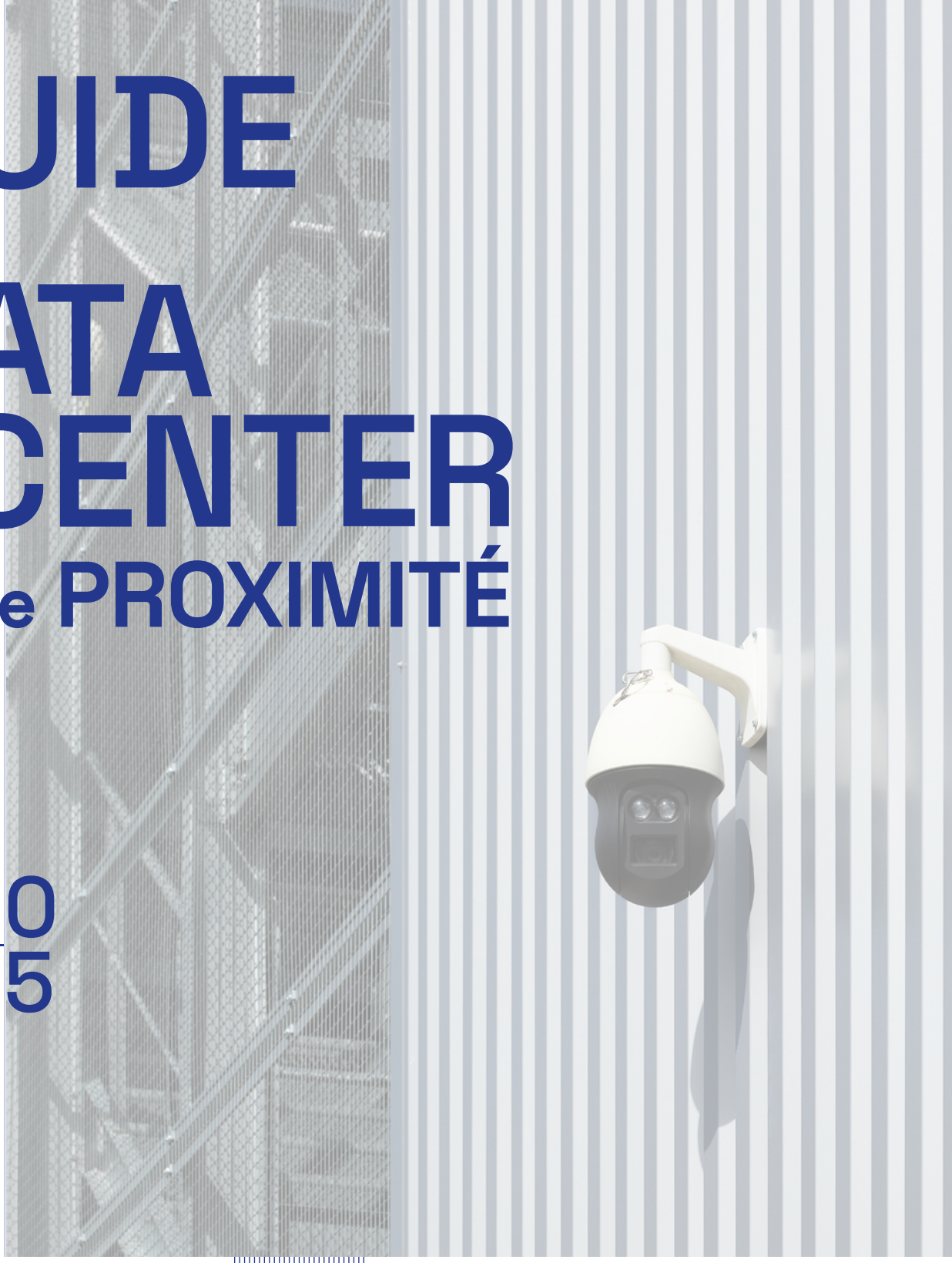
le GUIDE du DATA CENTER de PROXIMITÉ

2025



InfraNum

DC MAG

BANQUE des TERRITOIRES

SOMMAIRE


11
12

EDITO

Les datacenters de proximité façonnent la souveraineté numérique des territoires

La transformation numérique n'est plus une perspective, elle est notre présent. Et ce présent s'écrit avant tout dans les territoires. La fermeture du réseau cuivre, qui accélère la généralisation de la fibre, marque une nouvelle étape : celle d'une **numérisation totale de notre économie**, entraînant dans son sillage tous les Français, quel que soit leur mode de vie.

Avec cette accélération, les organisations produisent, traitent et exploitent une **quantité de données sans précédent**. L'enjeu n'est plus seulement technologique, il devient **économique, écologique et souverain**. Car derrière chaque service numérique, chaque usage, chaque décision, se pose désormais la question de **l'hébergement et de la maîtrise des données**.

Au cœur de cette économie de la donnée se trouvent les datacenters, infrastructures essentielles et pourtant souvent méconnues. Cette catégorie recouvre une pluralité d'acteurs et de modèles, du méga-datacenter international aux structures plus locales, plus agiles : **les datacenters de proximité**.

Depuis mon élection à la présidence d'**InfraNum**, fédération qui réunit l'ensemble des acteurs des infrastructures numériques, ceux qui collectent, transportent, stockent et traitent la donnée, je fais un constat simple : **on ne parle pas assez des datacenters dans et pour les territoires**. C'est pourtant là que se joue une part essentielle de notre **souveraineté numérique** et de notre **résilience collective**.

Ce nouveau guide, revisité et enrichi depuis sa première édition en 2021, vient répondre à ce manque. Il apporte un éclairage concret et stratégique sur cette typologie d'infrastructures encore méconnue, implantée au plus près des villes moyennes et des zones rurales, au plus proche des usagers.

Ce document montre que ces datacenters de taille intermédiaire ne sont pas une version réduite des grands centres, mais bien **une réponse adaptée à des besoins spécifiques**. Ils répondent à des enjeux de souveraineté et de maîtrise locale des données, s'inscrivent dans **des démarches RSE exigeantes**, favorisent **la valorisation énergétique** et **la mutualisation des ressources**, et redonnent confiance aux acteurs publics comme privés dans leur indépendance numérique.

Mais au-delà du diagnostic, ce guide est un outil d'action. Il s'adresse à celles et ceux - élus, dirigeants, techniciens - qui souhaitent comprendre, anticiper et décider. Il clarifie ce qu'est réellement un datacenter de proximité, ses promesses comme ses limites, et propose **des bonnes pratiques** et **des repères essentiels** pour aborder ces sujets complexes avec lucidité.

Car le numérique reste souvent perçu comme une abstraction, une source d'inquiétude autant qu'un levier indispensable. En redonnant de la clarté et de la proximité, les datacenters territoriaux deviennent **un maillon de confiance** : ils incarnent un numérique plus **ancré**, plus **sobre**, plus **maîtrisé**.

Chez InfraNum, nous en sommes convaincus : ces infrastructures locales ont une carte décisive à jouer. Elles ne remplaceront pas les méga-datacenters, mais elles en sont **le complément intelligent et stratégique**. Elles permettent **d'ancrer la donnée au cœur des territoires**, de favoriser **les synergies locales**, et d'offrir aux collectivités la possibilité de bâtir **des projets de mutualisation vertueux**.

ILHAM DJEHAICH,
PRÉSIDENTE D'INFRANUM

Ce guide des datacenters de proximité est à destination des **collectivités et des entreprises locales,** afin de les **accompagner dans leur stratégie d'hébergement numérique** sur leur territoire et avec des partenaires locaux.

En effet, une organisation utilise et utilisera une diversité de solutions d'hébergement en fonction de ses besoins. **Les datacenters de proximité ont leur place dans l'écosystème des solutions d'hébergement**, ils adressent des besoins précis, souverains et intéressent aujourd'hui toute taille d'organisation.

À travers une approche pragmatique et documentée, sur la base de retours d'experts et d'une vingtaine d'entretiens auprès d'entreprises et de collectivités, ce guide montre que **les datacenters de proximité sont une opportunité** pour les territoires :

- **Ils s'adressent à toute taille d'organisation**, pour des raisons bien spécifiques à leur modèle économique et politique ;
- **Ils assurent une parfaite garantie de la localisation des données, le respect des normes et réglementations**, ils favorisent une relation de confiance ;
- **Ils s'intègrent plus facilement dans l'environnement**, ils donnent plus de latitude à des projets de récupération de chaleur ;
- **Enfin ils sont une opportunité pour les collectivités de créer des offres d'hébergement mutualisées** à destination des plus petits acteurs du territoire.

le GUIDE du DATA CENTER de PROXIMITÉ

LES DATACENTERS DE PROXIMITÉ

les DATACENTERS de PROXIMITÉ

“Il en va des datacenters comme du cloud, il y a une autre réalité, géographique, économique et politique que celle les géants qui font l’actualité, c’est la force de la proximité. Car si je suis une entreprise ou une collectivité, pourquoi irai-je chercher un partenaire qui n’est pas proche de moi, que ce soit par sa localisation, par sa taille ou par ses choix de vie ? Ainsi en est-il du datacenter de proximité, partenaire local de l’économie et du numérique, physiquement proche de ses clients, engagé dans la sécurité et la souveraineté de leurs données, et qui pour eux maîtrise la technologie.

Le datacenter de proximité est une réponse aux attentes et aux projets des territoires. Il sait accueillir ses voisins, héberger leurs infrastructures, offrir des services, se montrer efficient, élever la sécurité des données, s’ouvrir au monde, à l’hybridation et à la clusterisation, et même servir de relais aux projets d’IA (Intelligence Artificielle). Et à des coûts maîtrisés. Le datacenter de proximité est l’avenir d’une informatique et d’un numérique engagés, partenaire de millions d’entreprises, d’acteurs publics, et de citoyens.”

YVES GRANDMONTAGNE,
RÉDACTEUR EN CHEF DE DCMAG

Ce chapitre présente les particularités des datacenters de proximité et recense les motivations qui amènent des organisations, entreprises et collectivités, à sélectionner ce type d’infrastructure.

De manière général, ce guide part du postulat qu’une organisation utilise et utilisera une diversité de solutions d’hébergement en fonction de la nature de ses données, de ses services.
En revanche **le contexte est favorable pour que les organisations repensent leur stratégie d’hébergement**. En effet, avec la transformation numérique, la multiplication des services en ligne, les organisations font face à une croissance significative de leur stockage de données ce qui peut questionner leur modèle économique initial. En parallèle, la résilience devient un sujet de plus en plus d’actualité, que ce soit pour répondre aux cyberattaques ou pour faire face à l’augmentation des températures. Les organisations n’ont plus nécessairement les infrastructures suffisantes pour répondre à ces nouveaux critères de plus en plus exigeants.

Plusieurs enseignements clés :

Les datacenters de proximité répondent à des besoins spécifiques que n’adressent pas les offres cloud en général, à travers l’hébergement sec en particulier, par exemple pour bénéficier d’une solution de redondance pour les données les plus critiques...

Ils s’adressent à toutes tailles d’organisations, les besoins peuvent varier mais tous peuvent y trouver un intérêt ;

Ils s’inscrivent dans une palette de solutions. Ils sont une vraie alternative aux offres cloud classiques et permettent de penser **des stratégies d’hybridation** ;

De manière générale, la notion de proximité est un réel critère de sélection car cela permet une relation de confiance avec des interlocuteurs repérés, une plus grande latitude à personnaliser l’offre « *on sait les joindre* » ;

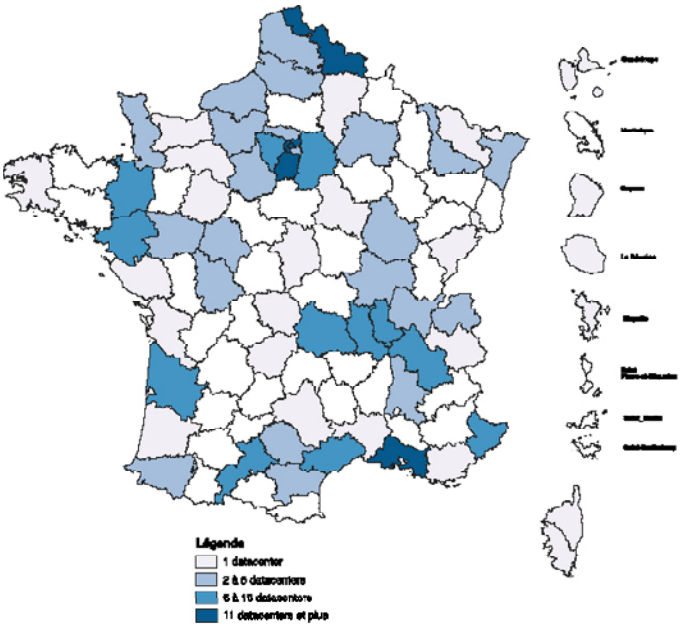
Plus spécifiquement, ils donnent la possibilité aux collectivités de créer des offres mutualisées sur le territoire, de manière à rendre plus accessibles les offres cloud pour les plus petits acteurs.

Si tout le monde a une idée de ce qu'est un datacenter, notamment un hyperscale, les datacenters de proximité passent souvent plus inaperçus bien que leur nombre s'accroît d'année en année.

Les datacenters de proximité sont des datacenters de plus petite taille qui s'implantent sur les territoires au plus **proche des utilisateurs finaux, y compris sur des territoires ruraux**. Réduire leur taille les rend accessibles et donne la possibilité à certains clients finaux d'envisager de **construire leur propre datacenter**, y compris en envisageant divers montages partenariaux.

S'il est vrai qu'il est possible de trouver de nombreuses manières d'héberger un service donné et que la plupart des organisations utilisent le cloud sans toujours être en mesure de connaitre la localisation de leurs serveurs, la notion de proximité répond des besoins, et parfois à de nouveaux besoins. Ce type d'infrastructure amène à réinterroger les organisations sur leur stratégie d'hébergement.

env. **300** DATACENTERS EN FRANCE



LES DATACENTERS DE PROXIMITÉ

Les datacenters au service des entreprises et des collectivités du territoire

Lesquelles souhaitent :

Garder **la maîtrise de leur SI** (internalisation)

Héberger **leur service numériques à proximité**

Assurer **la souveraineté** de leurs données (localisation des données)

La proximité devient alors un critère de choix, notamment pour développer **un écosystème local** de services numériques.

Cartographie DCmag & InfraNum, en partenariat avec Tactis
Périmètre : liste des datacenters ouverts à des tiers (datacenters privés non inclus)

Carte des datacenters neutres, ouverts à l'hébergement et la colocation. La carte ne prend pas en compte les datacenters et salles informatiques privés. On compte environ 5000 datacenters privés en France.
Cartographie en ligne : https://carte.dcmag.fr/

Les datacenters de proximité sont au coeur d'un écosystème large et mondial de datacenters :
- Situés : in-situ, à l'échelle locale, nationale, européenne, mondiale ;
- De tailles variées : micro-datacenter, petits et moyens datacenters, hyperscales, méga datacenters.

L'ensemble de nos données et services transitent à travers ces pluralités de datacenters, de manière plus ou moins consciente pour les utilisateurs finaux. Ci-dessous quelques définitions pour rentrer dans l'univers des datacenters.

QUELQUES DÉFINITIONS

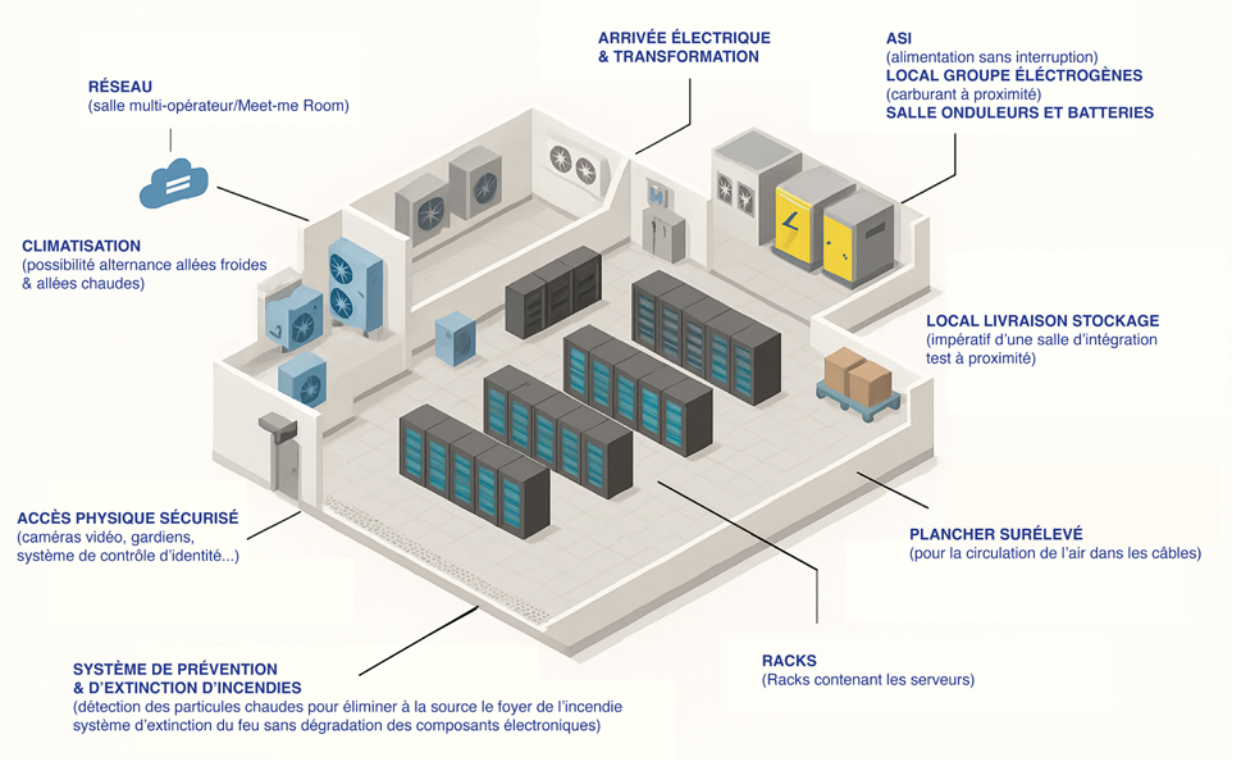
DATACENTER - Un datacenter est une infrastructure immobilière et technique qui héberge des ressources informatiques (baies, serveurs, stockage, réseaux …) avec tous les équipements nécessaires (électricité, refroidissement, connectivité, sécurité, accès…). Cet environnement est utilisé par des entreprises / collectivités /administrations pour stocker des données, utiliser des applications, et par des fournisseurs de services Cloud.

DATACENTER DE PROXIMITÉ - C'est un datacenter présent localement pour accueillir les systèmes d'informations d'une entreprise ou d'une collectivité. Il peut également héberger des services de fournisseurs et éditeurs extérieurs (hébergement, cloud privé, applications en mode SaaS, télécoms, IA...).

DATACENTER PRIVÉ - C'est un datacenter entièrement dédié aux besoins d'une organisation, qui concerne plus particulièrement les grandes organisations. La notion de proximité est à nouveau fondamentale.

HYPERSCALER - C'est un fournisseur de Services Cloud public à très grande échelle, qui dispose de très importants moyens d'infrastructures et de services, généralement hébergés dans ses propres Méga Datacenter , ou Hyperscale, à l'échelle mondiale. Exemples : Amazon Web Services, Microsoft Azure, Google Cloud.

SALLE SERVEUR ou SALLE INFORMATIQUE : C'est une salle abritant des équipements informatiques qui peut exister en interne d'une organisation, utilisée pour les besoins propres de cette organisation. Une salle serveur est parfois considérée comme un mini datacenter



Les analyses présentées ci-dessous sont issues d'une enquête qualitative menée auprès d'une dizaine de collectivités de tailles variées (communes, métropoles, syndicats, département) et d'une dizaine d'entreprises (TPE, PME, acteurs des datacenters).

