CALIF
COMMUNICATION - AFFAIRES PUBLIQUES

THINK-TANK
DIGITAL
NEW DEAL

INFRASTRUCTURES DU NUMÉRIQUE DE CONFIANCE

UN ENJEU STRATÉGIQUE POUR LES TERRITOIRES.

Réflexions et propositions pour une Infrastructure de confiance, sous la direction de François Massardier et Arno Pons.

novembre 2021

Digital New Deal

SOMMAIRE

PRÉFACE

Pour cette publication, nous avons souhaité nous allier au cabinet de conseil CALIF, dont la fine connaissance des collectivités et entreprises locales était pour nous la meilleure garantie de traiter avec justesse la question des territoires, évitant ainsi de projeter une vision « hors sol » qui aurait été totalement contre-nature.

Cette note a une autre particularité, c'est qu'elle s'inscrit dans un triptyque « Numérique de confiance » mené par notre think-tank. Trois notes qui se suivent et se complètent :

- « Les infrastructures du numérique de confiance », comme fondations architecturales de la souveraineté numérique pour nos territoires ;
- « Le Cloud de confiance », pilier indispensable à la création d'un espace commun de données (publié en mai avec la Mission Numérique des Grands Groupes);
- « IA de confiance », véritable vigile d'un Internet des Lumières (en cours de rédaction pour le Gouvernement)

C'est en consolidant ces trois couches « Infra, data, IA » que nous pourrons bâtir cette troisième voie numérique européenne et humaniste, pour laquelle Digital New Deal milite depuis des années.

Une double conviction nous a animés pour la rédaction de cette note. La première, c'est que nous devons certes digitaliser l'Europe via nos propres technologies, infrastructures, et standards, mais aussi et surtout européaniser le numérique par nos valeurs.

La seconde, c'est que nous devons adapter le numérique aux territoires et non pas seulement l'inverse. La digitalisation des territoires n'est pas une fin en soi ; ce qui se joue, c'est l'intégration des principes humanistes et démocratiques aux espaces numériques, ces nouveaux territoires qui n'ont ni frontières ni élus, mais qui structurent de plus en plus nos vies. Se poser la question des infrastructures de confiance, c'est s'interroger sur le cadre technologique et politique qui sous-tend l'autonomie de nos territoires.

C'est aussi l'opportunité de clarifier le rôle de chacun dans notre gouvernance, avec d'un côté les États européens qui peuvent penser et financer ces infrastructures, et de l'autre les collectivités locales qui sont les plus à même de générer et orchestrer cette confiance.

C'est en combinant vision continentale et exécution locale que nous pourrons offrir un écosystème politique de confiance et ainsi contenir l'entrisme des géants du net dans nos organisations humaines.

Arno Pons, délégué général *Digital New Deal.*

MODALITÉS

Animation des auditions et rédaction du support :
François Massardier (CALIF) **et Arno Pons** *(Digital New Deal)*

MEMBRES DU COMITÉ DE PILOTAGE DU RAPPORT :

Collège des collectivités :

- Florian Bercault, *maire de Laval et président de Laval Agglomération ;*
- Anne-Sophie Bordry, *adjointe au maire du XV^e^ arrondissement de Paris, chargée de la ville connectée et de la transformation numérique ;*
- Pierre Ferrari, *directeur de la stratégie numérique de la Ville d'Arras ;*
- Arnaud Murgia, *maire de Briançon, président de la communauté de communes du Briançonnais et 5e vice-président, en charge de l'aménagement du territoire et des parcs naturels ;*
- Marie Tribout, *ex-conseillère régionale Grand Est déléguée aux usages numériques.*

Collège des personnalités qualifiées :

- Audrey Briand, *responsable des relations institutionnelles France chez Eutelsat ;*
- Liza Bellulo, *secrétaire générale de Bouygues Télécom et membre du conseil d'administration de la Fédération française des télécoms ;*
- Laurent Depommier-Cotton, *directeur du département Transition Numérique au sein de la direction de l'investissement de la Banque des Territoires ;*
- Philippe Tavernier, *délégué général de Numeum.*

Collège des associations :

- Lucile Aigron, *cogérante de la Coopérative des Tiers-Lieux, administratrice du CRESS Nouvelle-Aquitaine et membre du CESER Nouvelle-Aquitaine.*

PERSONNALITÉS AUDITIONNÉES :

