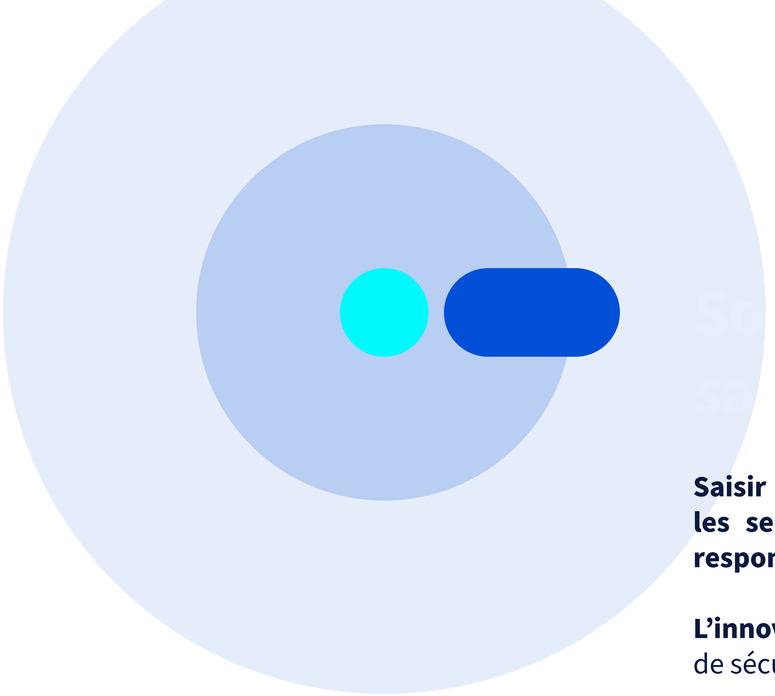
Les administrations publiques évoluent dans un environnement technologique profondément transformé. **L'émergence et la maturité de nouvelles technologies** à l'instar du cloud, de l'automatisation, de l'intelligence artificielle, du traitement massif de données et des plateformes distribuées, **ouvrent des perspectives inédites pour la conception et l'exécution de l'action publique.**

Ces technologies permettent désormais de penser **des services publics plus agiles,** capables de s'adapter rapidement aux évolutions réglementaires, aux attentes des citoyens et aux situations de crise. Elles offrent la possibilité de déployer des services à la demande, d'automatiser des processus complexes, d'exploiter la donnée à grande échelle et de renforcer la capacité de pilotage des politiques publiques.

Elles transforment également la manière dont l'État opère en rapprochant les capacités numériques des besoins opérationnels, en permettant un fonctionnement distribué entre centres nationaux et sites de terrain et en introduisant de nouveaux leviers d'efficacité, de résilience et d'anticipation.

Toutefois, tirer pleinement parti de ces avancées suppose de **disposer d'un socle technologique adapté.** Sans infrastructures capables de supporter ces nouveaux usages, le potentiel des technologies modernes reste largement inexploité, voir inaccessible.

C'est ce décalage entre les possibilités offertes par les technologies actuelles et la réalité des infrastructures publiques qui rend la modernisation numérique incontournable.



Saisir pleinement le potentiel des technologies numériques implique, pour les services étatiques, de le faire dans un cadre maîtrisé, conforme à leurs responsabilités régaliennes et à la confiance qui leur est accordée.

L'innovation technologique ne peut être dissociée des exigences de souveraineté, de sécurité et de protection des données.

Les administrations et agences publiques traitent des informations sensibles relatives aux citoyens, aux entreprises et aux intérêts stratégiques nationaux. Leur exploitation doit s'inscrire dans des environnements garantissant la maîtrise des données, la traçabilité des accès, la conformité réglementaire et la capacité de l'État à exercer un contrôle effectif sur ses infrastructures numériques.

Dans ce contexte, la souveraineté ne constitue pas un frein à l'innovation, mais une condition de sa pérennité. Elle permet aux institutions publiques d'adopter les technologies les plus avancées comme le cloud et l'IA, tout en assurant que les données restent protégées, que les dépendances technologiques soient maîtrisées et que l'évolution des systèmes demeure réversible et gouvernable.