UNE DIVERSITÉ DE SOLUTIONS D'HÉBERGEMENT EN FONCTION DES BESOINS

Une organisation, quelle que soit sa taille, que ce soit une collectivité ou une entreprise, utilise et utilisera une diversité de solutions d'hébergement en fonction de la nature de ses données et ses services.

LES CHOIX QUI SE PRÉSENTENT :

	Je garde mon informatique chez moi	Je garde mon hébergement et je la place dans un datacenter externe	J'installe mes applications et mes données chez un hébergeur	Je consomme des services dans le cloud
Déclinaison technique	**ON-PREMISE**	**HÉBERGEMENT SEC**	**CLOUD PUBLIC, PRIVÉ / PaaS, IaaS**	**SAAS**
Infrastruture concernée	Salles serveurs le plus couramment DC privé pour une grande entreprise	**Datacenter de proximité**	**Datacenter de proximité**, datacenter national, européen, à l'échelle mondiale, localisation plus ou moins comuniquée	Datacenter dont la localisation est plus ou moins communiquée
Qui les utilise	Toute taille d'organisation, publique ou privée	Organisations : ° avec du patrimoine informatique et qui souhaite le conserver, garder la maîtrise ° sans alternative jugée suffisamment souveraine et qui veut garder la maîtrise, y compris en anticipant une migration « *C'est notre matériel et demain on peut le prendre comme on veut.*" ° qui souhaitent mettre à disposition une infrastructure pour d'autres organisations (DC de proximité mutualisé) ° avec des besoins / serveurs spécifiques (ex : multimédia)	Organisations : ° sans patrimoine informatique ° avec du patrimoine mais qui diversifie ses solutions d'hébergement pour maîtriser sa charge de travail ou limiter sa capacité informatique. « *on a une petite tendance quand on a le choix et la possibilité d'aller plutôt vers des solutions hébergées* » La notion de **proximité** reste privilégiée, sous réserve que cela existe et des tarifs associés.	Toute organisation qui souhaite utiliser un logiciel spécifique : ° qui n'est pas téléchargeable ° ou que l'organisation ne souhaite pas télécharger Pour les organisations qui ont du patrimoine, à nouveau le sujet de la diversification, sous réserve des tarifs associés.

Ce guide va plus particulièrement détailler les solutions proposées par les datacenter de proximité. Pour autant, pour comprendre les motivations d'adoption, il est nécessaire d'aborder les autres solutions d'hébergement, le sujet est global.

FOCUS COLLECTIVITÉS

LE CONTEXTE ACTUEL EST MARQUÉ PAR TROIS PHÉNOMÈNES

1. **Une numérisation grandissante des services qui entraîne une augmentation des besoins et des coûts SI**, quelle que soit la taille de la collectivité, et ceci dans un contexte où il n'est pas nécessairement prévu une augmentation du personnel ;

2. **Des éditeurs de logiciels qui tendent à basculer leurs outils en mode SaaS** de manière à s'affranchir de l'acquisition d'équipements informatiques et de ressources dédiées à la maintenance sur site, pour simplifier également l'exercice des mises à jour ;

3. **Une bascule progressive des coûts d'investissements (Capex) en frais de fonctionnement (Opex)**, notamment le coût des licences qui étaient préalablement comptabilisées en coûts d'investissement. C'est un changement de fonctionnement majeur de l'achat à la location qui peut freiner les prises de décision.

LES PRINCIPAUX CRITÈRES DE SÉLECTION D'UNE SOLUTION D'HÉBERGEMENT

Patrimoine informatique / Tarification / Continuité de service / Criticité des données / Acteur de confiance

QUELQUES MESSAGES CLÉS

Les retours d'expérience montrent que **les choix sont pragmatiques**, que la notion de souveraineté n'est pas nécessairement adossée au fait que le datacenter soit entièrement gérée par une collectivité. **Un datacenter de proximité privé peut tout à fait convaincre** pour peu qu'il ait les garanties de souveraineté suffisantes et une tarification jugée convaincante.

Pour les collectivités qui ont les compétences, les stratégies sont hybrides : on-premise et cloud sont utilisés de manière alternative via différents critères de sélection et rien n'est définitif. Un service sur le cloud pourra à terme revenir en interne une fois que son fonctionnement sera connu et vice-versa. Le sujet de la sauvegarde donne également lieu à des stratégies très spécifiques, souvent hybrides.

Les datacenters de proximité sont des choix privilégiés dans la mesure où ils répondent à un souhait politique de conserver les données sur le territoire, parce que c'est concret "*c'est là, ça me rassure*". En revanche, la tarification reste un critère prioritaire et peut freiner l'adoption.

La mise à disposition d'infrastructures mutualisées par une collectivité est une option qui semble très convaincante pour l'ensemble des communes et entreprises d'un territoire sous réserve de trouver une structure qui porte le projet. Cette solution permet de **garantir une maîtrise des données**, en s'affranchissant de tout risque d'application de loi extraterritoriale, **tout en optimisant les coûts**.

À noter que **les modalités de mise en œuvre d'infrastructures mutualisées peuvent être extrêmement variées**, de l'hébergement sec à la construction complète d'un datacenter, et ne veut pas dire que c'est entièrement géré par la collectivité.

RECENSEMENT DES MOTIVATIONS PAR SOLUTION D'HÉBERGEMENT

	Je garde mon informatique chez moi	Je garde mon hébergement et je la place dans un datacenter externe	J'installe mes applications et mes données chez un hébergeur	Je consomme des services dans le cloud
Déclinaison technique	**ON-PREMISE**	**HÉBERGEMENT SEC**	**CLOUD PUBLIC, PRIVÉ / PaaS, IaaS**	**SAAS**
Collectivité AVEC du patrimoine informatique	Les collectivités qui ont du patrimoine ont l'avantage de pouvoir **comparer** par rapport à leur existant. Aujourd'hui les DSI font face au dilemme **de conserver les services sur site ou de les déplacer sur le cloud**. Les deux solutions ont des avantages et le choix se fait **au cas par cas** : • **Le cloud permet** de décharger l'infrastructure existante, de s'affranchir de service dont la capacité est difficile à dimensionner, de réduire la charge de travail, de garantir la continuité de service. En revanche, il faut que la collectivité ait confiance en l'éditeur. • **Le On-Premise garantit** une maîtrise totale des données, de la configuration du service, de la tarification. Conserver un minimum de services on-premise permet également de conserver des compétences, de challenger les offres en ligne, d'avoir une solution de repli. Une alternative perçue comme convaincante est **le datacenter mutualisé** qui permet de garantir un niveau de résilience et de sécurité, de garantir la continuité de service, tout en maîtrisant les tarifs.			
	Cette option est conservée dans la majorité des cas si : ° les locaux répondent aux exigences de sécurité et de résilience, redondance *« je vais pouvoir avoir ma propre politique de sauvegarde et ne pas dépendre de la p olitique des autres »* ° ils n'y répondent pas mais il n'existe pas d'alternative convaincante	La solution est étudiée lorsque les salles serveurs ne répondent plus à toutes les exigences, de sécurité, de redondance, d'isolation... Ce choix est observé également lorsque de grandes collectivités mettent en place un nouveau service qui génèrent beaucoup de données sensibles (Wifi, IoT…) En revanche, il faut une équation économique favorable.	Cette option peut être étudiée notamment au moment du renouvellement du matériel informatique (tous les 5-7 ans) À noter que la tarification peut être jugée complexe, avec des coûts supplémentaires pas toujours prévisibles. Certaines collectivités au contraire privilégient cette solution, en fonction de la criticité des données, en comparant les coûts on-premise et cloud. Elles ont les compétences, de l'expérience et une capacité de négociation. A noter, une métropole qui fournit la connectivité à un datacenter local (RIP), ce qui lui permet d'être à la fois fournisseur et client. Deux avantages : force de négociation et suppression des coûts d'accès très haut débit.	Cette option peut être subie ou choisie. Dans le cas où elle est choisie, les motivations sont proches de celles en PaaS et IaaS : - réduire la charge de travail ou la capacité informatique on-premise, - notamment pour les services qui demandent beaucoup de configurations ou sont de forte capacité ; - Spécifique au SaaS : la continuité de service, le weekend notamment. Quelle que soit la motivation, elle s'accompagne d'une série de vérifications : localisation des données, sécurité… avec la possibilite d'associer ses propres outils de sécurité (ex : WAF) En revanche : *"sur certaines données on est plutôt frileux")*

	Je garde mon informatique chez moi	Je garde mon hébergement et je la place dans un datacenter externe	J'installe mes applications et mes données chez un hébergeur	Je consomme des services dans le cloud
Déclinaison technique	**ON-PREMISE**	**HÉBERGEMENT SEC**	**CLOUD PUBLIC, PRIVÉ / PaaS, IaaS**	**SAAS**
Collectivité SANS patrimoine informatique	Si les collectivités sont de petites tailles, les choix sont limités, sauf si d'autres collectivités mettent à disposition leurs propres solutions (salles serveurs ou datacenter mutualisé).			
	NA	Cas observés : ° Une grande collectivité a besoin d'héberger un nouveau service dont elle veut particulièrement protéger les données. Avoir son propre matériel peut permettre de faciliter une mobilité future. A noter que, sur le cas présenté, l'éditeur se chargeait de l'installation-maintenance. ° Option envisagée si les options cloud sont trop chères.	Solution plus particulièrement sélectionnée avec le mode SaaS et d'autant plus si l'offre est proposée par une autre collectivité (infrastructures mutualisées). Pour les plus grandes collectivités, cette solution peut être sélectionnée pour des services précis si l'hébergeur est repéré comme un acteur de confiance.	Cette option est souvent subie dans les retours d'expérience et peut s'accompagner d'une forte augmentation tarifaire. Pour celles qui en ont la capacité, elles peuvent renégocier les tarifs et s'assurer des conditions d'hébergement : localisation… Et dans certains cas, ajouter des modules de sécurité, de chiffrement.

FOCUS ENTREPRISES

LE CONTEXTE ACTUEL EST MARQUÉ PAR TROIS PHÉNOMÈNES

1 **Une numérisation grandissante des services qui entraîne une augmentation des besoins et des coûts SI**, quelle que soit la taille de l'entreprise, de manière assez similaire à ce qui s'observe côté collectivité.

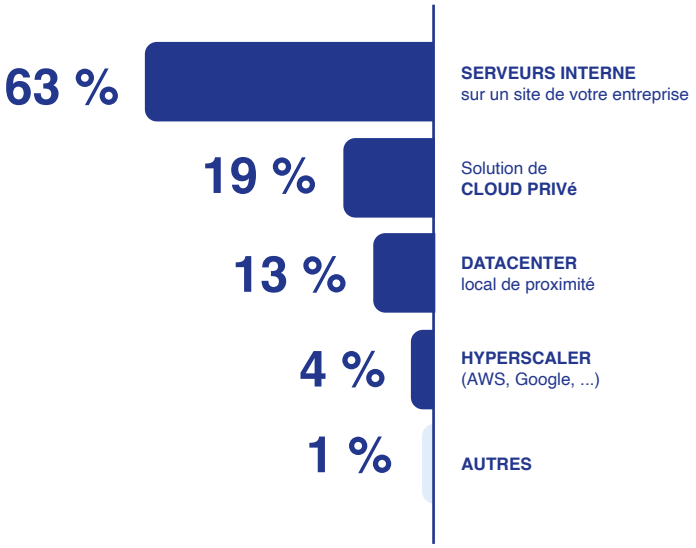
2 **Les plus grandes entreprises qui ont des datacenters privés changent de modèle,** les évolutions technologiques et les exigences en sécurité rendent leurs infrastructures existantes de plus en plus coûteuses à faire évoluer et à maintenir en propre. On observe deux tendances qui peuvent être complémentaires :

- **Basculer leur informatique et leurs datacenters privés vers le cloud**, afin d'adopter une approche Opex (locatif) plus économique au départ plutôt que Capex (investissement), même si à l'arrivée le mode cloud se révèle souvent plus coûteux.
- **Basculer leur datacenter privé vers des datacenters de proximité** de manière à avoir une meilleure qualité de service, à mieux anticiper les évolutions technologiques notamment l'intelligence artificielle, tout en conservant les bénéfices initiaux de leur datacenter privé (souveraineté des données, latence, à proximité).

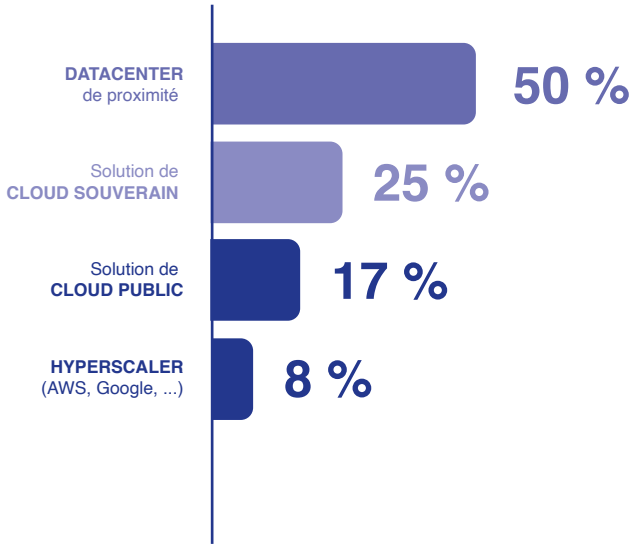
3 Le dernier baromètre « Fibre et usages numériques en entreprise » montre une **appétence significative des PME pour les datacenters de proximité**, une forte attention en général sur des offres d'hébergement souveraines.

BAROMÈTRE IFOP 2025 POUR COVAGE INFRANUM FIBRE ET USAGES NUMÉRIQUES EN ENTREPRISE

Actuellement **où sont hébergées vos solutions SI ?**



Pour les entreprises qui ont un projet **d'évolution de leurs solutions d'hébergement** dans les 12 prochains mois



Le taux actuel d'adoption d'une solution sur datacenter de proximité est à pondérer : la présence d'un datacenter de proximité, c'est-à-dire rapidement accessible du lieu de l'organisation, n'est pas systématique.

TENDANCES OBSERVÉES AUPRÈS DES PME, MEMBRES INFRANUM

Un sondage mené auprès des membres InfraNum, acteurs qui ont la spécificité d'être très bien informés sur les enjeux numériques, présente les enseignements suivants :

- **Un certain nombre d'entreprises met en place une stratégie hybride** : solution on-premise ou colocation associée à des solutions d'hébergement sur le cloud avec différentes modalités en fonction de la stratégie : PaaS, IaaS ou SaaS.

- **Certaines ont changé de stratégie récemment. Quelques exemples cités :**
  - **Passage d'une solution en colocation ou cloud public à une offre en cloud privé** pour des raisons de montée en gamme sur la sécurité. A noter que cela peut être à la demande des clients de l'entreprise, pas uniquement pour ses besoins propres.
  - **Certaines testent une offre cloud** le temps d'observer le comportement de leurs nouveaux services en termes d'impact sur le stockage des données, **avant de potentiellement étudier un retour en colocation.**

- **La solution en colocation est perçue comme la solution la moins coûteuse en théorie mais elle demande des ressources** dont il faut évaluer la charge de travail. Les solutions PaaS et IaaS sont des alternatives qui demandent moins de ressources et sont plus économiques qu'en mode SaaS. Le mode SaaS a l'avantage de disposer immédiatement de l'application.

LES PRINCIPAUX BÉNÉFICIAIRES DES OFFRES ADOSSÉES AUX DATACENTERS DE PROXIMITÉ

		MOTIVATIONS	CRITÈRES DÉTERMINANTS
DATACENTER DE PROXIMITÉ : GESTION DES INFRASTRUC-TURES DU DATACENTER	GRANDES ORGANISATIONS	Passer d'un datacenter privé à un hébergement privé sur un datacenter de proximité Redondance en propre (PRA)	**Proximité** / déplacement Qualité de service
	PETITES & MOYENNES ORGANISATIONS	Colocation si ressources en interne et suffisamment de besoin Plusieurs variantes possibles : uniquement en colocation ou stratégie hybride en fonction de la criticité des données	**Proximité** / déplacement Qualité de service Prix par rapport au cloud
	OPÉRATEURS TÉLÉCOMS	Besoin d'interconnexion au plus proches des antennes, micro-datacenters	**Proximité** / latence
	OPÉRATEURS CLOUD	Sécuriser les offres client une présence locale avec redondance et réduction de la latence Diversifier le réseau datacenters pour leurs offres cloud	**Local** / Prix / foncier moins cher Contrats / plus de facilité à négocier
	SOCIÉTÉS DE SERVICES INFORMATIQUE		
	COLLECTIVITÉS	Notamment pour mutualiser les ressources La gestion du datacenter peut être internalisée ou externalisée	**Proximité** / localisation Prix Confiance Autonomie
& CAPACITÉ À GÉRER DES SERVICES/ SERVEURS	TOUS	Colocation ou cloud dans un datacenter choisi, sur son territoire La notion de proximité est un vrai atout, y compris sur une offre cloud	**Proximité** / localisation / accès interlocuteurs / Confiance Prix

La notion de proximité est essentielle dès qu'il est question de colocation, d'hébergement sec, pour la gestion des serveurs. Il faut être en mesure de se rendre rapidement sur place.

De manière générale, à iso-services, une offre de proximité sera privilégiée par rapport à une offe cloud classique car elle permet de connaitre ses interlocuteurs, de créer un lien de confiance, de savoir que ses ressources informatiques sont physiquement sur le territoire sur un lieu clairement identifié.

Au delà de la proximité, il y a ensuite une segmentation des datacenters à prendre en compte en fonction de ses besoins : gamme de services adressées, du niveau de sécurité associé, etc..

Une collectivité ou un groupement d'acteurs publics peuvent décider de mettre à disposition des acteurs du territoire des infrastructures numériques mutualisées, avec des services de location et/ou d'hébergement. La personne publique est alors bien **propriétaire des ressources informatiques ce qui lui permet de s'affranchir de tout risque d'application de loi extraterritoriale** à ce niveau.

Les raisons qui amènent à déployer un tel projet sont de mettre à disposition une solution d'hébergement qui garantisse une **maîtrise optimale des données**, qui garantit un niveau de sécurité et d'empreinte environnementale optimisé, **à coût accessible pour les plus petites communes**.

On observe plusieurs modalités de mises en oeuvre, ci-dessous quelques exemples repérés (liste non exhaustive) :

Exploit-Maint* des serveurs externalisée	*NC*	Ville Sables d'Olonnes	Sarthe Numérique[3] (DSP)	*NC*	RUBIX CU du Creusot Montceau
Exploit-Maint* des serveurs internalisée	Val d'Oise numérique[4]	*NC*	GIP Eskemm Data (éducation)	*NC*	
	Scénario 1 Hébergement sec	**Scénario 2 Achat d'un datacenter existant**	**Scénario 3 Construction d'un site public** dédié acteurs publics	et privés	**Scénario 4 Favoriser la création d'un DC yc AAP**

** Exploitation-Maintenance*

Tous les exemples repérés ont en commun :

- Une absence d'offre territoriale
  Pas de datacenter de proximité
  Ou conditions non satisfaisantes
- Une collectivité qui a le besoin et les compétences pour mener un tel projet, et parfois une opportunité de lancement. Tout part de ses besoins et est ensuite élargi.
- Un support politique département et/ou région avec un besoin clairement identifié des communes

Le scénario choisi dépend ensuite principalement des opportunités qui s'offrent sur le territoire, du niveau de services demandés par les acteurs des territoires, du patrimoine existant.

SCÉNARIO

ACHAT D'UN DATACENTER EXISTANT

Entretien avec Carole Pesnel, Directrice des Systèmes d'Information à la Mairie des Sables d'Olonne

Un projet de datacenter public qui naît d'une opportunité sur le territoire des Sables d'Olonne.