- Guillaume Poupard, *directeur général de l'ANSSI ;*
- Fabrice Koszyk, *directeur général de Serenicity ;*
- Margot Corréard, *co-fondatrice et directrice générale de DiagRAMS Technologies ;*
- Jean-Guy de Ruffray, *avocat-associé chez Advant Altana ;*
- Jean-Baptiste de Scorraille, *21^e^ adjoint au maire de Toulouse en charge des antennes radio et de téléphonie ;*
- Agnès Touraine, *présidente fondatrice d'Act III Consultants*
- Sébastien Duré, *directeur général et co-fondateur de Hoppen ;*
- Cédric Messina, *président fondateur de MyCoach, président de la FrenchTech Côte d'Azur ;*
- Cédric Denoyel, *président de H7 ;*
- Laure de la Raudière, *présidente de l'ARCEP ;*
- Jean-Michel Mis, *député de la 2^e^ circonscription de la Loire ;*
- Sébastien Missoffe, *directeur général de Google France ;*
- Thibaut Kleiner, *directeur de la DG Connect auprès de la Commission européenne ;*
- Jean-Luc Sallaberry, *chef du département numérique à la FNCCR ;*
- Vincent Bergeot, *co-président OpenStreetMap France, associé Territorio, entrepreneur-salarié-associé pour Coop'Alpha et Num&Lib et chercheur associé UMR Passages ;*
- Hervé Bonazzi, *président-directeur général d'Archipels ;*
- Paul Duan, *fondateur de Bayes Impact*
- Olivier Dion, *CEO Onecub et co-fondateur de a NewGovernance*

Remerciements à Pierre-Henri Picard (CALIF) et Prune Zammarchi (Digital New Deal) pour leur aide dans la production de ce document.

INTRODUCTION

Le numérique est l'un des domaines où la confiance des citoyens est la plus fragile, que ce soit en raison des divers scandales qui ont émaillé la dernière décennie, en raison de son potentiel totalitaire lorsqu'il sert un agenda idéologique, ou du fait de l'opacité des positions dominantes des géants numériques étrangers. Ces grandes peurs se conjuguent à des risques tout aussi réels : cyberattaques, espionnage industriel, manipulation d'images, de données, voire d'élections.

Pour autant, le déploiement et l'accélération du numérique restent une opportunité inédite pour les collectivités humaines, que ce soit en termes de partage de l'information, de réduction des distances ou pour se donner les moyens techniques d'effectuer une transition écologique chaque jour plus urgente.

Malgré la dimension virtuelle qu'il construit, le numérique repose sur des installations et des équipements bien matériels. Des câbles sous-marins aux réseaux de fibre optique en passant par les pylônes et les centres de données, c'est tout une chaîne matérielle de production qui rend possible la dématérialisation. Or ces installations sont soumises aux aléas, qu'ils soient naturels ou humains. Étant donné l'importance qu'elles ont pris dans nos vies, leur protection est une préoccupation de tous les instants. À cet égard, les infrastructures sur lesquelles repose le numérique ont pris une importance vitale.

QU'EST-CE QU'UNE INFRASTRUCTURE ?

On appelle infrastructure la composante d'un système qui constitue une condition préalable au fonctionnement de ce système. Les infrastructures *« sont classiquement composées d'ouvrages, surtout de communication et de transport, qui assurent la connexion des lieux de l'espace géographique et leur confèrent une fonction sociale créatrice de territoire/territorialité. L'infrastructure constitue un schème organisationnel et matériel d'un réseau imprimé sur (ou sous) l'espace terrestre. Les équipements qu'elle suscite permettent son fonctionnement. »*

Guy Di Méo, Géographie sociale et territoires, Nathan, Paris, 1998

LA PRIVATISATION DES INFRASTRUCTURES CRITIQUES

Les géants du numérique ne se contentent plus de fournir des services aux extrémités, ni même d'enclore les nœuds ; ils vont jusqu'à privatiser le réseau lui-même en fournissant les infrastructures. En finançant ces socles matériels, et en encapsulant les opérateurs économiques via des technologies comme le edge et surtout le cloud, ces géants créent les conditions d'une totale dépendance de nos acteurs historiques.
Peu à peu, ces acteurs déploient leurs technologies dans l'espace public, avec cette double caractéristique : elles deviennent à la fois omniprésentes et invisibles. Ainsi, non contents d'être propriétaires de portions intégrales d'Internet et de technologies matérielles (certains câbles sous-marins par exemple), ces acteurs eux aussi omniprésents et parfois invisibles sont désormais dépositaires de certains services publics nécessitant leurs technostructures.

La dynamique de sous-traitance du service public par le biais de cette infrastructure en privatisation croissante suscite la méfiance du côté de certains citoyens, du fait notamment de l'opacité du fonctionnement des Big Tech ; pour d'autres, la naïveté a laissé place à l'incrédulité face à ces mastodontes économiques qui défient le législateur en obéissant à leurs propres règles, à leur propre rythme…

Ce sentiment d'échappement des géants du numérique au pouvoir accroît la distance entre gouvernants et gouvernés tant au niveau national que local. En effet, il y a danger pour certains projets numériques concernant les territoires moins peuplés et les petites villes de rater leur rencontre avec les habitants. Certains projets se sont ainsi révélés décalés par rapport aux besoins immédiats des populations et par rapport à des contraintes d'ordre pratique (disparition des services publics, zones blanches, illectronisme ou précarité). Il semble dès lors nécessaire de repartir de l'existant, du terrain afin que le numérique puisse remplir sa vocation première : servir la communauté.