C'est cette capacité à évoluer, innover et se transformer, tout en protégeant durablement les données des citoyens et des entreprises nationales, qui fonde une modernisation numérique responsable et soutenable de l'action publique.

La souveraineté numérique comme levier de compétitivité, de sécurité et d'influence.

Au-delà de la protection des données et du contrôle des infrastructures, la souveraineté numérique constitue aujourd'hui un facteur déterminant de compétitivité économique et de positionnement stratégique des États.

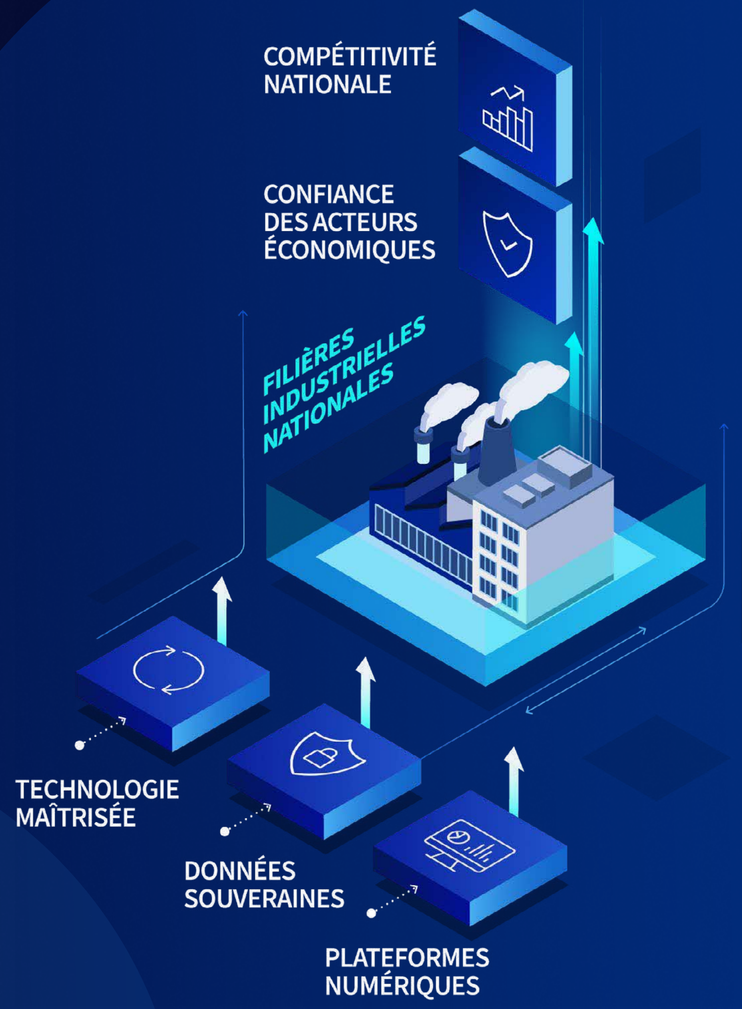
La capacité à maîtriser ses technologies, ses données et ses plateformes numériques influence directement la solidité des filières industrielles nationales et la confiance accordée par les acteurs économiques.

Un environnement numérique souverain offre aux entreprises un cadre stable, sécurisé et prévisible pour innover, investir et se développer. Il protège les savoir-faire stratégiques, limite les dépendances technologiques critiques et favorise l'émergence d'écosystèmes industriels compétitifs, capables de rivaliser à l'échelle européenne et internationale.

La souveraineté numérique renforce également la sécurité des citoyens. Elle garantit que les données personnelles, les services essentiels et les infrastructures critiques sont opérés selon des règles maîtrisées, réduisant les risques d'ingérence, de captation ou de perturbation externe.