La réflexion commence lorsque Mme Pesnel, auparavant DSI dans le secteur de la santé, découvre que les salles blanches de la ville n'ont pas de redondance électrique, pas de groupe électrogène dédié. En parallèle, la Mairie des Sables-d'Olonne souhaitait promouvoir le numérique et la souveraineté et il y avait sur le territoire un datacenter à vendre, qui avait des difficultés à trouver repreneur. Ce datacenter avait 10 ans d'âge, n'avait jamais été équipé, n'avait jamais servi : des bureaux, un plancher technique pour le cœur du datacenter, une partie avec trois groupes électrogènes.

Pour convaincre la direction générale, le projet a été présenté au département et à la région lesquels ont rapidement soutenu l'initiative. Par ailleurs, comme la ville n'était pas en mesure de gérer en propre ce datacenter, elle a fait appel à la région qui a proposé la structure Gigalis pour les accompagner. La société est ainsi autonome quant à la commercialisation du datacenter, vis à vis d'acteurs publics comme privés.

Par ailleurs, les DSI du département ont pu montrer un intérêt réel à cette nouvelle solution d'hébergement parce qu'il s'agit d'un datacenter situé sur le territoire, appartenant à une collectivité. En revanche, le sujet de la tarification reste déterminant : "*Parce que si c'est dix fois plus cher, personne n'ira. Mais si les prix sont raisonnables, le fait que ça a été racheté par une collectivité, c'est réellement un plus.*"

SCÉNARIO

CONSTRUCTION D'UN DATACENTER ET EXPLOITATION-MAINTENANCE EN PROPRE

Entretien avec Monsieur Philippe Lemonnier, Directeur Général du GIP Eskemm Numérique

Eskemm Numérique est un GIP qui porte le projet de création d'un datacenter ayant vocation à héberger les données des acteurs publics de l'Enseignement supérieur, de la Recherche et de l'Innovation de la Région Bretagne. C'est un projet labellisé par le ministère de l'Enseignement Supérieur et de la Recherche pour soutenir et rationaliser le développement de ressources IT et de calcul HPC pour les acteurs régionaux.

Le datacenter a nécessité un investissement d'un million d'euros. La salle réalisée répond aux plus hautes exigences de qualité avec un PUE cible de 1.4, et des critères de sécurité très élevés (ISO 27001 et HDS) liés au monde de l'ESR. Eskemm Numérique se définit comme un « grossiste en services d'infrastructure IT» qui a la capacité de fournir des services numériques (télécoms, hébergement, calcul, stockage, cloud, …) à sa communauté d'usagers. Ces derniers restent vraiment maîtres de leurs usages, de leurs stratégies numériques. Eskemm Numérique est donc un outil de mutualisation efficace, à disposition d'une communauté avec des exigences élevées de réactivité, de sécurité, de performances, d'ultra haut débit, … « *Ce positionnement stratégique doit permettre d'atténuer les inquiétudes des DSI : ils sont déchargés des problèmes et servitudes « mécaniques » et ils continuent à gérer leurs stratégies et leurs schémas directeurs* ».

L'adoption de l'offre est assez lente mais en ligne avec les prévisions. Les freins de la commercialisation reposent sur des interrogations légitimes des usagers concernant leur capacité à migrer dans l'infrastructure. Les usagers finaux ne peuvent pas la plupart du temps **évaluer les coûts réels des services utilisés** sur les infrastructures actuelles, ce qui peut être complexe pour faire prendre conscience du prix réel des services proposés. Cette équation économique est un véritable défi. Pour autant, une fois qu'ils ont testé les services, **ils ne font pas machine arrière et deviennent de vrais ambassadeurs.**

[3] Présentation du projet dans la partie 4 « Cadre légal et contractuel »
[4] Présentation du projet dans la partie 4 « Cadre légal et contractuel »

SCÉNARIO

FAVORISER L'ARRIVÉE D'UN DATACENTER

Entretien avec Monsieur Benjamin Ledoux, Directeur Technique de Rubix et Monsieur Yves Labaune, Chef de Projet numérique au sein du Pôle Aménagement et Projet territorial de la Communauté Urbaine du Creusot Montceau (CUCM)

Rubix est le premier datacenter de proximité de Saône-et-Loire soutenu par la Communauté Urbaine Creusot Montceau. L'ambition des fondateurs reposait sur la capacité à offrir une offre d'hébergement alternative sur l'axe TGV Paris-Lyon avec des tarifs plus compétitifs.

Pour favoriser l'arrivée de ce datacenter sur son territoire, la commune de communes a joué son rôle d'aménageur qu'elle avait déjà initié en 2004 avec la création d'un réseau fibre d'environ 300km à destination des entreprises et des établissements publics. **Elle a ainsi pris à sa charge un des deux raccordements électriques** via la mise à disposition du foncier et un des deux raccordements télécoms via son délégataire. **Elle a aussi débloqué une subvention de 100 000 euros** en tant qu'aide à l'installation des entreprises, ce qui a permis de participer au financement du projet qui s'est élevé à 2 M€. **Elle a facilité l'implantation du projet via le réseau de télécommunication délégué** qui a assuré un premier raccordement opérateur. Par ailleurs, la DSP initiale du réseau fibre étant arrivée à échéance, une nouvelle délégation a été lancée en élargissant le scope territorial en association avec la Communauté Urbaine du Grand Chalon **via la création de la SPL Sud Bourgogne. Le datacenter Rubix a de fait un champ d'action plus étendu grâce à l'interconnexion des deux RIP.**

Rubix est aujourd'hui compétitif car les coûts d'investissements sont maîtrisés : le foncier au Creusot Montceau permet d'offrir une gamme de services très compétitive à destination des collectivités et des entreprises.

le GUIDE du DATA CENTER de PROXIMITÉ

2

SOUVERAINETÉ NUMÉRIQUE

La souveraineté des données

Maîtrise technique

Sécurité et cybersécurité

Résilience

Vrai / Faux

SOUVERAINETÉ NUMÉRIQUE

“Souveraineté ! Souveraineté ! … souverainetés ?

L’évolution rapide ces dernières années du contexte géopolitique nous amène à rencontrer voire employer fréquemment le terme souveraineté – tel un leitmotiv – sans vraiment le définir.

Sur le plan numérique, si je stocke mes données et réalise mes calculs sur un serveur stocké dans un placard avec une sauvegarde sur une clef USB rangée dans un coffre-fort, suis-je souverain ?

Le mot souverain renvoyant la notion de pouvoir suprême, il y a alors une forme de souveraineté à l’échelle du placard. La révolution numérique en cours apportant des gains d’efficacité considérables, chacun de nous a conscience qu’une telle souveraineté en autarcie n’est pas une option sauf à revenir à l’ère pré-numérique.

Dans une démarche pragmatique, la souveraineté sur le plan numérique est considérée ici sous l’angle de l’autonomie stratégique : capacité d’une organisation à protéger ses données à la fois sans dépendances indésirables et sans contraintes excessives.

L’analyse du point de vue de l’autonomie stratégique amène à se pencher sur les différents aspects pratiques à considérer lorsque l’on cherche à conserver la maîtrise de ses données dans un monde numérique ouvert : l’Etat voire les Etats à même d’agir sur ses données, la maîtrise technique et tarifaire de leur hébergement, le niveau de sécurité et notamment de cybersécurité et enfin le degré de résilience.

Si ce guide est consacré aux datacenters de proximité, ce chapitre souveraineté a été rédigé dans une approche ouverte considérant le panel des solutions à la disposition des organisations pour l’hébergement de leurs données. Il permet ainsi de montrer que l’hébergement dans un datacenter de proximité constitue un équilibre dépendances / contraintes particulièrement intéressant dans un monde très ouvert sur le plan numérique mais avec une géopolitique devenue très instable”

ANTOINE FOURNIER,
PRÉSIDENT DE THÉSÉE DATACENTER
PRÉSIDENT DE LA COMMISSION DATACENTER INFRANUM

D’un point de vue juridique, la souveraineté numérique fait directement référence à la souveraineté des données et donc à la territorialité intègre par définition un ensemble d’obligations qui concernent tous les acteurs.

La souveraineté numérique est un concept complexe à décliner opérationnellement, qui peut sembler utopique si l’on réfléchit à toutes les implications matérielles, logicielles que cela signifie. Pour autant il s’agit de rester pragmatique et, **selon le niveau de criticité de ses données, faire des choix qui permettent d’être le plus souverain possible**, en tenant compte que c’est un processus d’amélioration continue.

La déclinaison opérationnelle utilisée dans ce guide s’appuie sur la décomposition du mot “maîtrise”. Sur base de cette définition, il devient possible de repérer les spécificités des datacenters de proximité.
Ainsi, bénéficier d’une offre d’hébergement sec dans un datacenter de proximité :

- **apporte une parfaite garantie sur la localisation des données** par rapport à une autre offre cloud, SaaS notamment, pour laquelle l’information n’est pas toujours disponible.
- **apporte ainsi la garantie de l’application à minima de la loi française**
- **peut répondre au besoin d’autonomie numérique des territoires** sur les enjeux du numérique.
- **une relation de confiance est plus facile à construire et à établir avec un fournisseur d’un datacenter de proximité** : c’est sur le territoire, les interlocuteurs sont accessibles, les infrastructures sont visibles, le fournisseur sait que son marché se limite aux acteurs du territoire et qu’il doit les convaincre. *“Je suis rassuré parce que quelque part, c’est proche de chez moi et je peux le voir.”*

2

Au-delà de la définition juridique de la souveraineté des données, au-delà des obligations RGPD, ce chapitre propose une déclinaison opérationnelle du terme "souveraineté numérique" et s'appuie notamment sur les retours d'entretiens menés auprès des collectivités et des industriels. Ci-dessous des extraits :

- Un terme "**garder la maîtriser**" revient particulièrement souvent lorsque les interlocuteurs sont interrogés sur leur définition de la souveraineté numérique. Cette maîtrise revêt alors divers aspects : **maîtrise des données, maîtrise technique, maîtrise tarifaire, maîtrise dans la gouvernance**…

- La deuxième notion qui revient régulièrement est la crainte de **l'application des lois extraterritoriales** et de tout ce qui peut découler autour du détournement de données. En approfondissant, il apparaît difficile de se prémunir totalement de ce risque au regard du nombre d'équipements et de logiciels utilisés au quotidien d'origine étrangère. Pour autant, en restant pragmatique, il est possible de garantir un minimum de souveraineté, sachant qu'il y a toujours une marge d'amélioration, que c'est un processus sur le temps long.

- De manière assez connexe, la crainte du **piratage** est évoquée avec l'usurpation de données, la commercialisation des données hébergées ou encore le contrôle à distance des infrastructures.

- **Le sujet des tarifs** revient régulièrement dans les entretiens, avec la difficulté d'anticiper un certain nombre d'options pour garder la maîtrise de ses outils, de ses données, les faire évoluer, les changer de datacenter, etc.

- La question des **logiciels utilisés** est également évoquée comme enjeu de souveraineté, de manière très pragmatique. Certains maintiennent l'accès à certains logiciels et y associent des politiques de sensibilisation sur les limites dans l'utilisation dans leur utilisation.

- **Enfin, la notion de maîtrise peut également recouvrer les sujets de résilience** : la capacité qu'a une infrastructure à se remettre en fonctionnement après un évènement exceptionnel, que ce soit lié au réchauffement climatique ou à un acte de vandalisme. Il est alors possible d'y intégrer les sujets de redondance les plus fondamentaux, de stratégie de **sauvegarde, de conditions de rétablissement**.

Ce chapitre présente, à travers une proposition de déclinaison opérationnelle de la souveraineté numérique, une description des obligations de chaque acteur et une description des bonnes pratiques à mettre en œuvre en fonction de la criticité des données hébergées.

[5] "Gestion des données : Quels outils et quelle stratégie pour les territoires ", Banque des territoires, 2020

UNE DÉCLINAISON OPÉRATIONNELLE DE LA SOUVERAINETÉ NUMÉRIQUE

SOUVERAINETÉ DES DONNÉES	MAÎTRISE TECHNIQUE ET TARIFAIRE	SÉCURITÉ / CYBERSÉCURITÉ	RÉSILIENCE
RGPD **Et ensuite : s'affranchir des lois extraterritoriales** • localisation des données et nationalité de l'entreprise • y compris de la solution de sauvegarde	**Maîtrise technique :** • clauses à prévoir en cas **d'externalisation** **Maîtrise tarifaire** : • **Evolutivité** de la solution et coûts associés • **Réversibilité des données** : capacité de changer de fournisseurs à coût maîtrisé	Mise en oeuvre d'une **politique sécurité / cybersécurité** adaptée au besoin NIS 2, ISO 27001, SecNumCloud	Assurance d'un **maintien des infrastructures** sur le temps long. Cela intègre les effets liés au **réchauffement climatique** Et doit se concrétiser par des engagements : • **Conditions de rétablissement de service** • **Redondance** numérique et énergétique • **Sauvegarde**

La première brique est bien celle qui crispe la majorité des débats, c'est la plus délicate à maîtriser de bout en bout (de l'équipement au logiciel). En effet, il s'agit de :

- **Vérifier le fonctionnement des outils** (logiciels et matériels) au moment de l'achat, de vérifier les interactions qu'ils peuvent avoir avec l'extérieur ;
- **Contrôler le fonctionnement des outils** en s'appuyant sur un tiers de confiance ou une certification pour assurer cette vérification ;
- **Dans le cas d'un outil de nationalité étrangère, vérifier la réglementation** qui peut s'appliquer indépendamment du fonctionnement de l'outil en conditions normales, indépendamment des clauses du contrat.

La souveraineté des données repose sur des engagements contractuels cohérents et la maîtrise du droit à appliquer.

Elle constitue un élément central de la souveraineté numérique. En effet la souveraineté numérique peut être vue comme la capacité, pour l'État, de contrôler et de protéger les données de ses citoyens, entreprises et administrations, en garantissant qu'elles restent soumises exclusivement aux lois de son propre territoire. Pour la France, il s'agit du droit français et européen.

En Europe, la protection des données repose sur le RGPD. Il s'agit du règlement européen qui a complété et renforcé la loi française de 1978 (loi « Informatique et Libertés ») qui avait créé le cadre juridique pour la protection des données personnelles, sous le contrôle de la CNIL, autorité chargée de vérifier le respect des mécanismes de protection et de garantir que les données personnelles restent soumises au droit national et européen. À titre d'exemple, la CNIL n'hésite pas à recommander des solutions d'hébergement auprès d'opérateurs relevant uniquement du droit français ou européen (CNIL, 20 avril 2020, délib. n° 2020-044 - à propos de l'hébergement de données de santé).

In fine, l'objectif est de se prémunir contre toute ingérence ou accès d'acteurs étrangers ou de leurs autorités, rendu possible par l'existence de lois à portée extraterritoriale, telles que le Cloud Act américain. Pour l'hébergement de ses données, ceci implique de veiller non seulement à la localisation géographique des données, mais également à leur sauvegarde et à la structure actionnariale des prestataires concernés. C'est pourquoi, la souveraineté des données implique notamment de veiller au statut des hébergeurs. Elle repose donc sur une contractualisation attentive avec ces prestataires, garantissant à la fois la protection des données et le respect des obligations légales.

La contractualisation avec les datacenters de proximité au service des entreprises et collectivités de leurs territoires permet de bénéficier de la souplesse de partenaires locaux de long terme. Les datacenters de proximité constituent donc des partenaires privilégiés pour toute organisation souhaitant maintenir ou reprendre la maîtrise de ses données : savoir précisément qui contrôle l'infrastructure et quels sont les engagements contractuels associés.

RGPD, RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

Le RGPD est fondamental sur le sujet de la souveraineté des données, il impose des obligations auprès de chaque acteur, lesquelles obligations visent à protéger les données des utilisateurs.

SYNTHÈSE DES OBLIGATIONS LÉGALES ET RESPONSABILITÉS

ACTEUR CONCERNÉ	DONNÉES CONCERNÉES	RESPONSABLE	OBLIGATIONS
Exploitant du datacenter	Données personnelles internes (badges, logs d'accès, vidéos internes, …)	Responsable de traitement	Responsable de traitement
Client en colocation (entreprise, collectivité)	Données hébergées sur ses serveurs	Responsable de traitement	Garantir la conformité RGPD de ses traitements Définir les mesures de sécurité Informer les personnes concernées Respecter les droits RGPD (accès, effacement, etc.)
Exploitant (en colocation)	Accès indirect aux données du clients	Sous-traitant éventuel (si accès technique prévu par contrat)	Clauses contractuelles RGPD (article 28) Obligation de confidentialité Respect des instructions du client
Collectivité exploitant son propre datacenter	Données des usagers, données internes, données sensibles (santé via CCAS, aide sociale, etc.)	Responsable de traitement	Respect intégral du RGPD Hébergement HDS obligatoire pour données de santé Sécurisation renforcée pour la vidéoprotection Transparence et information des usagers
Usagers / citoyens	Données personnelles confiées à la collectivité	N/A	Bénéficient de droits : accès, rectification, effacement, opposition, portabilité Droit à l'information sur l'usage de leurs données

Lorsque l'organisation n'assure pas directement l'exploitation-maintenance du datacenter, du bâtiment et/ou des ressources informatiques, elle doit alors assurer un contrôle renforcé de ses prestataires, en s'assurant que les cahiers des charges garantissent bien la souveraineté de ses données.

À cet effet, il existe des leviers juridiques pour encadrer l'hébergement des serveurs à plusieurs niveaux :

LA GOUVERNANCE / LES MODES DE GESTION DES DATACENTERS

GESTION DIRECTE : si l'organisation assure directement la construction, l'exploitation et la gestion du datacenter (ex : en régie), la souveraineté de la gouvernance est garantie.

GESTION EXTERNALISÉE : Si elle fait appel à un prestataire externe (ex : location d'un espace d'hébergement dans un datacenter existant, marché public ou concession pour la construction et l'exploitation d'un datacenter), le prestataire doit disposer de capitaux majoritairement français, ou à défaut européens afin d'éviter l'impact des législations extra-européennes. Elle peut également pérenniser une structure juridique européenne en incluant une clause de changement de contrôle dans le contrat de prestation de services. Ainsi, elle pourra aisément renégocier, voire résilier le contrat en cas de rachat du prestataire par une entité dont le siège social est hors de l'UE.

LA CHAÎNE D'APPROVISIONNEMENT DU DATACENTER

Le choix des fournisseurs de matériels et logiciels doit être encadré pour éviter que certains équipements ne compromettent la souveraineté en raison des transferts de données hors de l'UE. Il est possible de veiller à la conformité avec les réglementations européennes en s'assurant que les fournisseurs de l'organisation disposent de la certification CISPE ou à défaut d'un équivalent.

LE CONTRÔLE DES ACCÈS PHYSIQUES AUX ESPACES SENSIBLES DU DATACENTER

En cas de gestion directe ou externalisée, l'organisation doit restreindre l'accès aux espaces sensibles (ex : salle informatique, meet-me-room) aux agents ressortissants de l'Union européenne. En cas d'externalisation, il convient de préciser dans le contrat que l'accès aux espaces sensibles est limité aux ressortissants de l'Union européenne.

BONNES PRATIQUES/RECOMMANDATIONS : En cas d'externalisation, inscrire ces trois exigences dans les cahiers des charges et les appels d'offres afin de garantir la souveraineté des données hébergées sur les serveurs de la collectivité.

LA SÉCURISATION PHYSIQUE DES INSTALLATIONS

En raison de leur caractère essentiel, il est **impératif de prévoir des dispositifs permettant d'assurer la sécurité physique des installations**. La transposition prochaine de la Directive NIS 2, qui s'impose aux datacenters de proximité et à certaines collectivités territoriales, viendra renforcer ce qui relevait jusqu'alors de la seule négociation contractuelle

Le choix des dispositifs associés dépend des niveaux de criticité et de sensibilité de l'exploitation.