L'HUMAIN EST LA MESURE DE TOUTE CHOSE

C'est précisément cette dimension qui semble s'évaporer dans le déterminisme technologique de certains projets. Non seulement les budgets locaux ne permettent pas la transposition de technostructures pensées pour des grandes métropoles, et cela ne fait parfois pas sens pour les communautés locales. Le « techno-solutionnisme » ne répond pas toujours aux demandes fondamentales des citoyens : participer à la décision publique, aménager cet espace public, et ce avec des acteurs de proximité, à qui l'on fait confiance car familiers.

La méfiance que peut rencontrer l'accélération du déploiement des infrastructures numériques dans les territoires est souvent liée au manque de pédagogie et de transparence, ce qui pose la question fondamentale de l'appropriation démocratique de ces nouveaux usages. La multiplication des actes de vandalisme contre les infrastructures, l'émergence de collectifs anti-5G ou encore les réticences d'une certaine partie de la population à prendre le virage de la transition numérique, ces réactions suggèrent aux pouvoirs publics d'identifier les freins actuels, et de se mettre à leur hauteur pour trouver les solutions.

L'infrastructure est le système nerveux d'un pays : elle conditionne le territoire autour d'elle. Elle est la condition de possibilité de l'ensemble des services et de la production de marchandises, ainsi que des pratiques et habitudes les plus quotidiennes de nos vies. La numérisation de ces infrastructures représente un ensemble inédit de défis, tant au niveau technique qu'éthique, économique, écologique et même géopolitique. À la confluence de ces enjeux, les données qu'elles sont amenées à produire apparaissent à la fois comme un point critique et comme un champ inédit de possibles. Au centre de ces enjeux, les données qu'il faudra collecter, exploiter et protéger — d'ores et déjà dans le cadre du RGPD, et demain avec entre autres[1] le Data Governance Act (DGA). Dans la mesure où beaucoup de services municipaux sont en passe d'être délégués à des entités privées, la question de l'accès aux données sensibles et/ou personnelles se pose, ainsi que celle du statut à accorder à ces entités dans la rédaction des contrats.

Fournir des infrastructures numériques de confiance dans les territoires est aussi un enjeu d'attractivité. Les installations numériques de qualité sont un gage d'attractivité économique

[1] *Le Data Governance Act s'insère dans le paquet numérique (Digital Markets Act, le Digital Services Act et le Data Act) en cours de discussion dans les instances de l'Union européenne.*

pour un territoire, qui, en favorisant ainsi la reconstruction des réseaux d'activité, contribue à restaurer la compétitivité nationale nécessaire au « patriotisme économique » et à la souveraineté. Enfin, l'attractivité économique enraye les dynamiques de dépeuplement que connaissent certains espaces.

QU'EST-CE QU'UNE INFRASTRUCTURE NUMÉRIQUE DE CONFIANCE ?

Par infrastructures de confiance, nous désignons l'architecture matérielle et immatérielle sur laquelle reposent les communications électroniques ; cette architecture doit *« garantir notre sécurité technologique et juridique, et protéger nos principes humanistes »*, et constitue le substrat de cette autonomie stratégique que nous appelons de nos vœux.

UN ENJEU DE SOUVERAINETÉ NUMÉRIQUE

Les infrastructures de confiance posent le problème de la souveraineté numérique, notion que le think-tank Digital New Deal a déjà défini dans son premier volet sur le numérique de confiance. Dans ce livre blanc « Cloud de confiance, un enjeu d'autonomie stratégique pour l'Europe » publié avec la Mission Numérique des Grands Groupes, nous avons établi que la souveraineté numérique n'était pas réaliste à court terme, qu'elle était plutôt un objectif. C'est pourquoi nous avons préféré la notion d'autonomie stratégique :

« La souveraineté numérique, c'est notre capacité à maîtriser nos dépendances aux solutions technologiques extra-européennes, à garantir l'autonomie stratégique des États et de leurs entreprises. Mais c'est aussi la capacité à ne pas se laisser imposer une certaine vision du numérique, et à garder notre propre pouvoir d'influence politique dans le monde qui se dessine sous nos yeux.»

La confiance est à reconstruire à partir de ces architectures. Nous en avons besoin pour que les collectivités territoriales puissent assurer la pleine gestion de leurs données dans une logique de réappropriation de l'espace public, pour s'assurer que les territoires restent maîtres de leur destin, pour voir éclore des écosystèmes capables de porter une croissance plus locale et plus responsable.