Enfin, elle devient un levier d'influence dans les relations internationales. La capacité d'un État à définir ses propres cadres numériques, à sécuriser ses infrastructures et à maîtriser ses flux de données conditionnent sa crédibilité, sa capacité de négociation et son autonomie stratégique dans un monde interconnecté.

La souveraineté numérique ne relève plus seulement de la protection car **elle devient un pilier de la compétitivité, de la sécurité collective et de la capacité des États à peser durablement sur la scène internationale.**



Construire les fondations d’une action publique augmentée par le numérique.

Introduire durablement les technologies dans l’action publique suppose désormais d’aller au-delà des premiers chantiers numériques.

Après avoir exploité les bénéfices de la dématérialisation et de la numérisation des démarches, les États européens font face à une nouvelle étape de leur transformation. Cette phase ne consiste plus seulement à digitaliser l’existant, mais à repenser en profondeur les fondations sur lesquelles repose l’action publique.

La montée en puissance des usages numériques, l’exploitation massive de la donnée et l’intégration de technologies avancées comme l’IA, exigent une transformation plus structurelle, à la fois organisationnelle, opérationnelle et technologique.

Il s’agit de faire évoluer les modes de fonctionnement des administrations et agences pour tirer pleinement parti des capacités offertes par le numérique, tout en garantissant cohérence, maîtrise et continuité.

S’engage ainsi une nouvelle ère de transformation, caractérisée par des chantiers structurants qui redéfinissent la manière dont les administrations conçoivent, opèrent et pilotent l’action publique.

Transformer le potentiel technologique souverain en capacités opérationnelles durables.

Les nouvelles technologies offrent aux institutions publiques des perspectives inédites, mais leur adoption ne peut être envisagée comme une simple superposition d'outils. Pour produire un impact réel sur l'action publique, ces capacités doivent être intégrées dans des environnements cohérents, maîtrisés et alignés avec les exigences institutionnelles.

La transformation de l'État repose désormais sur la capacité à **traduire le potentiel technologique en capacités opérationnelles concrètes :**

- → déploiements rapides de nouveaux services,
- → automatisation et industrialisation fiable des opérations,
- → exploitation sécurisée de la donnée,
- → continuité des services même en situation de crise,
- → adaptation aux contextes opérationnels les plus variés, localement (edge) ou de manière critique (air-gap).

Cette évolution implique de rapprocher les capacités numériques des réalités de terrain, tout en conservant une vision d'ensemble à l'échelle nationale.

Or, sans un socle technologique adapté, les avancées technologiques restent difficiles à exploiter durablement. Les infrastructures doivent être en mesure de supporter ces usages dans le temps, d'évoluer sans rupture et de garantir un haut niveau de sécurité, de résilience et de gouvernance.

C'est dans cette capacité à structurer, pérenniser et gouverner les usages numériques que se joue aujourd'hui la réussite de la modernisation de l'action publique.

Des administrations centrales confrontées à des enjeux numériques et opérationnels croissants.

Dans ce contexte d'usages numériques en forte expansion et de missions publiques toujours plus exigeantes, les services centraux et agences nationales font face à une complexité croissante de leurs systèmes d'information.

Ils doivent à la fois soutenir des opérations critiques, gérer des volumes massifs de données sensibles et accompagner la transformation de l'action publique, tout en garantissant performance, continuité et souveraineté numérique.

Des systèmes d'information sous forte contrainte.

Les ministères, directions générales, agences et opérateurs publics s'appuient encore largement sur des systèmes anciens, hétérogènes et fortement interdépendants. Cette fragmentation rend les évolutions complexes, alourdit l'exploitation quotidienne et accroît les risques sur des applications souvent critiques pour les missions publiques.

La gouvernance distribuée entre entités crée par ailleurs des doublons, des écarts de maturité numérique et des charges opérationnelles importantes pour les DSI, dans un contexte où chaque réforme, évolution réglementaire ou situation de crise impose de faire mieux, plus vite et sans interruption du service public.

Une intensification des usages et des dépendances numériques.