L'opérateur du datacenter peut faire le choix d'installer plusieurs SAS d'accès, de restreindre l'accès au bâtiment au travers de solutions allant du simple badge d'accès jusqu'au lecteur d'empreintes digitales ou rétiniennes. Les bâtiments sont généralement équipés de caméras de vidéo-surveillance et peuvent disposer de personnels assurant la surveillance des locaux 7j/7 24h/24. Cela permet une réaction rapide non seulement en cas d'intrusion, mais également en cas d'évènements intérieurs au datacenter comme un incendie ou une fuite du système de refroidissement. Il existe une notion de sécurité dite « périmétrique » : il s'agit en général d'une clôture renforcée voire rehaussée pour éviter les intrusions (dans certains cas, un barbelé concertina est installé entre deux clôtures grillagées). Certains exploitants choisissent de mettre en place des sas périphériques : la salle d'hébergement est au centre des salles passives (sans équipement) pour en éviter l'accès direct depuis l'extérieur.

Enfin, les systèmes informatiques eux-mêmes sont équipés de dispositifs de protection contre les intrusions informatiques. Contractuellement, il est également possible de prévoir une redondance de la solution.

LA SÉCURISATION DES ACCÈS FIBRES (HORS DE L'ENCLOS)

Bien que les datacenters soient eux-mêmes très sécurisés, leur connexion aux réseaux télécoms peut constituer un point de vulnérabilité puisque les câbles transitent par des chambres de proximité qui, généralement, n'appartiennent pas au datacenter et sont souvent bien moins (voire pas) sécurisées. Malgré la sécurisation de l'enceinte du datacenter et ses accès redondés au réseau, il reste vulnérable à une action concertée visant les câbles fibres optiques d'accès, même redondés, qui sont (trop) facilement accessibles via des chambres situées à proximité.

Selon le niveau de sensibilité identifié, il peut être essentiel de sécuriser non seulement le datacenter lui-même, mais aussi ces chambres de proximité par lesquelles transitent tous les flux de données et protéger les activités critiques contre l'isolement et l'accès à des secrets d'affaires.

Cette sécurisation additionnelle nécessite toutefois des installations supplémentaires, qui ne peuvent être réalisées qu'en lien avec les opérateurs télécoms exploitant les accès fibres en question.

UNE DIFFICULTÉ TECHNIQUE :
PROTÉGER EFFICACEMENT SANS COMPLEXIFIER LES OPÉRATIONS DE MAINTENANCE

Le verrouillage des chambres ne semble pas être une solution efficace, comme l'a montré l'expérience des armoires pour les réseaux de fibre optique. La solution réside probablement dans une surveillance continue de l'accès à ces chambres, par caméras de vidéoprotection pointées vers les chambres sensibles éventuellement complétées par des capteurs en détectant l'ouverture, qui s'inscrirait dans une démarche plus générale de la collectivité, dans le cadre de ses pouvoirs de police. En l'absence de vidéoprotection et d'énergie à proximité, une détection optique de l'ouverture peut être placée sur la fibre ou les chambres elles-mêmes, éventuellement associée à une levée de doute par caméra spécifique.

Cette surveillance doit être associée à une capacité d'intervention rapide en cas d'événement suspect, par les services de police municipale, idéalement depuis le datacenter à proximité, en coordination avec les opérateurs télécoms et idéalement avec le datacenter à proximité.

UNE CONTRAINTE JURIDIQUE : CONCILIER LES DROITS ET OBLIGATIONS DE L'EXPLOITANT DU DATACENTER ET DES OPÉRATEURS TÉLÉCOMS

Dès lors que les chambres d'adduction et fibres optiques qui desservent le datacenter appartiennent à un ou plusieurs opérateurs télécoms contractuellement chargés de la connectivité du local, une coopération étroite et une communication transparente entre toutes les parties sont essentielles pour atteindre cet objectif de sécurisation supplémentaire.

Le partage des responsabilités peut ainsi être négocié dans le cadre de l'ingénierie d'un réseau public de vidéoprotection, ou du renforcement des modalités contractuelles renforcées avec l'opérateur télécom exploitant la chambre d'adduction ou la connectivité du datacenter. Un renforcement des obligations contractuelles des opérateurs télécoms vis à vis des préfectures en cas d'intrusions sur les réseaux pourrait également être envisagé.

Si cette sécurisation additionnelle n'est pas expressément prévue par les mesures de contrôle de l'accès aux datacenters de la Directive NIS 2 ou de son règlement d'exécution 2024/2690, l'exploitation des chambres d'adduction pour accéder aux données transitant par le datacenter est susceptible de constituer un incident important devant donner lieu à notification.

LA CYBERSÉCURITÉ : DIRECTIVE NIS 2

La Directive NIS 2 (2022/2555), publiée le 27 décembre 2022 au JO de l'UE, s'inscrit dans la continuité de la première Directive NIS 1, adoptée en 2016.

OBJET : Ce texte a été adopté d'une part, en raison de l'augmentation exponentielle des attaques de rançongiciels, dans lesquelles des logiciels malveillants chiffrent les données et les systèmes et exigent le paiement de rançon pour les débloquer et, d'autre part, en raison de la mise en œuvre hétérogène dans les différents Etats membres de l'Union européenne de la Directive NIS 1, si bien qu'il a été nécessaire d'harmoniser de manière plus importante les règles au niveau européen.

Ainsi, ce texte vise à créer une approche commune et harmonisée au sein de l'Union Européenne, garantissant que tous les États membres appliquent des exigences de cybersécurité similaires en matière de sécurité des réseaux et des systèmes d'information pour les entreprises privées et les administrations publiques. Cette harmonisation doit favoriser également le partage de l'information et des connaissances, ainsi que la capacité à répondre aux cyberattaques.

À la date de la publication du guide, elle n'a toujours pas été transposée en droit français, alors que la date limite de transposition était fixée au 17 octobre 2024. Un projet de loi a été déposé le 15 octobre 2025 au Parlement. Sa transposition sera examinée le 11 mars 2026 au Sénat. L'ANSSI, en tant qu'autorité nationale en matière de cybersécurité et de cyberdéfense, est l'autorité compétente pour assurer sa mise en œuvre.

CHAMP D'APPLICATION : Le champ d'application de la Directive NIS 2 a été fortement élargi par rapport à la Directive NIS 1, pour concerner de nouveaux secteurs d'activités. Ces secteurs incluent notamment les infrastructures numériques, la gestion des eaux usées, ou encore les administrations et collectivités publiques.

Ces secteurs, définis dans le texte de la Directive NIS 2, sont classés en deux grandes catégories (annexe I de la Directive) : les secteurs hautement critiques et les secteurs critiques.

Cette distinction permet d'imposer des obligations proportionnées, en tenant compte des différents niveaux d'exposition aux risques d'une entité. Avec cette nouvelle classification, les entités opérant dans ces domaines seront désormais identifiées comme entités importantes (EI) ou entités essentielles (EE).

S'agissant plus spécifiquement des infrastructures numériques, la Directive NIS 2 cible plusieurs acteurs, notamment les fournisseurs de services de centres de données, les fournisseurs de réseaux de communications électroniques publics ou encore les fournisseurs de services d'informatique en nuage, dans les secteurs hautement critiques.

OBLIGATIONS IMPOSÉES (liste non exhaustive) : Les data centers fournisseurs de services de centre de données, identifiés comme entités importantes (EI) et entités essentielles (EE) par la Directive NIS 2, doivent mettre en place des mesures de gestion des risques en matière de sécurité et notamment la mise en place d'un pilotage de la sécurité des réseaux et système d'information comprenant la formation à la cybersécurité de la direction et des personnes physiques exposées au risque en la matière[6].

Une obligation de notification des incidents est désormais obligatoire, sans retard injustifié, pour tout incident ayant un impact important sur les fournitures des services auprès du CSIRT[7] ou de l'ANSSI. En outre, ces mesures peuvent également porter sur la sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs.

[6] Article 14 du projet de loi de transposition
[7] https://www.cert.ssi.gouv.fr/csirt/csirt-territoriaux/

SANCTIONS : En cas de non-respect de ces obligations, la Directive NIS 2 prévoit que des sanctions pénales ou administratives peuvent être infligées. Par exemple, pour les sanctions administratives, des amendes pourront être appliquées par l'ANSSI, de manière proportionnées en fonction de la gravité du manquement.

Entretien avec Jean Bernard YATA - Directeur dans la branche conseil Thales Cyber Solutions

L'objectif principal de la Directive NIS 2 vise à contraindre notamment les entités visées, à respecter les exigences minimales de cybersécurité ;

Délai de trois ans pour respecter les obligations contraignantes visées de la Directive NIS2 compte tenu du coût et de la technicité organisationnelle à mettre en oeuvre pour répondre aux exigences de la Directive ;

Solutions à mettre en place dès maintenant : nécessité pour les collectivités territoriales d'investir dans les solutions de sauvegarde, protection des postes de travail et sensibilisation des collaborateurs.

LA CERTIFICATION ISO 27001

La certification d'ISO 27001 participe à une démarche **volontaire** visant à renforcer la protection des informations et notamment le système de management de la sécurité de l'information. Cette certification permettra de renforcer les exigences mentionnées dans la Directive NIS 2, mais ne permet pas de satisfaire totalement aux exigences mentionnées de la Directive NIS 2 qui ces dernières sont bien plus contraignantes.

Entretien avec Luc CHAUSSON, BYCYB

Le déroulement d'une certification ISO 27001 suit un processus structuré autour de deux phases principales : un **audit documentaire** et un **audit sur site**. Ces audits, réalisés par un organisme accrédité comme le BYCYB, sont suivis d'un rapport d'audit qui oriente la décision finale de certification. L'objectif est d'accompagner l'entreprise vers la réussite, même en cas de non-conformités initiales, via des audits complémentaires.

La certification, valable trois ans, est renforcée par des audits annuels de surveillance et un audit de renouvellement, assurant la pérennité du management de la sécurité.

SECNUMCLOUD

Luc CHAUSSON : " La qualification SecNumCloud repose sur un processus rigoureux, jalonné de quatre étapes clés allant de la validation de l'éligibilité à la décision finale de qualification par l'ANSSI. Au-delà de la conformité technique, cette démarche intègre des exigences spécifiques de souveraineté, telles que la localisation en Europe, des règles sur la détention du capital et le contrôle des activités chez les sous-traitants."

LE CODE CISPE

Entretien avec Alban Schmutz, CLOUD DATA ENGINE

Les datacenters peuvent répondre aux besoins croissants d'outils fiables pour prouver leur conformité réglementaire, en intégrant des services de conformité directement à leur infrastructure : gestion des accès, journalisation des événements, sécurisation des traitements, archivage conforme…

Par exemple, pour répondre aux exigences du RGPD, un hébergeur peut être audité sur un code de conduite sectoriel reconnu, comme le **Code CISPE**, approuvé par le Comité Européen à la Protection des Données. **Ce cadre permet de produire des preuves électroniques opposables, enrichies automatiquement, qui démontrent la conformité effective des traitements**.

Ces engagements peuvent être renforcés par des certifications techniques comme **ISO 27001, SecNumCloud ou CNDCP**, qui viennent documenter la maturité opérationnelle, sécuritaire ou encore environnementale des offres d'hébergement. Ensemble, ces éléments permettent l'obtention du **label Gaia-X**, désormais exigé ou valorisé dans des appels d'offres émanant de grands groupes comme EDF ou Airbus.

Le principe de résilience trouve une déclinaison opérationnelle au travers un certain nombre de garantie sur lesquelles s'engagent les acteurs des datacenters. Les datacenters sont classifiés en 4 catégories (ou TIER en anglais) en fonction de leur niveau d'équipement et de leur niveau de disponibilité. La certification TIER est attribuée par l'entreprise américaine de certification Uptime Institute (aujourd'hui 451 Group).

CLASSIFICATION DES DATACENTERS

	TIER 1	TIER 2	TIER 3	TIER 3+	TIER 4
TEMPS DE COUPURE PAR AN	28,8 h	22 h	1,6 h	1,6 h	0,4 h
DISPONIBILITÉ	99,671 %	99,741 %	99,982 %	99,982 %	99,995 %
MAINTENANCE DURANT LE FONCTIONNEMENT	Non	Non	Oui	Oui	Oui
RÉSEAU ÉLECTRIQUE ET REFROIDISSEMENT	Unique	Unique + relais de secours	Unique + relais de secours	Au moins 2	Au moins 2 + relais de secours
DISTRIBUTEUR D'ÉLECTRICITÉ	Unique	Unique	Unique + relais de secours	Unique + relais de secours	Au moins 2
RÉSEAU DE COMMUNICATION	Unique	Unique	Unique + relais de secours	Unique + relais de secours	Au moins 2 (actifs en permanence)
STRUCTURE	Salle intégrée	Salle intégrée	Bâtiment en propre	Bâtiment en propre	Bâtiment en propre
PARC ACTUEL	Obsolète	Anciennes structures	Majorité de l'offre actuelle	De plus en plus de constructions	Niche
COÛT DE PRODUCTION AU M²	- 5 000€	- 6 500€	- 8 000€	- 10 000€	- 12 000€

Source : Uptime Institute, Banque des Territoires - Caisse des Dépôts

Note : **La catégorie TIER 3+ ne figure pas dans la classification officielle**, mais figure sur ce tableau car elle est communément utilisée

La certification TIER 4 est complexe à obtenir. Elle suppose que l'opérateur du datacenter soit en capacité de restaurer l'alimentation électrique de son site sans aucune incidence sur la disponibilité de ses équipements. Il est nécessaire d'avoir deux lignes électriques venant de deux sources d'électricité différentes par des cheminements différents. Si les configurations multi-sites ne sont pas obligatoires pour obtenir la certification, certains datacenters TIER 3 et TIER 4 sont répliqués sur plusieurs sites géographiques, afin d'éviter toute indisponibilité en cas de destruction de l'un d'eux.

Au-delà de la résilience dite «classique», il y a des territoires qui sont confrontés à des phénomènes climatiques exceptionnels et qui demandent des adaptations exceptionnelles. Les datecenters de proximité intègrent alors de l'innovation au service de la résilience.

LE DATACENTER DE MAYOTTE EN SITUATION EXTRÊME

Entretien avec Feyçoil MOUHOUSSOUNE, Directeur Général d'ITH

ITH a créé un datacenter à Mayotte dont l'ouverture a été réalisée en octobre 2022 après une construction en 12 mois en pleine période COVID. Ce projet longuement réfléchi, a bénéficié du soutien financier de la Banque des Territoires en tant qu'investisseur avisé. Le Datacenter d'ITH a démontré tout son intérêt et sa résilience lors du passage du cyclone Chido, événement climatique majeur.

En effet, la philosophie du projet a évolué pour intégrer dès sa conception un projet résilient aux phénomènes naturels et climatiques. La démocratisation du Cloud et des nouveaux usages IT a également conduit à approfondir l'analyse des besoins auprès du marché local. Ce dernier s'est montré à la fois très attentif et demandeur d'une infrastructure pérenne, résiliente, répondant aux plus hauts critères à la fois d'évolutivité et de sécurisation des infrastructures et des services. Ainsi le datacenter a été imaginé dans une zone géographique à proximité de l'arrivée du câble sous-marin, mais également **suffisamment en hauteur pour éviter tout risque naturel de submersion marine. Il a été conçu selon des normes sismiques et cycloniques très élevées**. L'idée de réhabilitation a été vite abandonnée car beaucoup trop chère et nécessitant de lourds travaux.

Dès 2018, le permis de construire a été déposé pour un datacenter de type Tier 3 de 80 baies dans deux salles blanches de 40 baies en étage et de la salle technique en rez-de-chaussée. Cet appui de cabinets spécialisés gage de qualité du dossier a conduit à **une première estimation d'investissements de l'ordre de 10 M€ pour intégrer l'ensemble des critères et contraintes** définies dans le cahier des charges.

Pour soutenir la faisabilité économique de l'opération, un tour de table à la recherche de fonds était nécessaire. Dès la présentation du projet, **la Banque des Territoires a été séduite par le projet.** Elle a réalisé une analyse du dossier et a exigé notamment **l'intégration d'enjeux de résilience, de souveraineté, de neutralité, d'enjeux de performances énergétiques et d'enjeux environnementaux**. Cet accompagnement a également validé la pertinence et l'intérêt d'un tel projet pour le territoire de Mayotte.

Dès l'ouverture du projet en octobre 2022, les commandes confirmées se sont traduites par **un taux de remplissage à 70% de la première salle.** Il n'existait auparavant aucune offre datacenter privé sur le territoire, l'attente était forte aussi bien pour les acteurs publics que les acteurs privés.

Le cyclone Chido a soumis le datacenter à une épreuve grandeur nature. Malgré des dommages extérieurs liés à des vents dépassant les 300 km/h, l'infrastructure est restée pleinement opérationnelle, démontrant la robustesse et la résilience du site. **Dans un contexte de crise, cette continuité de service a achevé de convaincre de nouveaux acteurs du territoire à se tourner vers ITH pour assurer la sauvegarde et la reprise de leurs activités**. Le datacenter s'est ainsi affirmé comme un véritable outil de plan de continuité et de reprise d'activité pour le territoire. À l'issue de l'événement, la sécurité a été renforcée par de nouveaux dispositifs de surveillance et de gardiennage. Le site est devenu un véritable refuge numérique, accueillant en urgence des infrastructures critiques et de nouveaux clients, ce qui a contribué à asseoir encore d'avantage sa crédibilité auprès des acteurs locaux.

MES DONNÉES ET LOGICIELS SONT HÉBERGÉES CHEZ UN HÉBERGEUR FRANÇAIS OU EUROPÉEN, IL N'Y A AUCUN RISQUE DE TRANSMISSION.

VRAI en partie

Il s'agit de bien distinguer le propriétaire du datacenter, le bâtiment, de l'opérateur cloud. L'acteur qu'il faut considérer est l'opérateur cloud, lequel peut les gérer sur site et à distance. Les lois extraterritoriales peuvent s'appliquer si cet acteur est étranger.

À noter la recommandation d'ajouter une clause de changement de contrôle dans le contrat de prestation de services. Ainsi, l'organisation pourra aisément renégocier, voire résilier le contrat en cas de rachat du prestataire par une entité dont le siège social est hors de l'UE.

MES DONNÉES ET LOGICIELS SONT SUR UN SERVEUR QUI M'APPARTIENT ET SI J'UTILISE UN LOGICIEL ÉTRANGER SUR MON SERVEUR POUR DU TRAITEMENT DE DONNÉES, LA LOI EXTRATERRITORIALE NE S'APPLIQUE PAS

FAUX

La loi extraterritoriale s'applique en fonction du mode d'utilisation du logiciel.

UN DATACENTER DE PROXIMITÉ N'A PAS BESOIN DE RESPECTER LES MÊMES NORMES DE SÉCURITÉ ET DE PROTECTION DES DONNÉES QU'UN GRAND CENTRE DE DONNÉES.

FAUX

Ce sont les mêmes normes quelle que soit la taille des datacenters.

Vous avez envie de poursuivre le débat, poursuivre le jeu, n'hésitez pas à nous joindre sur contact@infranum.fr

le GUIDE du DATA CENTER de PROXIMITÉ

3

ENVIRONNEMENT

Indicateurs énergétiques et environnementaux

Analyse du cycle de vie

La récupération de chaleur fatale

Les technologies de refroidissement des datacenters

Réglementation Environnementale et urbanistique

ENVIRONNEMENT

“Le Numérique, notamment les Data Center, génère plus d’émission de CO2 que l’aéronautique, 3 à 4% des émissions mondiales selon les études. Le refroidissement des serveurs dans un Centre de données représente de l’ordre de 40% de la consommation d’énergies total du Data Center. Ces 2 constats posés, il est donc capital de penser sa stratégie d’hébergement de serveurs et ou de logiciels en pensant aux impacts environnementaux.

Le Data Center de proximité est une réponse à cette problématique par sa petite taille et son intégration dans le territoire. Quand bien même les effets d’échelle des Hyperscaler réduisent théoriquement les impacts environnementaux, la personnalisation des solutions permise par les Data Center de proximité limitent les conséquences sur le climat. Le Data Center de proximité rend plus soutenable l’hébergement de ses data en favorisant les circuits courts.