Au fil des auditions que nous avons menées auprès des acteurs technologiques, politiques, et économiques, locaux et nationaux, deux dimensions sont apparues, que Guillaume Poupard, directeur de l'ANSSI, résume parfaitement ainsi : *« Une infrastructure de confiance, c'est une capacité à maîtriser l'indépendance d'une architecture, et la capacité à la défendre ».*

Cette déclaration nous la faisons nôtre, au point d'articuler le plan de ce rapport sur cette vision, qui relie naturellement la question de la confiance dans le numérique avec l'enjeu d'autonomie stratégique.

“UNE INFRASTRUCTURE DE CONFIANCE, C'EST UNE CAPACITÉ À MAÎTRISER L'INDÉPENDANCE D'UNE ARCHITECTURE, ET LA CAPACITÉ À LA DÉFENDRE”

Guillaume Poupard, *directeur général de l'ANSSI.*

Défendre nos infrastructures numériques, c'est renforcer nos capacités en cybersécurité, pour les entreprises comme pour le régalien ; c'est aussi protéger économiquement nos atouts face aux assauts des géants du net.

Maitriser nos infrastructures numériques, au niveau local, c'est introduire des tiers de confiance dans des relations parfois compliquées entre puissance publique, entreprises et citoyens ; c'est aussi imaginer une maitrise garantie par la participation du plus grand nombre pour empêcher la privatisation de services numériques d'intérêt général.

Défense et maitrise de nos infrastructures numériques : cette double exigence conditionnera la confiance dans nos architectures. Confiance dans leur autonomie technologique et juridique, mais aussi, à l'échelle des populations, confiance dans des infrastructures accessibles, efficaces et transparentes.

I. MAÎTRISER NOTRE INDÉPENDANCE

1. GARANTIR LA SOUVERAINETÉ VIA UN TIERS DE CONFIANCE PUBLIC

Nos concitoyens manifestent une certaine méfiance à l'encontre des nouvelles technologies et de leurs usages. Les exemples sont nombreux, et se déclinent : peur de la réduction de la masse salariale par la robotisation, ou du potentiel de surveillance des terminaux, des objets connectés ou encore manipulation à travers les réseaux sociaux, la réception des controverses et scandales liés au numérique a considérablement fragilisé la confiance des citoyens envers le numérique.

Pour faire face à cet écueil et apporter des éléments de réponse, Thibaut Kleiner, directeur de la DG Connect au sein de la Commission européenne, prône la création de cadres de confiance – comme le règlement général sur la protection des données (RGPD) — pour que les citoyens s'orientent plus facilement vers de nouveaux services permis par l'émergence des nouvelles technologies. Selon le fonctionnaire européen, une réglementation cohérente est *« un levier de compétitivité plutôt qu'un problème*[2]*»*.
L'Union européenne défend ainsi des propositions visant à favoriser le partage des données avec l'Acte sur les données (Data Act), actuellement en cours de préparation, et la réglementation sur la gouvernance des données (DGA) en cours de finalisation. En résumé, il s'agit de défendre la protection des socles de droits fondamentaux et de calibrer la réglementation pour faciliter l'appropriation, l'accessibilité, le partage et la réutilisation des données.

Cette notion de confiance dans les règles d'usage est fondamentale, à la fois pour les usagers mais aussi pour les institutions, notamment celles concernées par les projets de smart territoires. La confiance est en effet un des garants de la souveraineté comme de la protection des données des usagers face à des acteurs tiers étrangers. Face à eux la puissance publique, dont la légitimité émane de la volonté générale, doit se positionner pour protéger et garantir le respect de ces règles d'usage.

Ce constat est d'autant plus vrai que plusieurs opérateurs ont aujourd'hui trop tendance à aller dans une logique d'intermédiarisation[3] dans la gestion de la donnée. Comme l'indique Jean-Luc Sallaberry, chef du département numérique de la Fédération Nationale des Collectivités Concédantes et Régies (FNCCR) : *« La donnée, la notion de tiers de confiance et de gouvernance doivent rester aux mains de la collectivité, tout comme la maîtrise d'ouvrage. Elle peut être déléguée mais le contrôle doit être effectué par la puissance publique*[4]*.».*

Ce dernier concède d'ailleurs que si la FNCCR s'est intéressée à des partenariats hybrides entre acteurs privés et publics pour assurer cette notion de tiers de confiance dans la gestion des données, les résultats n'ont pas été probants. Transmettre les pleins pouvoirs aux acteurs privés n'est donc pas nécessairement recommandé au regard des jeux de concurrence qui peuvent exister entre ces acteurs mais aussi des fusions éventuelles, soit autant de paramètres qui engendrent une complexité dans la gouvernance de la donnée.