Parallèlement, **l'État, ses services et ses agences forment organisation de plus en plus data-driven.** L'explosion des données publiques (sociales, fiscales, environnementales, sanitaires ou de mobilité), la généralisation des téléservices et démarches en ligne, ainsi que la montée en puissance de l'IA , des traitements analytiques et des besoins de prédiction, augmentent fortement les charges et les exigences portées sur les infrastructures.

Cette dynamique renforce **la nécessité d'une interopérabilité réelle entre administrations et opérateurs publics,** tout en mettant sous tension des infrastructures et des organisations qui peinent à absorber durablement ces nouveaux usages.

Des enjeux structurants pour la modernisation de l'État.

Face à cette complexité croissante, plusieurs enjeux majeurs structurent désormais la transformation numérique des services centraux et agences :

- **Souveraineté et confiance,** par la maîtrise totale des données, des flux et des politiques d'accès,
- **Sécurité et résilience,** pour garantir la continuité des fonctions essentielles qui ne peuvent jamais s'interrompre,
- **Modernisation progressive,** afin de faire évoluer les systèmes critiques sans rupture,
- **Rationalisation et maîtrise des coûts,** dans un contexte de ressources contraintes et de pilotage budgétaire renforcé,
- **Interopérabilité et innovation,** pour permettre le développement de services transverses, l'exploitation avancée de la donnée, l'automatisation et l'usage maîtrisé de l'IA.

Ces enjeux définissent le cadre dans lequel les administrations centrales doivent repenser leurs infrastructures numériques, afin de soutenir durablement la performance publique et la souveraineté de l'État.

Le socle de l'action publique repose sur des infrastructures cloud de nouvelle génération.

La modernisation des services publics via l'utilisation des nouvelles technologies ne peut reposer ni exclusivement sur le cloud public ni sur des infrastructures historiques.

Pour répondre aux besoins réels des administrations présents et futurs, l'État doit s'appuyer sur **des infrastructures de pointe,** capables de fonctionner :

- → **au centre** (SI ministériels et plateformes nationales),
- → **à la périphérie** (sites distants, préfectures, laboratoires, centres opérationnels),
- → **en environnement sensible** (zones à accès restreint, réseaux spécialisés, espaces classifiés),
- → **en mode déconnecté** (crise, coupure réseau, opérations terrain).

Ces nouveaux besoins imposent une infrastructure capable de :

- → **déployer en quelques minutes** des applications, environnements ou services,
- → **fonctionner en local** lorsque le réseau n'est pas garanti,
- → **s'automatiser intégralement,**
- → **s'adapter à des charges de travail hétérogènes,**
- → **protéger les données les plus sensibles,**
- → **assurer de très faibles latences pour les usages Edge,**
- → **isoler totalement certains traitements (air-gap),**
- → **coopérer avec le cloud public lorsque c'est pertinent,** sans dépendance.

En résumé, le numérique de l'État doit désormais couvrir trois réalités complémentaires :

- → **Le cloud :** élasticité et scalabilité.
- → **L'on-prem modernisé :** maîtrise, souveraineté, continuité.
- → **L'Edge et l'Airgap :** proximité opérationnelle, sécurité et autonomie.

OPCP : une plateforme on-prem de dernière génération qui couvre l'ensemble des besoins.

OPCP n'est pas un simple cloud local : c'est **une plateforme cloud-native installée au sein des infrastructures de l'État**, conçue pour fonctionner :

- → **dans un datacenter ministériel**
- → **sur un site critique**
- → **en préfecture ou en agence opérationnelle**
- → **dans un environnement isolé**
- → **en mode déconnecté**
- → **ou en complément d'un cloud public**

OPCP apporte à l'État une infrastructure locale aussi moderne que le cloud :

- → **déploiement automatisé à la demande**
- → **catalogue de services prêt à l'emploi**
- → **provisionnement instantané**
- → **standardisation entre entités**
- → **sécurité durcie**
- → **gouvernance centralisée, segmentation fine,**
- → **opérations simplifiées**
- → **fonctionnement autonome dans toutes les configurations (Edge, Airgap, remote, crise)**