Enfin il faut mettre en balance tous les impacts positifs du numérique, comme les visio conférences, le télétravail, les optimisations des processus de toutes sorte : industriel, de gestion, d’échange, … En résumé, le numérique agit comme un levier puissant pour réduire les émissions de CO2 en transformant les modes de production, de consommation et de déplacement. Il permet une meilleure efficacité et une dématérialisation qui combinées, contribuent à limiter l’empreinte carbone globale.

Le Numérique n’est pas le problème, en matière d’émission de CO2, mais plutôt une partie de la solution.”

ETIENNE DUGAS,
DIRECTEUR GÉNÉRAL DE GROLLEAU
CO-PRÉSIDENT DE LA COMMISSION DATACENTER INFRANUM

Ce chapitre présente les différents indicateurs et solutions liées à l’impact environnemental des centres de données qu’une organisation peut considérer dans son choix d’hébergement numérique.

Dans ce cadre, il est intéressant de s’interroger sur les spécificités d’un datacenter de proximité par rapport à un autre datacenter ou autre offre sur le cloud.

En ce qui concerne les principaux indicateurs, le PUE notamment, les considérations sont les mêmes quelle que soit la typologie de datacenter.

- **Ils peuvent arriver à des performances environnementales équivalentes aux autres datacenters** : si les économies d’échelle sont moindres, les offres sur datacenters de proximité favorisent une optimisation des ressources informatiques au plus proche des besoins client ;
- **Ils garantissent en revanche de meilleurs résultats que les solutions internes** aux organisations.

Sur d’autres aspects les datacenters de proximité ont des avantages :

- **Ils s’intègrent** plus facilement dans l’environnement, ils peuvent réutiliser du foncier existant (moindre artificialisation des sols) ;
- Leur intégration territoriale facilite **des projets de récupération de chaleur** ;
- **Ils répartissent la consommation des ressources** (eau, énergie) territoire à territoire, à l’instar des méga-datacenters qui concentrent une forte consommation en un point du territoire et peuvent provoquer des conflits d’usage.


BPA-1

ENERGIE

Le plus proche possible de 1
Objectif CNDCP : 1,3 - 1,4

Certains projets atteignent 0,05 - 0,1

Hyperscalers : 1
Colocation : 0,4 - 0,7
DC anciens : 0,05 - 0,1

EAU

Le plus proche possible de 0
0,3 environ en 2025
Objectif CNDCP : < 0,4

CARBONE

Plus on se rapprochede 0
Moyenne mondiale : 0,3 - 0,5
France : 0,05 - 0,15

Les indicateurs existent sur 3 dimensions principales de l'impact environnemental : **la consommation énergétique, la consommation d'eau, et les émissions de CO2.**

Ces indicateurs permettent de comparer la performance des datacenters et de fixer des objectifs (par exemple le Climate Neutral Data Center Pact ou CNDCP). Cependant, pour être représentatif, un indicateur tel que le PUE doit être calculé sur une moyenne annuelle avec suffisamment de données.

La facture d'énergie est une donnée clé pour calculer l'efficacité énergétique, et l'implication des équipes d'exploitation lors de la conception des datacenters est essentielle.

$$PUE = \frac{\text{Énergie consommée par le datacenter}}{\text{Énergie consommée par les équipements informatiques}}$$

$$ERE = \frac{\text{Énergie consommée par le datacenter - Énergie réutilisée}}{\text{Énergie consommée par les équipements informatiques}}$$

$$REF = \frac{\text{Énergie renouvelable consommée par le datacenter}}{\text{Énergie totale consommée par le datacenter}}$$

$$WUE = \frac{\text{Quantité d'eau consommée par le datacenter}}{\text{Énergie consommée par les équipements informatiques}}$$

$$CUE = \frac{\text{Émissions de CO2}}{\text{Énergie consommée par les équipements informatiques}}$$

ENERGIE

Le PUE est **le principal indicateur de performance énergétique.**

Plus le ratio est proche de 1, plus le datacenter est performant, mais il est impossible d'atteindre 1 car il y aura toujours d'autres équipements consommateurs (refroidissement…).
Le PUE est un indicateur clé qui a beaucoup évolué ces dernières années, passant de 1,47 de moyenne en 2024[1]. La valeur du PUE peut être dégradée ou améliorée en fonction de l'utilisation d'eau pour le refroidissement ou de la récupération de chaleur.

On peut compléter le PUE avec d'autres indicateurs :

- **Pour accentuer les gains de performance sur le refroidissement** : le CER est plus sensible à l'efficacité du système de climatisation que le PUE. Il est particulièrement important lors de l'évaluation de la chaleur résiduelle.
- **Pour mieux valoriser la réutilisation d'énergie :** l'ERE permet de mesurer la réutilisation de l'énergie (Reuse). Si le datacenter valorise l'énergie dégagée par ses équipements, l'ERE est inférieure au PUE. Il permet par exemple de prendre en compte la chaleur émise par les serveurs qui est réinvestie, par exemple pour chauffer un bâtiment annexe.
- **Pour encourager l'utilisation d'énergie renouvelable :** le REF valorise l'achat d'énergie dite « verte » ainsi que la production en autoconsommation. Cela inclut les PPA car l'origine renouvelable de l'énergie achetées est garantie.
- **Pour avoir une mesure plus complète** : le DCEM (Data Center Energy Management) est un outil européen qui vise à remplacer le PUE en proposant une mesure plus complète et fiable, mais sa complexité le rend aussi peu utilisé actuellement. Il consolide les 4 dimensions ci-dessus.

[1] *Refroidissement des Datacenters - Technologies utilisées en France, potentiel d'économies* - ADEME et CRITICAL BUILDING, 2025.

EAU

Le WUE est **le principal indicateur pour mesurer l'efficacité de la consommation d'eau d'un datacenter.**
Il s'exprime en l/kWh/an.

CARBONE

Le CUE est **le principal indicateur pour mesurer les émissions de gaz à effet de serre liées au fonctionnement d'un datacenter**. Le CUE est le rapport entre la quantité totale de gaz à effet de serre équivalent consommée par le datacenter (en kgCO2) et la quantité d'énergie utilisée par les équipements informatiques, exprimée en kWh. La méthodologie de calcul sur l'ensemble du périmètre (scope 1, 2 et 3) devant encore être précisée, l'indicateur reste tendanciel.

POURQUOI FAIRE UNE ACV ?

Pour les exploitants et gestionnaires : avoir un outil pour optimiser l'efficacité énergétique et réduire son empreinte carbone afin **de diminuer les coûts opérationnels tout en respectant les engagements environnementaux et réglementations** (RE2020…). Une ACV complète peut valoriser un dossier auprès de certaines préfectures et collectivités.

Pour les entreprises et collectivités clientes : **sélectionner des partenaires plus responsables dans le cadre d'une stratégie numérique responsable.**

1ER POSTE D'IMPACT : L'EXPLOITATION

70 et 85 % des émissions
La phase d'exploitation représente en moyenne la part **la plus importante** des émissions, de par la consommation électrique des serveurs et des systèmes de refroidissement.

LE DÉFI : COMMENT RÉDUIRE LA CONSOMMATION TOUT EN GARANTISSANT LE FONCTIONNEMENT OPTIMAL DES SERVEURS ?

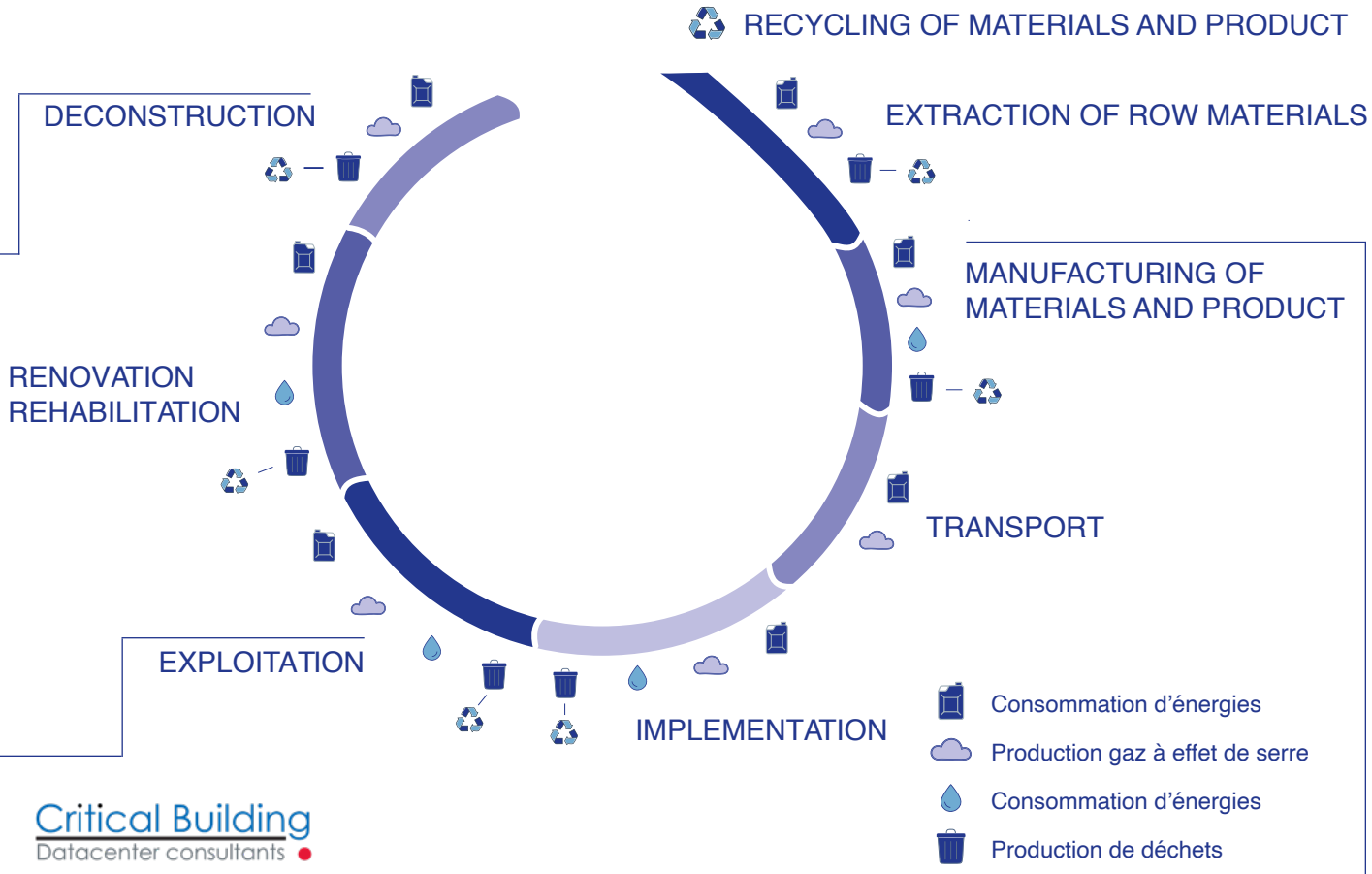
Par des évolutions technologiques sur les besoins **et systèmes de refroidissement** (voir p56)

Par **le choix du mix énergétique** : passer d'un mix énergétique conventionnel à des énergies renouvelables

L'IMPACT DES BATTERIES DES ONDULEURS

Elles représentent jusqu'à 60 % des émissions du lot électricité.
Leur fort impact est dû à leur durée de vie relativement courte et aux matériaux très émetteurs utilisés dans leur fabrication.

Il est donc essentiel de **privilégier des batteries plus respectueuses de l'environnement et optimiser leur durée de vie.**



Critical Building
Datacenter consultants

2ÈME POSTE D'IMPACT : LA CONSTRUCTION

Soit l'extraction des matières premières, la fabrication, la transformation, le transport et l'implantation sur site.
L'électricité est généralement le plus contributeur en grande partie à cause des batteries des onduleurs.
Il est donc essentiel **d'adapter le centre de données à son environnement géographique**, en tenant compte notamment de la disponibilité énergétique du réseau électrique, qui est excellente en France.

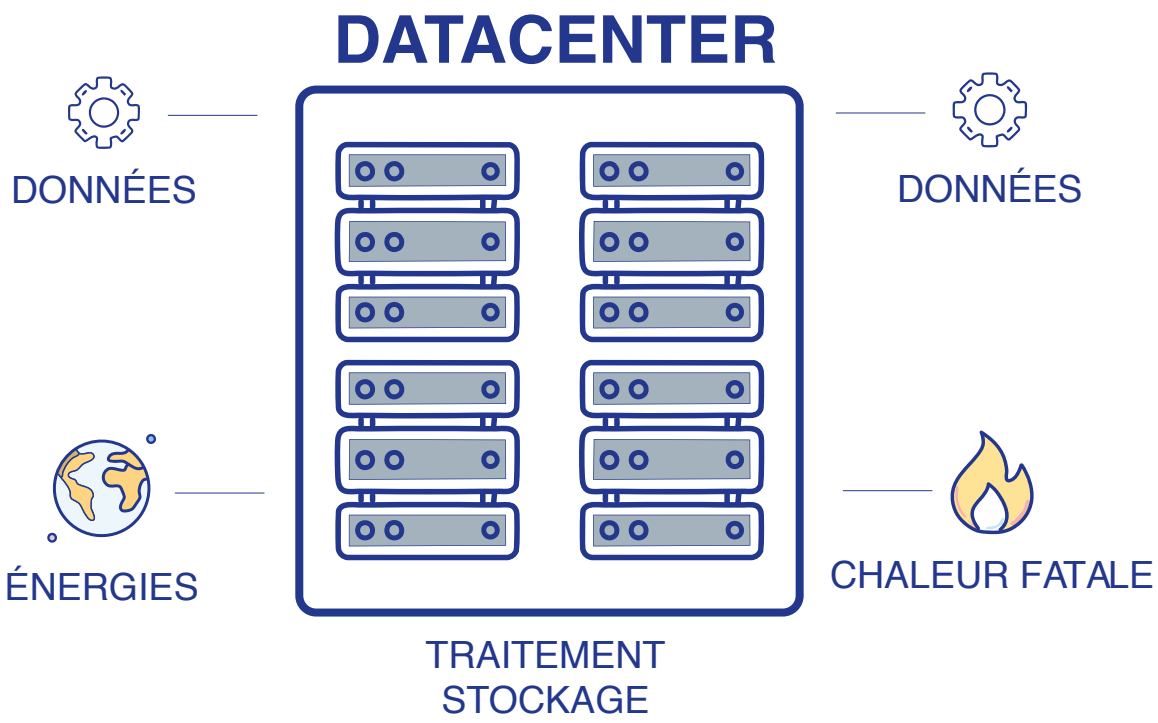
La récupération de chaleur consiste à réutiliser de l'énergie issue d'un procédé industriel (ici, l'utilisation de serveurs informatiques), qui n'est pas utilisée par le procédé en lui-même. On nomme cette énergie thermique, chaleur fatale ou chaleur de récupération.

L'objectif de la récupération de chaleur est de réduire l'impact environnemental global :

- **en réutilisant une énergie une seconde fois**
- **en évitant qu'un système produisant de la chaleur (par exemple, un réseau de chaleur) ait à utiliser d'autres sources d'énergie.**

La récupération et la valorisation de chaleur fatale offrent donc aux collectivités **une solution énergétique innovante, durable et économique qui s'intègre parfaitement dans les démarches de transition énergétique.**

Actuellement, l'État met en œuvre de grandes opérations favorisant le développement de réseaux de chaleur dans une optique d'optimisation énergétique et de décarbonation des territoires. **L'intégration urbaine des datacenters repose donc de plus en plus au volume de valorisation de la chaleur fatale dans les réseaux de chaleur.**



L'exploitation (transport, distribution) de cette chaleur demande généralement la mise en œuvre de systèmes techniques complémentaires, ce qui pose plusieurs défis.

La difficulté principale aujourd'hui est d'obtenir un retour sur investissement favorable à la réalisation du projet : certains projets nécessitent des investissements coûteux, tels que la mise en place de pompes à chaleur de grande puissance, mais également la création de nouveaux réseaux, ce qui peut mettre en péril la rentabilité du projet.

POUR QUE LA RÉCUPÉRATION DE CHALEUR SOIT INTÉRESSANTE

	LE PROJET IDÉAL...	TYPE DE CONTRAINTE
RETOUR SUR INVESTISSEMENT (RoI) Il est essentiel de trouver un équilibre entre le volume d'énergie fatale disponible et les coûts d'investissement nécessaires pour le réseau de chaleur. *NB : la valorisation de la chaleur fatale présente aussi des avantages indirects : réduction de la dépendance aux énergies fossiles, réduction de la dépendance aux énergies fossiles, stabilisation des prix de l'énergie, augmentation du taux d'énergies renouvelables et de récupération (ENR&R) dans le réseau de chaleur, et accès à des subventions.*	*Les coûts d'investissement permettent de maintenir un prix de l'énergie compétitif pour les abonnés du réseau de chaleur…*	enjeu économique **CONTRAINTE FORTE**
CAPACITÉ D'INVESTISSEMENT DES COLLECTIVITÉS Les réseaux privés étant rares, la capacité d'investissement des collectivités est primordiale.	*…la collectivité a déjà un projet de réseau avec un budget alloué…*	enjeu économique **CONTRAINTE FORTE**
EXISTENCE D'UN RÉSEAU DE CHALEUR L'existence d'un réseau de chaleur facilite la démarche, même s'il est possible d'en créer un.	*…ou un réseau de chaleur est déjà présent…*	enjeu technique critère facilitateur
PROXIMITÉ DE LA CHAUFFERIE La proximité de la chaufferie permet d'optimiser l'injection de chaleur.	*…dont la chaufferie est proche du data center…*	enjeu technique critère facilitateur
DENSITÉ THERMIQUE POTENTIELLE La densité thermique du réseau doit être suffisante pour justifier l'investissement.	*… dont la densité thermique est suffisante (>5 kWh/mL)…*	enjeu technique **CONTRAINTE FORTE**
TEMPÉRATURE DU RÉSEAU DE CHALEUR Toutes les installations nécessitent une réhausse de température (pompe à chaleur). La chaleur est généralement récupérée à 30°C alors que les réseaux fonctionnent à plus haute température : plus la température du réseau est élevée, plus les coûts seront élevés. Au-dessus de 100°C, la valorisation est impossible.	*…et dont l'eau est tempérée (rare) ou à moyenne température (65 à 70°).*	enjeu technique **CONTRAINTE FORTE**
DISTANCE DATACENTER/UTILISATEURS FINAUX Plus cette distance est courte, plus le projet est viable. Les (grands) datacenters sont souvent situés loin des zones habitées, rendant difficile le transport économique de la chaleur sur de longues distances.	*Le data center est situé en zone péri-urbaine, en contact direct d'un consommateur final (bureaux, piscine, serres agricoles, réseau de chaleur)...*	enjeu économique **CONTRAINTE FORTE**
CHARGE IT DU DATACENTER La capacité de fournir de la chaleur au réseau dépend essentiellement de la charge IT en place au sein du data center, élément difficilement maîtrisable pour un hébergeur / acteur de la colocation ou un data center neuf (sinon, des investissements supplémentaires peuvent être nécessaires pour garantir la livraison de chaleur).	*…la capacité du data center à fournir de la chaleur est relativement prévisible…*	enjeu technique critère facilitateur
TAILLE DU DATACENTER Plus les datacenters sont grands, plus il est difficile de valoriser la totalité de la chaleur fatale. (perte si concentration)	*…il s'agit d'un datacenter Edge ayant une charge IT constante de 400MW IT minimum…*	enjeu environnemental critère facilitateur
TECHNOLOGIE DE REFROIDISSEMENT La présence d'un circuit de distribution d'eau froide facilite la récupération de chaleur, alors que les systèmes free cooling/ chilling limitent la quantité de chaleur récupérable en hiver/période froide.	*…et il dispose d'un circuit de distribution d'eau froide.*	enjeu technique critère facilitateur

POUR QU'UN PROJET DE RÉCUPÉRATION DE CHALEUR RÉUSSISSE

✓	La récupération de chaleur est prise en compte dès le démarrage de la conception du projet de data center (impact bâtimentaire et refroidissement important)	enjeu technique
✓	Les besoins énergétiques locaux ont été évalués	enjeu organisationnel
✓	Le volume d'énergie récupérable sur le centre de données est évalué	enjeu technique
✓	Une étude de faisabilité technico-économique est réalisée	enjeu organisationnel enjeu économique
✓	La conception d'un système de récupération et de distribution adapté est assurée	enjeu technique
✓	Le type de raccordement est identifié	enjeu technique
✓	Une gouvernance locale implique toutes les parties prenantes *NB : veiller à inclure l'opérateur énergétique qui transporte et valorise l'énergie fatale.*	enjeu organisationnel
✓	La coordination étroite entre différents acteurs est assurée	enjeu organisationnel
✓	Une planification minutieuse du projet est mise en place	enjeu organisationnel

QUEL CADRE JURIDIQUE ?