[2] *Audition de Thibaut Kleiner par le comité de pilotage du rapport.*
[3] *C'est à dire l'émergence et la multiplication des intermédiaires dans une relation.*
[4] *Audition de Jean-Luc Sallaberry par le comité de pilotage du rapport.*

“

LA DONNÉE, LA NOTION DE TIERS DE CONFIANCE ET DE GOUVERNANCE DOIVENT RESTER AUX MAINS DE LA COLLECTIVITÉ, TOUT COMME LA MAÎTRISE D'OUVRAGE. ELLE PEUT ÊTRE DÉLÉGUÉE MAIS LE CONTRÔLE DOIT ÊTRE EFFECTUÉ PAR LA PUISSANCE PUBLIQUE."

Jean-Luc Sallaberry, *chef du département numérique de la Fédération Nationale des Collectivités Concédantes et Régies (FNCCR).*

Ici, la collectivité est, en tant qu'acteur public, un garant possible pour le citoyen du respect de règles juridiques et éthiques. Elle peut également être à l'origine de la constitution de « tiers de confiance », qui permettent aux acteurs d'un territoire de mutualiser des données et des outils performants d'analyse et de datascience dans le respect d'un cadre éthique et de principes partagés.

Enfin, l'élaboration de standards partagés sur ces enjeux est également essentielle dans la constitution d'une souveraineté numérique européenne, d'autant qu'il existe en Europe un héritage et une légitimité sur cette question. Du GSM à la 5G, l'Union européenne est à la manœuvre pour permettre l'avènement d'un leadership au niveau mondial dans la constitution de standards communs, d'autant que le niveau national est souvent un échelon trop petit pour des industries qui ont une vocation globale. C'est tout l'enjeu de la boussole numérique de 2030[5], qui doit permettre l'élaboration d'un haut standard d'infrastructures, de compétences, de services publics numérisés, et de PME. Le potentiel est important, au vu de la transformation de l'immobilier, du transport, des énergies renouvelables et de toutes les techniques qui permettront d'effectuer la transition écologique.

D'après Thibaut Kleiner, *« le grand risque en Europe est de ne pas être aussi ambitieux qu'on le devrait et qu'on travaille chacun dans son coin. Il faut travailler sur une taille continentale, Il faut développer ces standards mondiaux, se les approprier pour innover.[6]»*
Une ambition qui répond à la volonté de l'UE de développer une politique régionale européenne en s'appuyant notamment sur les FEDER, FSE+ et FEAMP, mis en œuvre au moyen de programmes régionaux ou nationaux ou de coopération territoriale européenne. Pour la période 2021-2027, la programmation de ces fonds, gérés en France par l'État et par les conseils régionaux, s'articulent autour de 5 priorités parmi lesquelles une Europe plus intelligente, grâce à l'innovation, et une Europe plus connectée, dotée de réseaux stratégiques de transports et de communication numérique.

Garantir la souveraineté de nos infrastructures et de nos données par des tiers de confiance publics pose donc la question du modèle adéquat vers lequel doivent tendre les smart territoires mais aussi les différents acteurs économiques et la façon dont les collectivités peuvent garder la maîtrise de leur destin face aux opérateurs de services numériques. Cette exigence de garder la maitrise face aux acteurs économiques est aussi une manière de réinscrire la gestion des infrastructures et des données des collectivités dans le principe de subsidiarité[7] qui régit la répartition des compétences au niveau de l'action publique.

Une fois n'est pas coutume, c'est vers la Californie que nous pouvons trouver l'inspiration avec l'exemple de Los Angeles, qui avait demandé à Uber de fournir les données de localisation des trottinettes et vélos électriques de sa marque Jump en temps réel pour gérer le problème d'encombrement des trottoirs et s'assurer de la dimension égalitaire de l'accessibilité de ces services (quartiers populaires moins desservis comme dans l'ensemble des grandes villes dans le monde). Uber ayant refusé la demande des autorités municipales, la ville avait alors menacé Uber en précisant que si l'entreprise n'obtempérait pas dans les temps, *« leur permis sera suspendu, et éventuellement révoqué[8]»*. La ville a mis ses menaces à exécution, montrant ainsi que les collectivités peuvent devenir les garantes de la souveraineté.

---

[5] *Décennie numérique de l'Europe : objectifs numériques pour 2030, Commission européenne, 9 mars 2021, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_fr*
[6] *Audition de Thibaut Kleiner par le comité de pilotage du rapport.*
[7] *"maxime politique et sociale selon laquelle la responsabilité d'une action publique, lorsqu'elle est nécessaire, revient à l'entité compétente la plus proche de ceux qui sont directement concernés par cette action. Lorsque des situations excèdent les compétences d'une entité donnée responsable de l'action publique, cette compétence est transmise à l'entité d'un échelon hiérarchique supérieur et ainsi de suite." Wikipédia, article "principe de subsidiarité".*
[8] *"LA suspends Uber's permit to rent out electric scooters and bikes", Los Angeles Times, 4 novembre 2019.*

QUEL MODÈLE PÉRENNE POUR LES SMART TERRITOIRES ?