Une réponse unifiée aux besoins variés de l'État :

- → Pour un ministère : **moderniser le SI sans rupture**, soutenir les charges critiques.
- → Pour une agence : **héberger des données sensibles,** avec souveraineté totale.
- → Pour un service opérationnel : avoir **de la puissance locale,** même sans réseau.
- → Pour une autorité indépendante : **isoler complètement certains traitements.**
- → Pour une mission régalienne : garantir **résilience et disponibilité totale.**

OPCP permet à l'État de disposer d'une infrastructure cloud qui n'est plus un héritage, mais un accélérateur.

Une architecture unifiée pour tous les usages : du datacenter national à l'Air Gap opérationnel.

Les services de l'Etat ne peuvent pas se contenter d'une seule infrastructure : ses missions exigent **une architecture capable d'opérer partout,** dans toutes les configurations, avec un niveau d'automatisation maximal.

OPCP CORE

La fondation automatisée et résiliente.

- → Orchestration complète (compute, réseau, sécurité)
- → Observabilité avancée
- → Mise à jour automatisée
- → Autonomie en site déconnecté
- → Résilience multi-niveaux
- → Durcissement sécurité intégré

OPCP Core permet de déployer une plateforme moderne **dans un ministère comme dans un sous-sol classifié.**

LANDING ZONE MANAGER

Gouvernance fine pour un État multisites et multi-entités.

- → Isolation par ministère, direction, agence, opérateur
- → Politiques de conformité personnalisées
- → Gestion avancée des rôles, quotas, accès
- → Adapté aux environnements sensibles ou restreints
- → Supervisable au niveau national ou local

Il garantit **une gouvernance uniforme**, tout en respectant les périmètres fonctionnels de chaque entité publique.