Aujourd'hui **la réglementation est peu restrictive** : il est par exemple aisé de valoriser la chaleur du data center pour faire de l'eau chaude sanitaire au sein du bâtiment, ce qui représente seulement une infime partie de l'énergie potentiellement valorisable dégagée par le datacenter.

La valorisation de la chaleur peut se faire dans plusieurs cadres légaux : sans opérateur de réseau de chaleur (la chaleur est directement revalorisée pour un usage donné : habitations, tertiaire, piscine utilisateur industriel de chaleur basse température) mais également dans le cas de la cession ou de la revente à un réseau de chaleur urbain :

CAS SANS OPÉRATEUR DE RÉSEAU CHALEUR

Il est possible de ne pas faire payer le prix de la calorie, uniquement les coûts d'investissement sont à la charge de l'utilisateur et/ou de l'opérateur de datacenter.

La réhausse de température n'est pas nécessairement obligatoire et la chaleur peut être distribuée sur un réseau basse température, la réhausse de température étant effectuée directement par l'utilisateur (par l'utilisation d'une pompe à chaleur).

CAS AVEC OPÉRATEUR DE RÉSEAU DE CHALEUR

Si un réseau existe déjà, la plupart du temps, la chaleur doit être valorisée par une réhausse de température. Dans ce cas, un contrat de revente de chaleur n'est pas forcément nécessaire : la chaleur peut être léguée en fonction de la responsabilité ou de l'engagement de l'entité qui met à disposition cette dite chaleur.

L'opérateur de datacenter met à disposition une connexion via un échangeur pour le réseau de chaleur.

ÉVOLUTION DES OBLIGATIONS RÉGLEMENTAIRES

L'Union européenne est venue renforcer par la directive dite « Efficacité énergétique » de 2023[1] les obligations d'une large partie des datacenters en matière de chaleur fatale, pour soutenir la transition énergétique.

Les États membres doivent ainsi veiller à ce que les datacenters disposant d'une **puissance totale nominale de plus de 1 MW doivent utiliser ou récupérer la chaleur fatale. Exception** : si une analyse coûts-avantages (« ACA ») obligatoirement réalisée avant construction ou rénovation substantielle démontre que cela **n'est pas techniquement ou économiquement faisable**.

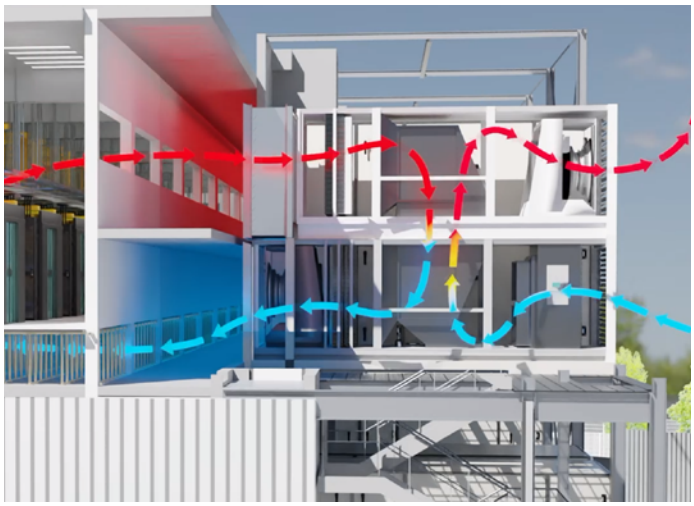
Les États membres peuvent toutefois exempter de l'ACA les datacenters **injectant la chaleur fatale dans un réseau de chauffage urbain ou l'utilisant sur place** pour le chauffage des bureaux ou la production de l'eau chaude sanitaire du bâtiment, la chaleur résiduelle étant alors exploitée.

Ce seuil d'1 MW a été repris dans le projet de loi dite « DDADUE » qui transpose la directive[2]. Par conséquent, une large majorité des datacenters de proximité sera concernée par l'obligation de l'article L. 236-2 du Code de l'énergie de valoriser la chaleur fatale qu'ils produisent, sous peine d'une amende administrative ne pouvant excéder 50 000 euros par datacenter.

Les modalités d'application de ce texte (modalités et exigences de la valorisation de la chaleurs fatale, dérogations, etc.) et de l'article L. 233-5 transposant l'obligation de réaliser une ACA (méthodologie d'analyse, autorité de contrôle[3], exceptions, etc.) ont été renvoyées aux décrets d'application. Ceux-ci devront être adoptés rapidement pour respecter la date d'entrée en vigueur de l'obligation de valorisation de la chaleur fatale, le **1er octobre 2025**.

À noter que le mécanisme des **Certificats d'Économies d'Énergie** permet de financer en partie certains investissements à ce titre.

[1] Directive UE 2023/1791 du 13 septembre 2023 relative à l'efficacité énergétique et modifiant le règlement UE 2023/955, art. 26
[2] Projet de loi portant diverses dispositions d'adaptation au droit de l'Union européenne en matière économique, financière, environnementale, énergétique, de transport, de santé et de circulation des personnes (ECOM2415026L), adopté le 3 avril 2025. La saisine du Conseil constitutionnel ne concerne pas les dispositions relatives aux obligations des centres de données.
[3] La recommandation UE 2024/2395 de la Commission européenne du 2 septembre 2024 préconise à ce titre, de manière facultative, que l'ACA soit réalisé par l'opérateur du datacenter, selon une méthodologie définie par chaque Etat membre.



C'est un **système classique de climatisation** : le fluide réfrigérant est directement utilisé comme fluide caloporteur pour évacuer les calories vers l'extérieur et les transmettre à l'intérieur des pièces à climatiser. Cela nécessite une unité interne (évaporateur, détendeur et compresseur) et une unité extérieure, reliées par un réseau de fluide frigorigène. L'unité intérieure refroidit l'air qui la traverse grâce au fluide frigorigène froid, puis renvoie le fluide réchauffé vers l'unité extérieure pour qu'il soit refroidi.

*NB : Pour une efficacité maximale et un PUE minimal, il faut **optimiser le soufflage de l'air en salle informatique**. Cependant, cette méthode de refroidissement est souvent négligée, ce qui limite les possibilités d'optimisation.*

LA DÉTENTE DIRECTE DANS L'AIR : UNE TECHNOLOGIE ANCIENNE ET TOUJOURS D'ACTUALITÉ

COMMENT REFROIDIR UN CENTRE DE DONNÉES ?

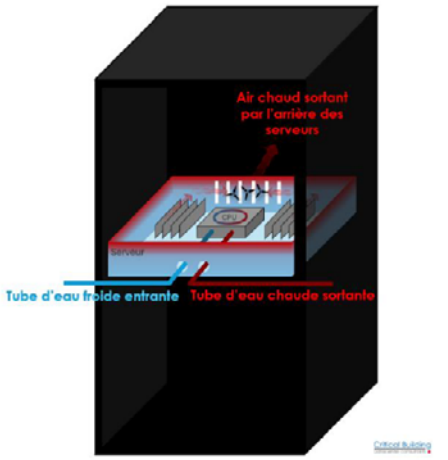
LES GROUPES FRIGORIFIQUES À CONDENSATION, UNE SOLUTION ÉCONOMIQUE INTÉRESSANTE

À AIR

L'air extérieur est utilisé pour condenser le réfrigérant dans le circuit de réfrigération. Le condenseur échange des calories entre l'air extérieur et le fluide frigorigène, tandis que l'évaporateur refroidit l'eau du circuit. L'eau glacée circule dans le bâtiment pour alimenter les unités de climatisation, qui utilisent cette eau pour refroidir l'air des salles informatiques. L'eau réchauffée est ensuite renvoyée au groupe frigorifique pour être refroidie à nouveau.

À EAU

Les calories sont évacuées **par l'eau**, soit sur un (ou un ensemble de) dry-cooler(s) situé(s) à l'extérieur du bâtiment. Ces installations reposent sur deux circuits d'eau qui circulent dans le bâtiment : un circuit primaire (eau « chaude ») et un circuit secondaire (eau « glacée »). Les groupes froids à condensation à eau sont souvent utilisés dans les bâtiments offrant la possibilité d'accueillir les groupes froids au sein de locaux fermés.

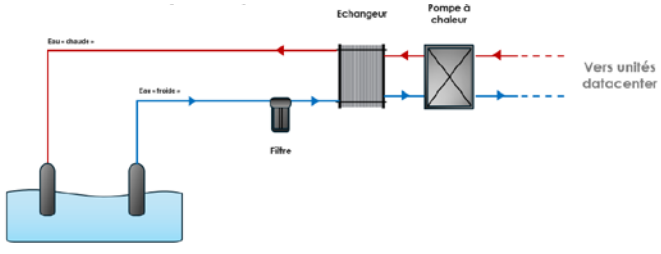


Récupère directement la chaleur émise par **les composants du serveur,** comme les processeurs, la mémoire, et les composants actifs. Cela améliore la gestion de la température, prolonge la durée de vie des serveurs, réduit leur consommation énergétique et augmente leurs performances. De plus, l'eau circulant sur ces composants peut être utilisée pour le chauffage.

LE DIRECT LIQUID COOLING, DE RETOUR AVEC L'IA

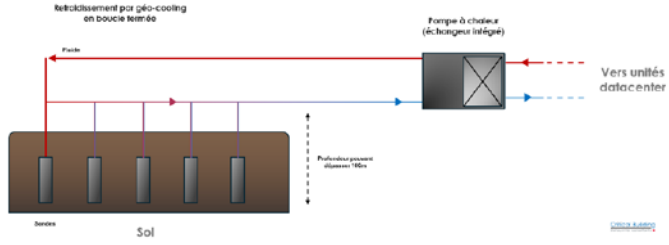
Pour plus de détails techniques et une étude approfondie du PUE de ces différentes solutions : voir *Refroidissement des Datacenters - Technologies utilisées en France, potentiel d'économies* - ADEME et CRITICAL BUILDING, 2025, dont sont issus les schémas.

LE COOLING DANS LE MILIEU ENVIRONNANT : DÉPEND DES CARACTÉRISTIQUES DU TERRITOIRE



GÉO-COOLING
PAR EAU DE NAPPE
PHRÉATIQUE OU RIVIÈRE

Utilisent l'eau de rivière / nappe. L'eau filtrée refroidit un fluide caloporteur qui absorbe la chaleur des serveurs, puis elle est rejetée après avoir été refroidie à nouveau.



GÉO-COOLING
PAR BOUCLE FERMÉE

Utilise la chaleur naturelle du sol. Un fluide caloporteur circule dans des tuyaux enterrés, transférant la chaleur des serveurs au sol.

SEA-COOLING

Utilise l'eau de mer. L'eau de mer est pompée, traverse un échangeur de chaleur, absorbe la chaleur des équipements, puis est rejetée dans la mer.

Aujourd'hui le système le plus utilisé et le plus versatile est l'utilisation de l'eau glacée / eau tempérée. Il nécessite cependant de bien gérer l'urbanisation des salles informatiques avec la gestion des couloirs chauds et froids, afin de bien segmenter les flux pour obtenir une meilleure performance énergétique.

Une variété de solutions sont envisageables, chacun présentant des avantages et des inconvénients.

	COÛT & SIMPLICITÉ D'INSTALLATION/ EXPLOITATION	EFFICACITÉ ÉNERGÉTIQUE	ADAPTABILITÉ À DES CONTRAINTES VARIÉES	RISQUES & NUISANCES
DÉTENTE DIRECTE DANS L'AIR	Coût modeste Installation simple	Peu efficace	Adapté aux DC de puissance basse (<100-200kW) Déploiement restreint (limite de distance entre unité intérieure et extérieure)	Augmente le PUE et les émissions CO2 Risque environnemental lié au fluide frigorigène (règlementation en évolution) Régulation peu précise
CONDENSATION À AIR	Coût intéressant Installation simple Faible emprise au sol	Possible d'utiliser les frigories naturelles pour améliorer l'efficacité (free cooling) Adapté aux grandes puissances frigorifiques	Efficace même si températures extérieures élevées	Risques de fuites d'eau dans la salle informatique Niveau sonore plus élevé à l'extérieur du bâtiment Risque environnemental lié au fluide frigorigène utilisé Régulation précise
CONDENSATION À EAU	Coût plus élevé que condensation à l'air Complexe à installer (pompes et réseau d'eau supplémentaires) Durée de vie prolongée	Possible d'utiliser les frigories naturelles pour améliorer l'efficacité (free chilling) Adapté aux grandes puissances frigorifiques	Bonne capacité d'évolution et de gestion de grandes puissances Moins adapté à des températures extérieures	Risques de fuites d'eau dans la salle informatique Faible bruit extérieur Risque environnemental lié au fluide frigorigène utilisé
DIRECT LIQUID COOLING	Coût important à la mise en place (nécessite des installations dédiées dans la salle informatique) Complexe à installer (raccordements et tuyaux à mettre en place) Création d'une boucle d'eau froide dédiée souvent nécessaire (température d'eau de retour peu valorisable)	Possible d'utiliser les frigories naturelles pour améliorer l'efficacité (free cooling)	Bonne capacité d'évolution et de gestion de grandes puissances Efficace même si températures extérieures élevées	Risques de fuites d'eau dans la salle informatique Niveau sonore plus élevé à l'extérieur du bâtiment Régulation précise

	COÛT & SIMPLICITÉ D'INSTALLATION/ EXPLOITATION	EFFICACITÉ ÉNERGÉTIQUE	ADAPTABILITÉ À DES CONTRAINTES VARIÉES	RISQUES & NUISANCES
GEO-COOLING PAR NAPPE PHRÉATIQUE OU RIVIÈRE	Coût d'exploitation réduit, Coût d'installation plus élevé Installations spécifiques pour traitement de l'eau nécessaires	Réduit la consommation d'énergie par rapport aux systèmes de refroidissement par air	Nécessite une source d'eau proche avec débit et température adaptés	Moins de bruit (absence de ventilateurs et climatiseurs) Impact environnemental (rejet d'eau réchauffée), normes strictes
GEO-COOLING PAR BOUCLE FERMÉE	Coût d'exploitation réduit, Coût d'installation plus élevé Nécessite de grandes surfaces pour l'enfouissement des réseaux Fonctionnement stable et fiable (source froide continue avec peu de variations)	Efficacité énergétique accrue (énergie renouvelable)	Convient aux data centers peu puissants avec de grandes surfaces disponibles	Peu de bruit
SEA COOLING	Équipements coûteux (titane) Economies long terme sur la consommation électrique et la maintenance (peu d'éléments à maintenir) Maintenance régulière et complexe	Réduit la consommation d'électricité		Eau de mer corrosive pour les équipements Impact environnemental (rejet d'eau réchauffée)

Comme toute construction, l'implantation d'un datacenter est conditionnée par **l'obtention d'un permis de construire**. Le plan local d'urbanisme (« PLU ») doit donc permettre l'implantation d'entrepôts, qui est la qualification consacrée pour les centres de données[1], voire de bureaux en complément des salles techniques.

Le projet de loi de simplification de la vie des entreprises qui devrait être adopté d'ici fin 2025 prévoit, dans sa version actuelle, des dispositions modifiant le Code de l'urbanisme pour faciliter l'implantation de centres de données de grande puissance, qui pourraient être qualifiés de projets d'intérêt national majeur (PINM) conférant au préfet la compétence de délivrer les permis de construire de telles installations.

En Ile-de-France, le Code de l'urbanisme confère déjà des prérogatives particulières au préfet de région, le porteur d'un projet d'une surface de plancher supérieure à 5 000 m2 devant obtenir un agrément d'immobilier d'entreprise pour la construction, l'extension de locaux ou leur réhabilitation[2], avant toute demande de permis de construire.
Dans ce cadre, le dossier devra démontrer que le projet s'inscrit dans les **objectifs de sobriété foncière et de sobriété énergétique** : implantation en site déjà urbanisé, performances énergétiques ambitieuses et dispositif de valorisation de la chaleur fatale[3].

Sur le volet environnemental, les datacenters constituent des installations classées pour la protection de l'environnement (« ICPE »), du fait des multiples équipements qu'ils mobilisent (postes électriques à haute tension, groupes électrogènes de secours, production de froid, batteries, cuves de fioul, etc.).
En fonction de l'ampleur du projet, celui-ci est susceptible de nécessiter une instruction plus ou moins complexe, voire une étude environnementale complète, selon la nomenclature des installations envisagées[4] :

- **Le régime d'autorisation** (A) nécessite notamment la fourniture préalable d'une étude des dangers industriels, une étude d'impact ou une étude d'incidence environnementale et une synthèse des propositions de prescriptions techniques envisagées pour respecter les préconisations environnementales en particulier. L'instruction du dossier nécessite l'avis des collectivités concernées et de plusieurs organismes, dont la mission régionale d'autorité environnementale (« MRAe »), puis une consultation du public de 3 mois ;

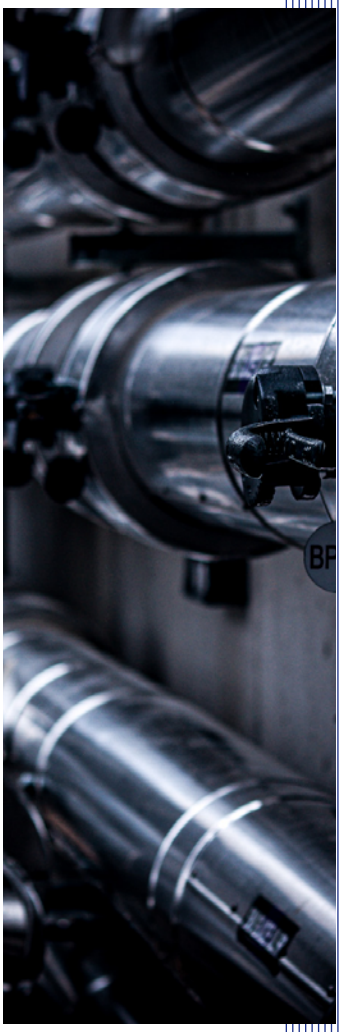
- **Le régime d'enregistrement** (E) nécessite la transmission au préfet d'un dossier détaillé comprenant en outre une description des incidences notables du projet jusqu'à sa démolition, des propositions de mesures permettant de réduire les effets négatifs sur l'environnement ou la santé humaine, des éléments permettant d'apprécier la compatibilité du centre avec les différents schémas directeurs et plans de prévention, et les mesures prises pour limiter la consommation d'énergie pour les installations de plus de 20 MW. Selon les cas, une étude environnementale peut toutefois être imposée ;

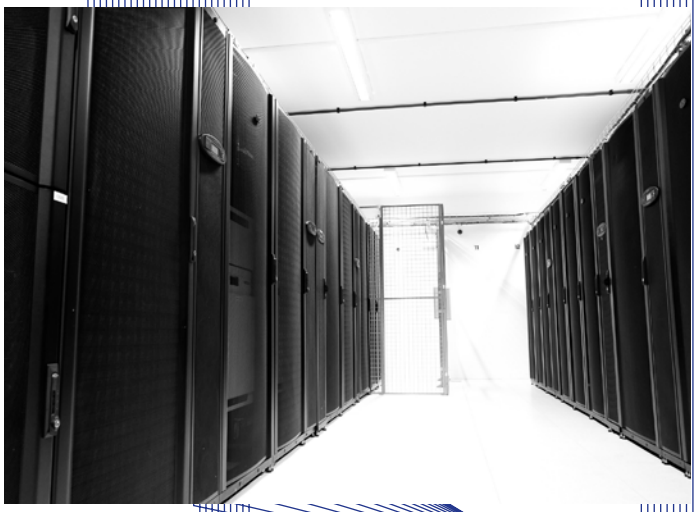
- **Le régime déclaratif** (D) est réservé aux installations les plus simples, présentant le moins de risques pour l'environnement et les humains.