Dans les smart territoires, l'usage des technologies de l'information et de la communication (TIC) dans tous les secteurs d'activité vise à produire des dynamiques urbaines inédites, capables de stimuler l'innovation et le développement économique sur le territoire, tout en impulsant de nouvelles formes de gouvernance publique/privée.

QU'EST-CE QU'UN SMART TERRITOIRE ?

Un smart territoire est un espace géographique où l'usage des technologies d'information et de communication est pensé pour améliorer la qualité de vie de ses citoyens. Parmi les objectifs du smart territoire, l'augmentation de son efficacité en réduisant les déchets et la consommation d'énergie, l'amélioration de la sécurité et la fluidification de la mise en place des politiques publiques pour des espaces de vie plus résilients, plus durables et plus localisés, où la technologie ne restera qu'un moyen de créer du lien pour plus de cohésion.

Le territoire est désormais perçu comme *« un laboratoire local vivant permettant aux entreprises de tester et de présenter des produits et services innovants aux bénéfices des citoyens et des institutions politiques présents sur le territoire*[9]*»*.
La mise en œuvre de cette nouvelle définition de politique publique au niveau local se fait à travers la récolte et l'analyse de données par des objets connectés, dans le but d'optimiser le fonctionnement de l'ensemble des mailles des réseaux, qu'ils concernent l'énergie, ou encore les mobilités. Redéfinir les politiques territoriales par la data passe aussi par le positionnement de ce territoire directement sur les usages finaux et le partage de données.

Angers Loire Métropole a confié au mois de novembre 2019 son projet de territoire intelligent à un consortium mené par Engie Solutions (filiale d'Engie) qui associe Suez pour la partie environnementale, le groupe mutualiste Vyv pour les questions de santé et La Poste pour l'hébergement et la gestion de données. Comme le concédait à l'époque Yann Rolland, directeur général d'Engie Solutions en charge de la Business Unit « villes et collectivités »,
« La Poste sera le tiers de confiance[10]*».*

S'il soulignait que ce projet était *« le plus abouti »*, Christophe Béchu, président de l'agglomération, reconnaissait par ailleurs au moment de la signature du contrat qu'il impliquait *« un certain nombre d'allers et retours sur les aspects qui [leur] conviennent moins*[11] *»*. Dans les faits, le projet s'articule autour du déploiement de lampadaires équipés de détecteurs de présence qui s'éteignent quand les rues sont désertes, de la pose de canalisations d'eau intelligentes qui signalent les fuites ou des conteneurs à déchets qui alertent les éboueurs quand ils sont à saturation.

La communauté urbaine d'Angers investit ainsi 178 millions d'euros sur les douze prochaines années pour installer quelque 50 000 objets connectés sur son territoire. Objectif affiché par les élus de la métropole : accélérer la transition énergétique et écologique de la collectivité tout en améliorant les services proposés aux habitants. Ces derniers ambitionnent de réaliser 101,2 millions d'euros d'économies générées sur 25 ans grâce aux technologies mises en

[9] *"Les enjeux de la politique énergétique de la métropole du Grand Lyon en matière d'ouverture des données", Thoma Lamb, Revue française d'administration publique 2018/3 n°167.*
[10] *"Angers confie les commandes de sa smart city à Engie Ineo", Les Echos, 22 novembre 2019.*
[11] *Ibid.*

place. Grâce aux capteurs installés dans les rues, les conducteurs pourront savoir où se trouve la place de parking libre la plus proche dans une logique visant la fluidification du trafic et le gain de temps. De fait, la collectivité expliquait au moment du lancement du projet vouloir *« économiser les ressources pour accélérer la transition écologique du territoire ; améliorer et proposer de nouveaux services aux habitants par une action publique plus efficace et plus proche des attentes ; optimiser la gestion du service public et ses coûts de fonctionnement, par la modernisation des moyens d'action et des process qui permettront d'importantes économies d'énergie*[12]*»*.

Notons qu'Engie Solutions est l'interlocuteur exclusif d'Angers. L'entreprise assure l'avancement du projet et des solutions prévues par livin', sa plateforme de gestion de l'ensemble des attributions de la smart city.

livin' joue également un rôle dans la gestion et l'optimisation de la circulation, de la qualité de l'air, du stationnement ou encore de l'efficacité énergétique. Enfin, grâce à cette plateforme, Angers peut générer des « jumeaux numériques » qui permettent de tester en amont différents process pour résoudre un problème spécifique.
Si Yann Rolland a promis lors du lancement du projet que *« ce ne sera pas Big Brother, les données sont la propriété de la collectivité, rien ne nous appartient et tout sera anonymisé. On ne saura rien sur personne, mais on saura tout sur l'ensemble*[13]», il est légitime de s'interroger sur les règles de gouvernance choisies, et sur la capacité de la ville à les faire respecter.