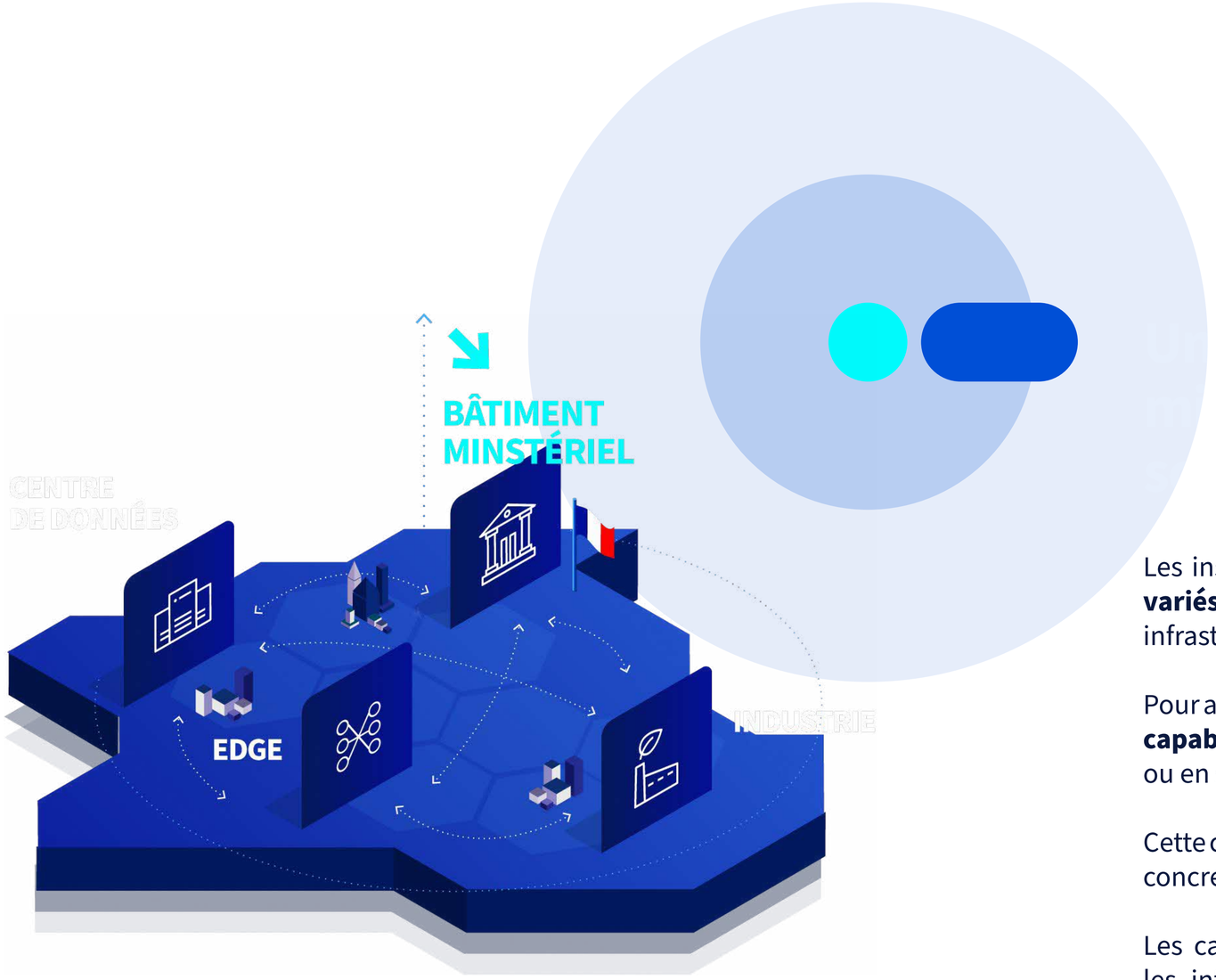
CLOUD STORE

Déploiement instantané de services, y compris en local isolé.

- → Catalogue d'applications et de services standardisés
- → VM, bases de données, stacks IA, services analytiques, microservices
- → Déploiement possible **en Edge ou en Airgap**
- → Standardisation entre centres et sites distants

Le Cloud Store permet à un service public de déployer **sur site,** en quelques minutes :

- → un environnement d'analyse
- → un outil métier
- → une base de données
- → un moteur IA
- → un service critique local

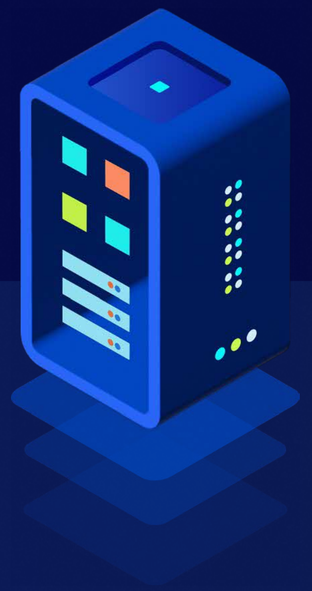


Les institutions publiques **évoluent dans des environnements extrêmement variés :** centres ministériels, sites distants, laboratoires, centres de crise, infrastructures critiques ou encore zones nécessitant un fonctionnement isolé.

Pour accompagner cette diversité opérationnelle, **OPCP fournit une architecture capable d'opérer partout,** en toutes circonstances, y compris en mode air-gap ou en situation de connectivité fluctuante.

Cette capacité d'adaptation ne relève pas du concept : elle se traduit par des usages concrets, au plus près des besoins des ministères, agences et opérateurs de l'État.

Les cas d'usage qui suivent illustrent comment OPCP permet de moderniser les infrastructures, renforcer la souveraineté, accélérer les déploiements et sécuriser les missions essentielles, quels que soient les terrains d'opération ou les contraintes rencontrées.



OPCP

USE CASE | **01**

Modernisation progressive et sécurisée des systèmes critiques de l'État.

Moderniser sans interrompre les missions régaliennes.