Le porteur de projet doit donc anticiper les délais liés à ce statut d'ICPE.

[1] Art. R151-28 du Code de l'urbanisme et Arrêté du 22 mars 2023 modifiant la définition des sous-destinations des constructions pouvant être réglementées dans les plans locaux d'urbanisme ou les documents en tenant lieu
[2] Art. R510-1 et suivants du Code de l'urbanisme
[3] Fiche repère relative aux instructions des demandes d'agrément relatives aux centres de données, mars 2022, de la DRIEAT Ile-de-France
[4] Art. L512-1 et suivants du Code de l'environnement


GROLLEAU
GROLLEAU





le GUIDE du DATA CENTER de PROXIMITÉ

4

CADRE LÉGAL & CONTRACTUEL

Généralités pour tous les acteurs

Collectivités : se lancer dans un projet datacenter

CADRE LÉGAL & CONTRACTUEL

Face à la montée en puissance des enjeux de souveraineté numérique, de résilience des territoires, de proximité des infrastructures numériques, les collectivités territoriales et les entreprises s'interrogent sur les solutions d'hébergement de leurs données, en propre ou par des tiers. Ces projets peuvent répondre à des besoins internes, aux enjeux réglementaires croissants (NIS 2, RGPD, etc.) mais également, pour les organisations, à des logiques d'aménagement numérique du territoire, de soutien aux acteurs économiques locaux ou de mutualisation.

La réussite d'un projet de datacenter de proximité repose avant tout sur une bonne anticipation des contraintes juridiques et une maîtrise des outils contractuels disponibles. Pour les collectivités territoriales comme pour les entreprises, il s'agit de choisir les bons montages, de sécuriser les relations avec les partenaires techniques ou exploitants, et de respecter les règles de la commande publique. Adapter sa stratégie contractuelle à chaque scénario – location, construction, mutualisation, appel à projet – est essentiel pour éviter les blocages juridiques et garantir la viabilité du projet dans la durée.

Dans cette section, nous proposons de décrypter les principales obligations juridiques applicables aux projets d'hébergement numérique des collectivités et entreprises locales, avant d'envisager une approche opérationnelle par scénario : pour chaque modèle, seront analysées les implications juridiques et les clauses clés à intégrer.

LES ORGANISATIONS FACE AUX ENJEUX RÉGLEMENTAIRE DE L'HÉBERGEMENT NUMÉRIQUE

Les projets d'hébergement numérique, qu'ils concernent la création d'un datacenter en propre ou le recours à des services externalisés, s'inscrivent dans un cadre réglementaire en constante évolution. Les collectivités territoriales et les entreprises rencontrent des contraintes réglementaires similaires :

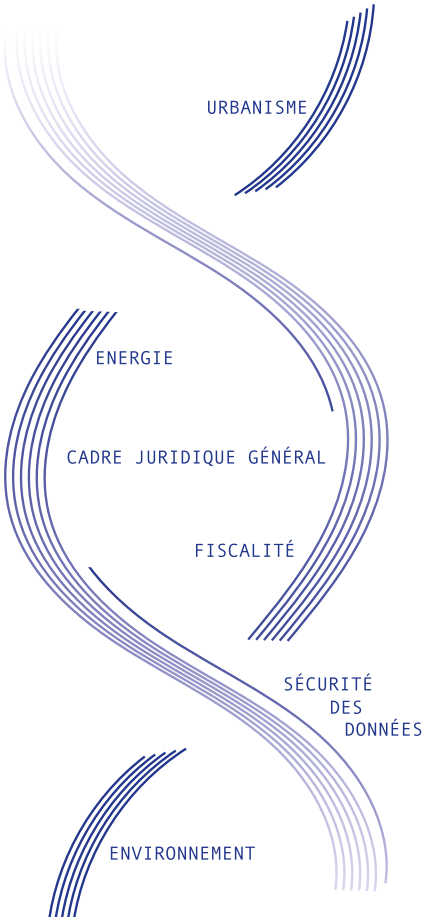
- ☐ **Des exigences en matière de protection des données et répondre à des critères de sécurité** de plus en plus précis. Prendre en compte des obligations croissantes en matière de cybersécurité, de conformité au RGPD
- ☐ Des normes européennes plus récentes, comme la Directive NIS 2, publiée le 27 décembre 2022, qui vise à renforcer le niveau de **cybersécurité** des opérateurs publics et privés
  NB: Certaines collectivités ou leurs prestataires pourraient être directement concernés par ces nouvelles obligations
- ☐ **Des exigences environnementales et de performance énergétique** (consommation énergétique, empreinte carbone, chaleur fatale).
  NB : Ces aspects peuvent influencer le choix entre hébergement local, cloud privé, ou cloud public certifié..

Point d'écart : Dans le cas des collectivités, les projets doivent principalement respecter les règles de la commande publique et intégrer les exigences précédemment énoncées. À l'inverse, les entreprises sont soumises à ces règles, sans en être à l'origine.

LES PRINCIPALES RÉGLEMENTATIONS

Les projets de datacenters, qu'ils soient portés par des acteurs publics ou privés, sont encadrés par un ensemble d'obligations issues de différents codes et textes législatifs.

Les exigences appartiennent à plusieurs domaines :



URBANISME / IMPLANTATION : Code de l'urbanisme (R.510-1 à R.510-6, L.421-1)

ÉVALUATION ENVIRONNEMENTALE : Code de l'environnement (étude d'impact, cas par cas)

ÉNERGIE / SOBRIÉTÉ : Code du CCH (L.174-1, R.174-22 à R.185-2), décret tertiaire 2019/771

FISCALITÉ / TICFE : Loi finances 2021 (Loi n° 2020-1721, art. 167), loi REEN 2021

NORMES DE SÉCURITÉ : RGPD, Loi Informatique et Libertés, ISO/IEC, EN, NIS 2, DORA

INITIATIVES LÉGISLATIVES : Projet loi simplification 2024, proposition 2025

LA DIVERSITÉ DES SCÉNARIOS POSSIBLES

Les collectivités ont une diversité de scénarios possibles pour déployer un projet datacenter, que ce soit :
- pour leurs propres besoins ou
- pour mettre en place une solution d'hébergement dite «mutualisée».

En revanche, il apparaît que dans la majorité des cas, les collectivités qui se lancent le font en priorité pour leur propres besoins et en profitent pour mettre à disposition ces infrastructures au service d'autres acteurs, à minima d'autres collectivités.

Dans ce chapitre, est examinée la mise en œuvre d'infrastructures mutualisées
Par des collectivités
Pour des collectivités et autres acteurs du territoire

SCÉNARIO 1 HÉBERGEMENT SEC	SCÉNARIO 2 ACHAT D'UN DATACENTER EXISTANT	SCÉNARIO 3 CONSTRUCTION D'UN SITE PUBLIC	SCÉNARIO 4 AAP

Des retours d'expérience sont présentés dans la première partie du guide

Par abus de langage, l'hébergement sec est intégré dans ce chapitre consacré au "projet datacenter" dans la mesure où ce projet n'est pas un simple projet d'hébergement. La personne publique va mettre à disposition cette infrastructure pour d'autres acteurs.

Ce qui est commun à l'ensemble des scénarios :
- La personne publique est propriétaire des ressources informatiques, les lois extraterritoriales ne peuvent pas s'appliquer et les coûts sont optimisés ;
- La personne publique a le choix entre internaliser ou externaliser l'exploitation-maintenance de ces ressources.

Ce qui change :
- Le niveau d'investissement initial ;
- Les coûts de fonctionnement associés ;
- Les modalités contractuelles associées.

Ce chapitre présente des étapes fondamentales à prendre en compte dans la mise en oeuvre de son projet

- ☐ **Définir un cadre d'intervention des collectivités territoriales**
- ☐ **Respecter les dispositions du code de la commande publique**
- ☐ **Définir le périmètre du projet** pour définir le cadre contractuel
- ☐ **Définir le cadre contractuel** des différents scénarios

DÉFINIR UN CADRE D'INTERVENTION DES COLLECTIVITÉS TERRITORIALES

La première contrainte est **l'absence de compétence « datacenter »** *stricto sensu* telle qu'elle peut exister par exemple pour la mise en place des RIP[8]. Faute de cette compétence dédiée, l'intervention des collectivités territoriales n'est pas toujours perçue positivement par les entreprises privées intervenant sur le secteur (elle n'est d'ailleurs pas toujours possible).

LA NÉCESSITÉ D'UN INTÉRÊT PUBLIC LOCAL

L'intervention des collectivités territoriales peut se justifier **en cas de carence de l'initiative privée** mais également si **un intérêt public local le justifie.** Dans la mesure où l'offre privée existante sur un territoire n'apparaît pas être pleinement satisfaisante, la collectivité territoriale peut prendre l'initiative de son projet, seule ou avec d'autres acteurs publics locaux, et même de s'associer avec le secteur privé.

Les personnes publiques sont chargées d'assurer les activités nécessaires à la réalisation des missions de service public dont elles sont investies et bénéficient à cette fin de prérogatives de puissance publique. Par ailleurs, si elles entendent, indépendamment de ces missions, prendre en charge une activité économique, elles ne peuvent légalement le faire que dans le respect tant de la liberté du commerce et de l'industrie que du droit de la concurrence.

Le portage de projets de datacenters locaux répond également aux nouveaux enjeux de mise à disposition et de protection des données publiques locales auxquels sont confrontées les collectivités territoriales. **Quelques collectivités territoriales ont fait de l'obligation de publication de leurs données dites « essentielles » dans le cadre des réglementations sur l' « Open data » le motif du recours à une infrastructure locale d'hébergement** afin de préserver la souveraineté sur ces données publiques et de remplir les engagements nouveaux de mise à disposition et de sécurité. Le recours à ce motif devrait prendre de l'ampleur dans les prochaines années au regard des obligations renforcées de cybersécurité qui s'imposeront à certaines collectivités suite à la transposition de la Directive NIS 2[9].

La création d'un datacenter ne relève pas directement de la compétence des collectivités territoriales, quel que soit l'échelon mobilisé. Elle n'est pas précisément identifiée comme telle dans le code général des collectivités territoriales (CGCT). Toutefois, l'intervention d'une collectivité peut se trouver justifiée en cas de carence de l'initiative privée et compte d'un intérêt public local particulier..

[8] L'article L. 1425-1 du code général des collectivités territoriales ne visant que les réseaux de communications électroniques
[9] Le projet de loi de transposition étant en cours d'examen à l'heure de la mise sous presse du présent guide

RESPECTER LES DISPOSITIONS DU CODE DE LA COMMANDE PUBLIQUE

DEFINITION DU BESOIN — PROCÉDURES D'APPEL D'OFFRES — ATTRIBUTION — EXÉCUTION — SUIVI

Une fois la question de l'intervention validée, les collectivités territoriales souhaitant mener un projet de datacenter sont soumises, comme dans tous les secteurs dans lesquels elles interviennent, **au respect des règles de la commande publique**, dorénavant codifiées dans le code de la commande publique.

Pour construire et/ou exploiter un datacenter local, les collectivités doivent donc lancer des procédures d'appel d'offres et mise en concurrence, plus ou moins longues selon le schéma contractuel retenu, et les renouveler de manière périodique. Cela représente une contrainte et un coût indéniables, qui doivent être anticipés avant de se lancer.

Il pourrait être opportun pour les collectivités qui souhaitent lancer des consultations publiques, **d'intégrer la problématique de la cybersécurité dans les appels d'offres**. Les collectivités territoriales peuvent par exemple décider d'intégrer le cahier des clauses simplifiées de cybersécurité (CSC) dans le périmètre des documents contractuels.

Il est également possible de privilégier le recours aux services de prestataires de services de confiance ou des produits de sécurité bénéficiant d'une certification/qualification, notamment la qualification SecNumCloud.

LE PRINCIPE DE REMISE EN CONCURRENCE PÉRIODIQUE

La collectivité y sera davantage confrontée si elle fait le choix de montages simples (marchés de travaux, de fournitures ou de services) qui sont généralement remis en concurrence tous les quatre ans, à la différence des montages dits globaux (concession ou marché global de performance) qui peuvent être plus longs (sous réserve que la durée longue soit justifiée par un niveau d'investissement élevé).

DÉFINIR LE PÉRIMÈTRE DU PROJET POUR DÉFINIR LE CADRE CONTRACTUEL

En amont de tout projet, un travail de fond d'étude des besoins des acteurs publics est à mener pour assurer un modèle économique pérenne au porteur de projet. Cette mission s'oriente à la fois vers le secteur public et vers l'écosystème privé local. La détention d'une certification HDS (hébergement de données de santé) en tant qu'établissement et non sur la gestion du cycle de la donnée, semble être un attribut supplémentaire convaincant pour attirer un certain nombre d'acteurs, notamment publics. Il permet en effet d'une part, d'attirer le secteur de la santé, et d'autre part, il est gage de confiance aux yeux des parties prenantes du projet par rapport à leur souveraineté sur les données.

Du point de vue des acteurs privés, la bonne connaissance du potentiel de marché est importante. En effet, elle permet de comprendre l'état du marché sur le territoire afin d'estimer si un niveau de service supérieur dans le cadre de l'appel à projet peut être exigé, et, le cas échéant, sur quels fondements économiques. Si le potentiel futur projet peut permettre de répondre aux besoins du secteur privé en embarquant des acteurs publics, l'appel à projet a lieu d'être lancé.

Parmi les exigences de futurs utilisateurs d'un site d'hébergement, le débit de connectivité en est une probablement déterminante. Par conséquent, la collectivité a aussi fort intérêt à se rapprocher du Réseau d'initiative Publique RIP local (s'il en est un), pour élaborer une offre de service associée au projet d'hébergement. Si le projet n'est pas conjointement mené avec l'acteur public local en charge du RIP, l'investir comme partie prenante principale paraît important pour la réussite du projet. Il entretient en effet une relation privilégiée avec les entreprises locales à travers ses offres professionnelles, ce qui peut en faire un acteur charnière d'une telle démarche. Finalement, il peut s'avérer stratégique que le tandem opérateur de réseau fixe/opérateur d'hébergement soit étroitement lié aux yeux des TPE-PME notamment.

CADRE CONTRACTUEL DES DIFFÉRENTS SCÉNARIOS

1 SCÉNARIO

HÉBERGEMENT SEC

Dans ce scénario, l'organisation a recours à un acteur privé ou public qui propose à la location des espaces de housing, c'est-à-dire **des baies informatiques pré-câblées dans lesquelles elle viendra disposer ses propres ressources informatiques.**
Dans ce mode d'exploitation, **la gestion de l'environnement technique est de la responsabilité** du prestataire qui doit s'engager sur des niveaux de services compatibles avec les exigences et besoins des usagers.

APPROCHE CONTRACTUELLE

La location de baies s'inscrit dans le cadre de **contrats de location et de services** définissant les engagements techniques, les niveaux de service (SLA), les conditions financières de la location et des services, la durée, les obligations et responsabilités de chaque partie, ainsi que les conditions d'accès et de sécurité.

Elle permet aux collectivités d'externaliser tout ou partie de leur environnement informatique. Le contrat permet la mise à disposition d'un espace physique au sein d'un datacenter sécurisé, pour l'installation des équipements informatiques (serveurs, pare-feu, routeurs, etc.).

Le client reste propriétaire de ses équipements et il en contrôle l'accès, tandis que le prestataire garantit la disponibilité et la gestion des infrastructures essentielles : alimentation électrique en redondance, maintenance du datacenter, refroidissement, sécurité physique et logique, connectivité réseau.

Lorsque le prestataire est certifié (par exemple ISO 27001, HDS, …), **ses engagements de conformité sont retranscrits dans le contrat**. Cela permet au client de s'appuyer sur ces garanties pour répondre à ses propres exigences réglementaires ou sectorielles. **Par principe, la protection des données est également au cœur du processus contractuel** et peut faire l'objet d'une **clause de changement de contrôle** pour garantir les engagements contractuels en matière de souveraineté. Ces éléments contractuels jouent un rôle dans le choix du prestataire, car ils permettent au client de **démontrer contractuellement** le respect de certains standards ou obligations légales.

Dans cet environnement **sensible et sécurisé, la contractualisation d'assurances** est un point important. En plus des assurances professionnelles usuelles (responsabilité civile, dommages aux biens, perte d'exploitation, etc.), **le marché de la cyberassurance** s'est fortement développé ces dernières années. Il répond à des risques spécifiques liés à la cybersécurité, aux atteintes aux données, ou aux interruptions de service, et **peut être exigé ou recommandé** dans le cadre contractuel entre le client et le prestataire.

Une autre approche, utilisée dans **le datacenter public de Val d'Oise Numérique, est celle d'une location de longue durée, sur le modèle de l'IRU propre aux réseaux fixes[10],** par exemple sur la base d'un bail emphytéotique. Pour une collectivité, cette approche qui consiste à devenir quasi-propriétaire pendant une durée déterminée, revient à investir sur un horizon de 15 ou 20 ans dans un espace au sein d'un datacenter, énergie, climatisation et connectivité comprise. Cela permet d'enregistrer cette dépense en tant qu'investissement du point de vue comptable, et cela garantit, pour l'acteur privé propriétaire du site, un revenu à long terme.

[10] Indefeasible right of use, ou droit d'usage indéfectible

2 SCÉNARIO
ACHAT D'UN DATACENTER EXISTANT

Dans ce scénario, **la collectivité achète par opportunité un datacenter présent sur son territoire.**

APPROCHE CONTRACTUELLE

Le dispositif est rare, est conditionné à des opportunités bien particulières sur le territoire, il est difficile à ce jour de recenser les modalités de mise en œuvre.
Cette section sera approfondie lors d'une prochaine édition.

3 SCÉNARIO
CONSTRUCTION D'UN SITE PUBLIC

Dans ce scénario, **la collectivité investit dans la construction d'un datacenter dans son intégralité (ou via la transformation d'un bâtiment préexistant dans une zone d'activité par exemple), dans une démarche de mutualisation de l'infrastructure entre acteurs du territoire.**

APPROCHE CONTRACTUELLE

En plus du génie civil, du système de climatisation-refroidissement, des infrastructures électriques et télécoms, la collectivité **acquiert les ressources informatiques** auprès des fournisseurs et exploite l'infrastructure informatique pour délivrer les applications aux usagers. Néanmoins, bien que l'exploitation et la maintenance soient de la responsabilité de la collectivité, **les prestations peuvent aussi être confiées à un acteur privé**, au travers d'un **marché d'exploitation-maintenance** par exemple.

Si la personne publique décide de **d'externaliser l'exploitation-maintenance, elle peut faire le choix de passer des marchés séparés pour la construction de l'installation d'une part, pour son exploitation d'autre part, pour sa maintenance** :

La personne publique peut sinon opter pour un **marché global** comprenant des prestations de travaux, d'installation, d'exploitation et/ou de maintenance des équipements. Cette seconde hypothèse peut s'avérer préférable dans les cas où il est démontré que la scission du phasage serait de nature à rendre techniquement difficile l'exécution des prestations. Plusieurs montages contractuels sont possibles :

CLASSIQUES
Comme le marché de travaux ou de fournitures pour la construction et l'installation des datacenters ou marchés de services pour l'exploitation du datacenter aux marchés globaux plus récents qui peuvent avoir l'avantage de confier à un seul et même groupement la conception, la construction et éventuellement l'exploitation de l'installation.

GLOBAUX
Comme le marché de conception-réalisation ou encore le marché global de performance semblent pertinents dans la mesure où ils font appel à des solutions techniques et/ou innovantes liées à des objectifs de performance mesurables, pleinement adaptées à des installations d'hébergement.