Le premier sujet auquel doivent prendre garde les collectivités concerne la collecte, l'exploitation et la protection des données entrant dans le champ du RGPD.
Aussi, l'apparition d'un nombre croissant de services privés sur des domaines qui étaient avant gérés exclusivement par les collectivités doit conduire les élus à bien calibrer leur intervention, la commande publique n'étant plus l'unique levier. C'est plus particulièrement le cas dans la mobilité où des sociétés proposent des services — locations de vélos, trottinettes, scooters, autopartage — susceptibles de trouver un équilibre financier rapide.

DES CHARTES MÉTROPOLITAINES DE LA DONNÉE

De fait, l'élaboration de chartes métropolitaines de la donnée telle que mises en œuvre à Nantes et Montréal est un prérequis nécessaire visant à partager les données d'intérêt général du territoire et définir des principes communs dans l'usage et le traitement de ces données. À la différence des chartes sectorielles existantes, l'originalité de ce document est d'être co-construit avec les acteurs locaux et de ne pas différencier les données publiques de celles traitées par des acteurs privés proposant des services sur l'espace public. Avec les contrats de délégation de service public (DSP), les collectivités restent en effet dans le pré carré de l'action publique mais ne peuvent pas accéder aux données des nouveaux acteurs des services urbains que sont Uber, Amazon ou AirBnb par exemple.

L'accès aux données produites par les acteurs urbains privés est une question pertinente à la lumière du lancement actuel de la troisième société dédiée aux smart cities issue de la scission d'Engie, Connect. Cette société doit réunir les activités encore naissantes de ville intelligente qui permettent d'optimiser les services urbains par l'usage du numérique. Connect se trouve à

[12] *"Engie va mener la transition d'Angers Loire Métropole en smart city", L'Usine Digitale, 25 novembre 2019.*
[13] *"Angers confie les commandes de sa smart city à Engie Ineo", Les Echos, 22 novembre 2019.*

la confluence entre les activités de services dont Engie souhaite se séparer en créant Equans. Or, il existe ici un flou en matière de gouvernance et de contrôle de Connect puisque la future entité qui récupérera la gestion du projet à Angers sera une co-entreprise, détenue à 50 % par Engie et 50 % par Equans, entité qui doit être prochainement cédée soit à un/des fonds d'investissement (Advent International, Carlyle, Bain Capital), soit à des industriels positionnés sur les sujets de territoires intelligents.

La charte métropolitaine de Nantes avait été approuvée par une cinquantaine d'acteurs – grandes entreprises (Engie, EDF), entreprises et acteurs publics locaux – mais aucune des entreprises américaines qui sont au cœur des craintes des habitants sur leur données personnelles. De fait, si un ou des fonds d'investissement américains venaient à prendre le contrôle d'Equans, la question de la pleine gestion des données par la collectivité dans une logique de réappropriation de la ville se poserait nécessairement. Il s'agit donc de s'interroger sur la façon dont les collectivités peuvent éviter l'ubérisation de la ville par la captation ou la dispersion des données entre des acteurs privés puissants, ou entre de multiples acteurs.

Ceci est d'autant plus vrai pour Angers car même si la collectivité assure avoir limité le rôle des entreprises — elles sont principalement vouées à construire l'infrastructure, assurer les opérations de maintenance et de mise à jour, et apprendre à la ville l'utilisation des outils de pilotage — certains domaines resteront toutefois entièrement gérés par des entités privées comme la signalisation et l'éclairage intelligent.

QU'EST-CE QU'UN HYPERVISEUR ?

Un logiciel d'hypervision a pour fonction de centraliser l'ensemble des outils de supervision, des applicatifs, des référentiels et des données d'une ville, et permet ainsi une gestion automatisée, fluide et transverse des infrastructures urbaines. Autrement dit, l'hyperviseur est une plateforme de pilotage des différents logiciels sur lesquels vont fonctionner les infrastructures connectées.

L'hyperviseur urbain est la pierre angulaire d'un projet de smart city. Plusieurs sociétés se sont positionnées sur ce type de marché à l'instar de l'entreprise française Capensis, qui a lancé Canopsis, sa solution d'hypervision en open source, à l'inverse de tous ses concurrents utilisant des logiciels propriétaires. Un travail doit donc être mené par les autorités publiques visant à renforcer les règles du jeu sur la protection, l'usage et les modalités d'accès à la data au niveau des territoires.