Les États dépendent d'applications historiques essentielles,systèmesfiscaux,registresnationaux, justice numérique, sécurité intérieure, dossiers sociaux, régulation des marchés. Ces systèmes, conçus parfois il y a plusieurs décennies, sont difficiles à migrer, fortement interconnectés, et doivent fonctionner sans interruption. Toute évolution technique doit donc être maîtrisée, progressive et totalement sécurisée.

OPCP permet :

- → d'**intégrer progressivement** des services modernes sans déstabiliser les applications existantes,
- → d'**automatiser les opérations** répétitives (patching, sécurité, mises à jour),
- → d'**unifier l'environnement technique** pour réduire les écarts entre entités,
- → de **sécuriser l'exécution des workloads** critiques tout en préparant leur modernisation,
- → de **garantir une continuité** parfaite lors des transitions de versions, migrations ou refontes.

OPCP transforme la modernisation des systèmes régalien en un processus continu, maîtrisé et sans interruption, un prérequis vital pour la stabilité institutionnelle.

OPCP

USE CASE | **02**

Environnement souverain pour les données sensibles de l'État.

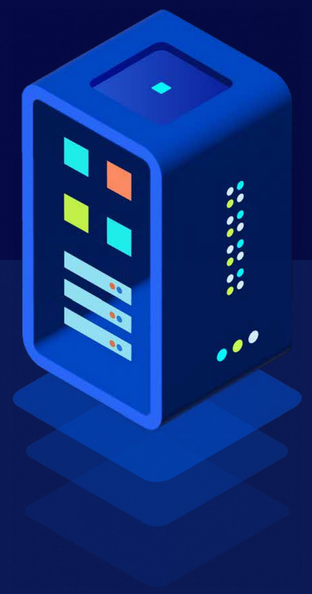
Créer un Data Hub national sécurisé et maîtrisé.

La donnée publique est devenue un actif stratégique : elle alimente les politiques sociales, environnementales, économiques et sanitaires. Or, ces données sont souvent dispersées dans des systèmes hétérogènes, parfois hébergés chez des tiers, compliquant leur gouvernance, leur analyse et leur sécurisation.

OPCP permet :

- la **centralisation de données sensibles** dans un environnement souverain contrôlé par l'État,
- la **gestion fine des accès** selon le niveau de sensibilité ou de classification,
- l'**exécution sécurisée** de traitements analytiques ou IA sur site, sans exposition externe,
- la **standardisation des formats et des flux** pour faciliter le partage inter-agences,
- l'**isolement complet** des traitements critiques (zones restreintes, air-gap, classification).

OPCP offre aux États un socle souverain pour exploiter pleinement leurs données, tout en garantissant un contrôle total de leur circulation, de leur sécurité et de leur intégrité.



OPCP

USE CASE | **03**

Continuité d'activité nationale : crises, cybersécurité et opérations sensibles.

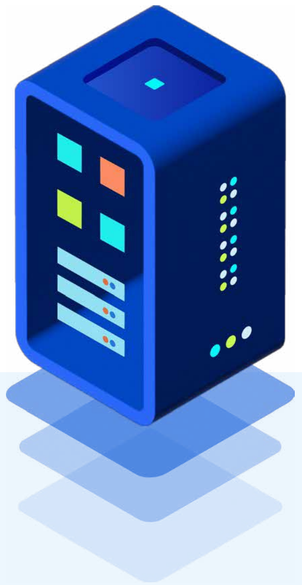
Assurer un fonctionnement de l'État en toutes circonstances.

Les gouvernements doivent garantir la disponibilité permanente de leurs systèmes : sécurité civile, chaînes de paiement, fiscalité, gestion des crises, coordination interministérielle. Or, les crises récentes (cyberattaques, catastrophes naturelles, tensions géopolitiques) ont révélé la nécessité d'une résilience accrue, capable de supporter un fonctionnement même en conditions dégradées.