Telle est la raison pour laquelle de nombreuses collectivités se positionnent aujourd'hui en faveur de **montages challengeant les candidats sur des engagements tangibles d'efficacité énergétique ou d'incidence écologique**. Les montages précités ne sont pas les seuls envisageables et il est difficile ici de les présenter de façon exhaustive tant le contexte, les enjeux et les objectifs poursuivis par un projet de datacenter local peuvent varier de manière importante d'un territoire à l'autre. Dès lors, **une étude de faisabilité technique, juridique, économique et financière** est toujours préférable avant de se lancer dans un projet de datacenter local.

En effet, l'un des enjeux forts souvent avancé par les collectivités territoriales pour porter un projet de datacenter local est de pouvoir proposer **une installation alliant protection des données publiques, disponibilité, haute technicité et engagements en faveur de l'environnement.**

Les montages précités ne sont pas les seuls envisageables tant le contexte, les enjeux et les objectifs poursuivis par les collectivités peuvent différer d'un territoire à l'autre. Dès lors, une étude de faisabilité technique, juridique, économique et financière est toujours préférable avant de se lancer dans un projet de datacenter local.

DATACENTER OUVERT AUX ACTEURS PUBLICS

La collectivité devra définir **les modalités de gouvernance et d'ouverture du datacenter aux acteurs publics**, y compris en assurant à ces derniers un niveau de service en adéquation avec les standards du marché.
Les modalités d'accès à ce nouveau service peuvent être par exemple déterminés en fonction des investissements supportés, des besoins avérés et/ou projetés.

De nombreuses collectivités menant actuellement des réflexions sur le lancement de projets de datacenters locaux, réfléchissent à créer des structures de portage du type **des sociétés publiques locales** (permettant de réunir plusieurs collectivités territoriales et groupements pour l'exercice en commun de compétences spécifiques) ou encore des **sociétés d'économie mixte locale** (alliant personnes publiques et au moins une personne privée pour réaliser des opérations en commun).

DATACENTER OUVERT AUX ACTEURS PUBLICS ET ACTEURS PRIVÉS

La collectivité peut choisir de **construire ab initio un espace destiné aux acteurs privés afin de développer une offre de services d'hébergement** qui s'inscrirait dans une stratégie territoriale plus large.
Dans la perspective de l'augmentation de ses besoins à moyen ou long terme, **la collectivité peut confier l'exploitation des espaces non utilisés à date à un exploitant privé pour une période finie**, renouvelable.

EXEMPLES DE CONTRAT

À titre d'exemple, la collectivité peut avoir recours à **un modèle de concession de services**. L'acteur privé, sous statut de prestataire en charge de l'exploitation technique et commerciale du site pourrait proposer à des acteurs privés (des PME typiquement) un catalogue de services d'hébergement sous la bannière de la collectivité. La remise de l'ouvrage en exploitation à un tiers se ferait contre des engagements contractuels (en termes de qualité de services), et une redevance pour la valorisation de l'infrastructure. Cette redevance pourrait s'établir selon différents critères, par exemple des considérations de consommation énergétique prévisionnelle, de volume de flux de données, de disponibilités, de niveau de service par rapport à la criticité des applications hébergées…

Une autre approche par exemple pourrait être **une location d'espace à un opérateur commercial neutre**. Assurant l'exploitation technique du site, la collectivité pourrait louer de l'espace IT à l'opérateur qui aurait toute la latitude de commercialiser ses propres offres, en son nom, sur des infrastructures informatiques distinctes de celles la collectivité. Différentes modalités sont possibles : l'opérateur loue-t-il un service « power and shell », mettant à disposition énergie, adduction en fibre, monitoring énergétique et baies vides, dans une logique de housing, ou bien loue-t-il des serveurs prêts à l'emploi, avec des offres d'hébergement mutualisé ou dédié. Enfin, il est probable que l'acteur privé exige de disposer d'un espace privatif au sein du datacenter. C'est donc un aspect de design du site à prévoir dès sa conception.

4 SCÉNARIO
AAP POUR LA CONSTRUCTION D'UN DATACENTER

À côté de ces trois scénarios, **une collectivité peut également décider de lancer un appel à projet**. Si une collectivité constate une carence de l'offre d'hébergement sur son périmètre, autant pour les services publics que pour le tissu économique local, l'appel à projet pour la réalisation d'un site d'hébergement sur son territoire est une approche à considérer qui a fait ses preuves. La rentabilité de l'acteur privé lauréat de l'appel à projet est l'enjeu sous-jacent à cette démarche.

PRINCIPALES MODALITÉS

Ce scénario demande à nouveau de bien anticiper le potentiel marché et les attentes techniques, aussi bien du côté des acteurs publics, du secteur de la santé notamment, que du secteur privé.

À titre de garantie pour le futur porteur de projet, il peut être bienvenu qu'une commande publique s'associe dès son lancement pour assurer une rentabilité minimale du modèle économique.

En effet, assuré d'une première commande, le prestataire peut se lancer rapidement dans la réalisation de la première tranche du projet le temps de gagner effectivement les commandes auprès des autres acteurs, notamment privés, sensibilisés par le travail de promotion en amont par la collectivité.

En somme, après une étude initiale des potentiels de marché et un travail de promotion pour agréger la demande d'un projet d'hébergement local, la collectivité peut lancer un appel à projet dont elle deviendra elle-même bénéficiaire par la suite. D'autres conditions clés se dégagent et sont à affiner selon les réalités de chaque territoire, telles que l'étroite collaboration avec l'opérateur de RIP local par exemple.

EXPLOITATION-MAINTENANCE EXTERNALISÉE

Dans le cas où la collectivité est propriétaire des infrastructures numériques et en externalise l'exploitation-maintenance.

Dans ce cas, il faut alors anticiper les problématiques de contrôle d'accès. En effet, par sécurité pour les équipements, et pour les données et les applications hébergées, la collectivité doit s'assurer qu'elles ne seront pas accessibles à des personnes non autorisées. Bien que tous les sites de ce type disposent d'un dispositif de contrôle d'accès centralisé, la multiplicité des acteurs autorisés à accéder aux infrastructures contraindra la collectivité à exiger l'hébergement de ses équipements dans des espaces privatifs, accessibles selon des règles de sécurité complémentaires.

PRINCIPALES CLAUSES À PRENDRE EN COMPTE

- ☐ **CONTRÔLE D'ACCÈS** : Définissent les modalités d'accès au datacenter et aux espaces privatifs : identification obligatoire (badges, biométrie), restrictions sur les personnes autorisées, horaires d'accès, et validation des droits d'entrée.
- ☐ **RESPONSABILITÉ** : Précisent les responsabilités respectives du prestataire et du client, notamment en cas d'accès non autorisé ou de manquement aux règles et politiques de sécurité.
- ☐ **CHANGEMENT DE CONTRÔLE** : Garantissent le respect des engagements contractuels de souveraineté, en cas de changement d'actionnaire du fournisseur.
- ☐ **AUDIT ET SURVEILLANCE** : Autorisent la collectivité à effectuer des audits ou contrôles réguliers pour vérifier le respect des conditions d'accès et de sécurité.
- ☐ **ESPACE PRIVATIF** : Garantissent l'hébergement des équipements de la collectivité dans des zones dédiées, distinctes des espaces mutualisés, avec des règles d'accès spécifiques renforcées.
- ☐ **TIERS ET SOUS-TRAITANTS** : Encadrent les conditions d'accès des sous-traitants du prestataire, qui doivent être contractuellement liés, informés des obligations applicables, et strictement soumis aux mêmes exigences de sécurité.
- ☐ **SÉCURITÉ PHYSIQUE ET ORGANISATIONNELLE** : Assurent le respect des processus internes du prestataire en matière de sécurité physique et du système d'information, conformément aux engagements contractuels.
- ☐ **RÉVERSIBILITÉ ET RÉSILIATION** : Prévoient des modalités de sortie encadrées en cas de fin de contrat ou de manquement, incluant la restitution sécurisée des équipements à la collectivité et l'absence d'impact sur leur intégrité. Ces modalités doivent être formalisées, au moins en annexe du contrat.

SCÉNARIO

CONSTRUCTION D'UN DATACENTER ET EXPLOITATION-MAINTENANCE EXTERNALISÉE

Entretien avec Monsieur Nicolas HECQ, Directeur de Sarthe Numérique

Depuis 2004, Sarthe Numérique, un syndicat mixte ouvert, assure l'aménagement numérique du département de la Sarthe et, depuis 2018, au travers d'une Délégation de Service Public portée par Sartel du groupe AXIONE. Le SMO regroupe le Conseil Départemental de la Sarthe, la Communauté Urbaine Le Mans Métropole et 15 Communautés de communes.

Sarthe Numérique souhaitait **renforcer la résilience de son cœur de réseau fibre historique et, parce que les bâtiments sont similaires à ceux d'un datacenter et que le contrat de délégation de service public le prévoyait**, il a été décidé d'en profiter pour créer un datacenter au service des collectivités et acteurs publics de la Sarthe. C'est ainsi que Sartera, le premier centre public d'hébergement de proximité en France, est né.

Avec ce montage affermo-concessif, Sartel capte les fruits liés à l'exploitation du datacenter et reverse à Sarthe Numérique une redevance d'affermage en contrepartie du cofinancement public. Les acteurs publics désireux de souscrire à l'offre d'hébergement le font auprès du délégataire via une **commande publique avec la possibilité d'acheter sous forme d'IRU** (Indivisible Right of Use ou Droit Irrévocable d'Usage) une baie ou une demi-baie et de n'avoir que l'énergie en récurrent.

Le marché adressable comprend non seulement les collectivités mais également des bailleurs sociaux, le SDIS 72 ou encore le groupe hospitalier du Mans. Il est très fréquent que les acteurs publics de plus petite taille ne disposant pas de compétences SI particulières, soient intéressés par une solution d'hébergement « clés en main ». Le catalogue des services de Sartera prend donc en compte l'obligation, rappelée en 2023 dans un audit réalisé par la Chambre Régionale des Comptes – Pays de la Loire, de **n'introduire aucune distorsion concurrentielle sur le marché privé de l'hébergement.**

La démarche intéresse particulièrement les DSI des acteurs publics. A titre d'exemple, la très haute performance énergétique du datacenter recherchée dès sa conception amène le département à s'interroger à en faire son site principal en vue de diminuer son propre impact. La métropole du Mans ou les communautés de communes mènent une réflexion similaire pour utiliser ce centre d'hébergement en remplacement de salles moins performantes.

ANNEXES

LEXIQUE STRATÉGIQUE DE LA SOUVERAINETÉ NUMÉRIQUE

DATE	TEXTE / AUTORITÉS / NOTION	NOTIONS
6 janvier 1978	CNIL	La loi de 1978 (loi « Informatique et Libertés ») est la loi française qui a créé le cadre juridique pour la protection des données personnelles, La loi a créé la Commission Nationale de l'Informatique et des Libertés (CNIL), une autorité indépendante chargée de veiller au respect de cette loi et de contrôler les traitements de données.
7 juillet 2009	ANSSI	Autorité française en charge de la sécurité et de la résilience des systèmes d'information. Elle élabore des référentiels de cybersécurité (ex. SecNumCloud), accompagne les acteurs publics et privés, et contribue à la souveraineté numériquede la France et de l'Europe.
27 avril 2016 - 25 mai 2018	RGPD	Règlement européen établissant un cadre harmonisé pour la protection des données personnelles, applicable depuis le 25 mai 2018. Il impose des obligations strictes aux responsables de traitement et renforce les droits des personnes concernées. Il est directement applicable dans tous les États membres de l'Union européenne sans nécessité de transposition en droit national. Le RGPD : • S'applique à tout traitement de données personnelles concernant des citoyens de l'UE. • Exige que les données soient protégées contre tout accès non autorisé. • Interdit en principe les transferts de données vers des pays tiers sans garanties adéquates. Le RGPD définit les données à caractère personnel • Données à caractère personnel : informations permettant d'identifier une personne, dont la protection conditionne le respect des droits et libertés fondamentaux, comme prévu par le RGPD.
12 juillet 2016	Privacy Shield	Mécanisme d'auto-certification pour les entreprises américaines, reconnu par la Commission européenne pour protéger les données personnelles transférées depuis l'UE (1er août 2016). Pour la Cour de Justice de l'Union Européenne (16 juillet 2020, arrêt « Schrems II »), il ne constitue pasune garantie juridique suffisante pour les transferts de données vers les États- Unis.
23 mars 2018	CLOUD Act	Permet aux autorités américaines d'exiger l'accès à des données détenues par des entreprises américaines, même si les serveurs sont situés en Europe. Cette réglementation fait entrave aux réglementations européennes de protection des données.
16 juillet 2020	L'arrêt Schrems II	A invalidé le Privacy Shield, ce qui signifie que vous ne pouvez plus transférer librement des données entre l'UE et les États-Unis, jusqu'au nouveau cadre d'adéquation de juillet 2023.
11 juillet 2023	Data privacy framework	Successeur du Privacy Shield, ce cadre vise à encadrer à nouveau les transferts de données entre l'Union européenne et les États-Unis, en renforçant les garanties de protection des données personnelles exigées par la CJUE.
20 mars 2024	Secnumcloud (v3.3) NB : version originale 2016	Qualification française de cybersécurité pour les fournisseurs cloud, exigeant un contrôle exclusivement européen du capital et de la gouvernance, aucune soumission à des lois extraterritoriales (type Cloud Act) et une sécurité opérationnelle élevée.

GLOSSAIRE & DOCUMENTATION

INFRASTRUCTURES

DATACENTER : Un datacenter est une infrastructure immobilière et technique qui héberge des ressources informatiques (baies, serveurs, stockage, réseaux …) avec tous les équipements nécessaires (électricité, refroidissement, connectivité, sécurité, accès…). Cet environnement est utilisé par des entreprises /collectivités /administrations pour stocker des données, utiliser des applications, et par des fournisseurs de services Cloud.

DATACENTER DE PROXIMITÉ : C'est un datacenter présent localement pour accueillir les systèmes d'informations d'une entreprise ou d'une collectivité. Il peut également héberger des services de fournisseurs et éditeurs extérieurs (hébergement, cloud privé, applications en mode SaaS, télécoms, IA...).

DATACENTER PRIVÉ : C'est un datacenter entièrement dédié aux besoins d'une organisation, qui concerne plus particulièrement les grandes organisations. La notion de proximité est à nouveau fondamentale.

HYPERSCALER : C'est un fournisseur de Services Cloud public à très grande échelle, qui dispose de très importants moyens d'infrastructures et de services, généralement hébergés dans ses propres Méga Datacenter, ou Hyperscale, à l'échelle mondiale. Exemples : Amazon Web Services, Microsoft Azure, Google Cloud.

SALLES SERVEUR OU SALLE INFORMATIQUE : C'est une salle abritant des équipements informatiques qui peut exister en interne d'une organisation, utilisée pour les besoins propres de cette organisation. Une salle serveur est parfois considérée comme un mini datacenter.

OFFRES DE SERVICE DES DATACENTERS

ON-PREMISE : C'est la faculté de gérer ses propres serveurs dans ses propres locaux c'est à dire les "salles serveurs".

HÉBERGEMENT SEC OU COLOCATION : L'organisation loue un espace dans un datacenter existant pour y placer son propre matériel et y installer ses propres services. Elle bénéficie en revanche des autres fonctions du datacenter : climatisation, énergie, raccordement en fibre, sécurité, gestion des accès… La forme de la location peut varier : soit des baies pour y installer ses serveurs ou directement une salle. La colocation correspond à la location de baies, l'organisation dispose d'emplacements pour ses serveurs et partage cet espace avec d'autres utilisateurs. La colocation est parfois confondue avec le terme datacenter mutualisé.

CLOUD OU CLOUD COMPUTING : Le cloud représente tout service informatique utilisé sur un serveur distant, que l'hébergeur ou la localisation soit connu ou non. Cela regroupe les notions d'hébergement de données, serveurs hébergés, SaaS, IaaS, PaaS, cloud computing.

CLOUD PUBLIC OU CLOUD MUTUALISÉ : Un cloud mutualisé est un cloud où plusieurs utilisateurs partagent les mêmes ressources informatique. Partagé un même serveur est possible grâce à des technologies de virtualisation. La limite de cette offre est qu'il n'est pas possible de personnaliser certaines performances, tous les utilisateurs ont la même configuration.

CLOUD PRIVÉ OU CLOUD DÉDIÉ : C'est un environnement de cloud computing dédié à un seul utilisateur. Il peut alors appliquer les critères de sécurité ou de performance qu'il souhaite. C'est naturellement une offre plus chère par rapport au cloud public.

IAAS / INFRASTRUCTURE AS A SERVICE, PAAS / PLATFORM AS A SERVICE : Ce sont des offres cloud où divers services liés à la gestion des serveurs sont externalisés ou non. Parmis ces services : la virtualisation des serveurs, le système d'exploitation...

SAAS / SOFTWARE AS A SERVICE : Un éditeur de logiciel a deux manières de proposer ses services, soit il les propose en téléchargement, soit il les propose sur le cloud sur des serveurs qu'il aura lui-même sélectionnés et qu'il gère à distance pour l'ensemble de ses clients. Le SaaS correspond au service accessible à distance.

ACRONYMES

IA : Intelligence Artificielle

IaaS : Infrastructure-as-a-Service

PaaS : Platform-as-a-Service

RIP : Réseau d'Initiative Public, réseau fibre détenu par des collectivités

SaaS : Software-as-a-Service

SI : Système d'Information

SPL : Société Publique Locale

WAF : Web Application Firewall

DOCUMENTATION DE RÉFÉRENCE

"Recourir à l'offre existante ou développer un datacenter local, Guide pratique à destination des acteurs publics", Caisse des Dépôts, janv. 2014

"Gestion des données : Quels outils et quelle stratégie pour les territoires", Banque des territoires, 2020

"Le datacenter de proximité", 1ère édition InfraNum, 2021

"Refroidissement des datacenters - technologies utilisées en France, potentiel d'économies", Ademe, Critical Building, 2025

DCmag.fr - Datacenter Magazine

DCmag, cartographie des datacenters DCmag & InfraNum en partenariat avec Tactis : https://carte.dcmag.fr/

REMERCIEMENTS

InfraNum tient à remercier tout particulièrement les membres InfraNum, et notamment les membres de la Commission Datacenter, pour leur mobilisation et la qualité des informations partagées, ainsi que l'ensemble des entreprises et des collectivités qui ont enrichi le rapport grâce à leurs retours d'expérience.

Nous tenons plus particulièrement à remercier les rédacteurs de ce rapport :
Estelle RIGAL-ALEXANDRE (Cabinet Soulier Bunch), Jean-Baptiste BARBENCHON et Chloé FAUCILLON (Critical Building), Terence CABOT et Camille LANGLADE DEMOYEN (Latournerie Wolfrom Avocats), Mathieu HULOT (Nation Data Center), Guillaume GOUDARD (Stranum), Emma ROUSSEAU (Thésée Datacenter), Jean-Pierre BALSENTE (Topo Consulting), Arnaud PASDELOUP (Arteria), Jean-Christophe D'ALEMAN (Axione), Gilles BILLET (IFOTEC), Thierry DURIEUX (Inherent), Agnès LE MEIL et Astrid VOORWINDEN (InfraNum).

Nous tenons également à mentionner les entreprises qui ont contribué au sondage et/ou aux entretiens : Axians, Axione, Covage, Cloud Data Engine, DTIX, Grolleau, Inherent, Kwarto, BYCYB, Lumière, Netalis, Netmore, Nexloop, Omega Data Centers, Sogetrel, Synox, Tactis, Terralpha, TDF, Thales Cyber Solutions, Thésée Datacenter.

Coordination : Grace-Léa MBADINGA et Agnès LE MEIL - InfraNum
Mise en page & Graphisme : Paola ROPELE - InfraNum

Crédit Photo : DTiX Datacenters, Eskemm Numérique, Grolleau,Thésée Datacenter