OPCP permet :

- → d'**opérer localement**, y compris en cas de rupture réseau ou d'isolement total,
- → de **déployer en urgence** des plateformes de gestion de crise pour coordonner les services de l'État,
- → de **soutenir des environnements tactiques ou sensibles** avec des nœuds Edge sécurisés,
- → de **garantir la continuité** des fonctions vitales (paiement, santé, sécurité) même sous pression,
- → de **renforcer les capacités de cyberdéfense** grâce à une infrastructure sécurisée et indépendante.

OPCP assure à l'État une continuité opérationnelle robuste, indispensable dans un monde où les crises peuvent survenir à tout moment.



OPCP

USE CASE | **04**

Plateforme nationale d'IA souveraine pour l'État.

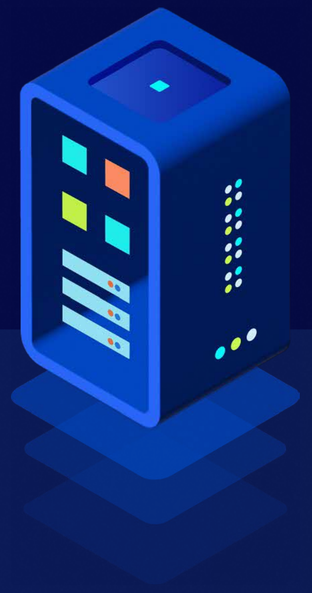
Exploiter l'IA sans exposer les données sensibles.

Les administrations publiques cherchent à utiliser l'IA pour optimiser les politiques publiques, détecter les anomalies, analyser les masses de données réglementaires, accélérer les inspections, améliorer les services aux citoyens ou prévoir des crises.Mais les modèles d'IA nécessitent des données sensibles, souvent classifiées, qu'il est impossible d'envoyer hors du périmètre étatique.

OPCP permet :

- → d'**héberger des modèles IA** dans une infrastructure souveraine et sécurisée,
- → d'**entraîner des modèles** sur des données sensibles sans jamais quitter le périmètre public,
- → d'**offrir un environnement air-gap** lorsque l'isolement maximal est requis,
- → de **mutualiser des capacités GPU** ou compute avancées entre ministères,
- → de **faciliter le développement d'IA spécialisées** par mission : sécurité, fiscalité, justice, climat, santé publique.

OPCP donne à l'État les moyens de déployer une IA souveraine, maîtrisée, et alignée avec la protection des données les plus sensibles.



OPCP

USE CASE | **05**

Un socle unifié pour mutualiser les infrastructures entre ministères et agences.

Mutualiser pour harmoniser, réduire les coûts et renforcer la cohérence publique.

La fragmentation des infrastructures entre ministères, agences et opérateurs entraîne des duplications coûteuses, des systèmes parallèles difficiles à maintenir, une hétérogénéité des pratiques et une surcharge opérationnelle. La mutualisation devient essentielle pour améliorer l'efficacité et optimiser l'usage des fonds publics.

OPCP permet :

- → de **regrouper plusieurs entités sur un socle commun** tout en préservant l'isolement organisationnel,
- → de **mettre en place des politiques unifiées** de sécurité, conformité et gouvernance,
- → d'**optimiser les ressources matérielles et logicielles** grâce à la standardisation,
- → de **réduire la dépendance** aux prestataires multiples et hétérogènes,
- → de **faciliter les projets transverses** et la coopération interministérielle.

OPCP constitue la base d'une mutualisation nationale moderne, permettant aux États de gagner en efficacité, en cohérence et en capacité d'action.

OPCP

Une complémentarité qui a du sens

D'un côté, une solution technique éprouvée.
De l'autre, une connaissance fine du terrain.
Il est clair qu'il y a des choses à faire ensemble.

Des cas à inventer, adapter, tester

Les cas d'usage ne manquent pas : edge, usines, sites critiques, infrastructures déconnectées…
Et si on en identifiait un ou deux pour avancer concrètement ?

Un atelier, un échange, un POC ?

Pas besoin de tout figer d'emblée.
Juste un moment pour creuser ensemble, voir ce qui a du sens, et construire, pas à pas.

ovhcloud.com
opcp@ovhcloud.com