Ces règles, édictées et contrôlées par des tiers de confiance, pourraient par exemple concerner la façon dont les collectivités peuvent garantir facilement le respect des droits des citoyens dans l'espace public, quel que soit le type de capteur mobilisé (caméra vidéo, outil de comptage ou de détection…), ou encore imposer la rédaction de clauses dans les contrats stipulant que les délégataires agissent en tant que sous-traitants de la collectivité pour garantir à celles-ci la pleine maîtrise des données.

L'enjeu de souveraineté repose donc bien sur le choix des outils qui garantissent à la collectivité qu'elle conserve la maîtrise de son territoire à travers la pleine gestion de ses données et de celles que les acteurs privés (prestataires ou non) génèrent sur ce même territoire. Comme le

pointe la Banque des Territoires, *« elle doit garantir que les prestataires (éditeurs de logiciels ou délégataires de service public par exemple), ne s'approprient pas les données publiques et donc la connaissance des territoires notamment en utilisant des formats informatiques dont ils seraient seuls propriétaires.*[14]*»*

LE RENFORCEMENT DE L'APPROCHE TERRITORIALE DANS L'USAGE DE LA DONNÉE

La transformation numérique de la société amène donc à la disponibilité de nouvelles données concernant le territoire : données collectivités, données commerçants, données usagers. C'est une multitude de données qu'il faut capter et agréger pour les valoriser, d'autant que les données sont le carburant de la transformation numérique des territoires et in fine, un vecteur de leur compétitivité. En effet, les informations produites par ces échanges aident les entreprises et les opérateurs publics présents sur un territoire donné à fournir de meilleurs services à leurs utilisateurs et partenaires.

Dans le cas du tourisme par exemple, la captation des données, leur partage et leur traitement peuvent améliorer l'immersion du voyageur grâce au développement d'une nouvelle offre touristique basée sur un écosystème de partage où le touriste bénéficie d'une expérience sans couture, personnalisée et respectueuse de sa vie privée. Ce partage des données devrait s'amplifier avec l'Internet des Objets, eux-mêmes matérialisés par des capteurs et des applications smartphones, ainsi que l'open data qui met à disposition les données du territoire à des partenaires tant publics que privés. L'émergence de ce type de dispositifs permet de gérer de façon plus agile les déplacements et les activités sur site des visiteurs grâce à l'inclusion des technologies numériques.

Mettre sur pied des standards communs de partage de la donnée dans une logique de renforcement de la coopération interterritoriale apparaît comme un prérequis nécessaire au développement des écosystèmes locaux, à l'image de l'échelon régional vis à vis des projets de smart cities. Ces données représentent par conséquent la base nécessaire de tout service numérique. De ce carburant découlent des enjeux pour les territoires et les collectivités. D'où la nécessité de développer un « Cloud de Confiance », sujet qui a fait l'objet d'un livre blanc dédié[15] en avril par le think-tank.

Les données peuvent provenir de différentes sources : entreprises, administrations, utilisateurs, tout ce qui est connecté à un réseau peut produire de la donnée. Chaque donnée est spécifique et répond à des règles juridiques claires dont découlent des questions de souveraineté, de transition environnementale et de choix technologiques. La gestion des données par les collectivités répond par conséquent à des choix politiques et stratégiques, c'est pourquoi l'acculturation numérique des élus et des services internes aux collectivités est un enjeu fondamental. D'où l'importance pour les collectivités sur ce sujet du délégué à la protection des données personnelles (DPO), en charge de la conformité au RGPD des différents projets digitaux.

Un autre texte juridique est contraignant pour les collectivités dans l'usage de la donnée. La loi pour une République numérique — dite Loi Lemaire — oblige depuis 2018 toutes les

[14] *"Aymeric Buthion, Jeanne Carrez-Debock, Didier Célisse, Chloé Friedlander, Lucas Griffaton-Sonnet, Emmanuel Passilly, Mathieu Prot, "Gestion des données : Quels outils et quelle stratégie pour les territoires ?", Banque des Territoires*
[15] *Cloud de Confiance, un enjeu d'autonomie stratégique pour l'Europe.*

collectivités territoriales de plus de 3 500 habitants (et 50 agents en équivalent temps plein) à publier les données de leur gestion *« par défaut »*.

L'usage de la donnée est strictement encadré en Europe, où les sanctions sont importantes (amende pouvant atteindre 20 millions d'euros ou dans le cas d'une entreprise jusqu'à 4% du chiffre d'affaires annuel mondial). Il est alors important dans le développement des services numériques que les élus et collaborateurs soient parfaitement conscients des enjeux et des risques.

Le développement des infrastructures numériques dans les territoires permet l'éclosion de services numériques utiles aux collectivités. La maîtrise des données territoriales peut permettre des économies substantielles dans la conduite des politiques publiques : gestion des réseaux, des transports, la mise en place de e-services, etc. À travers ces technologies, il est aisé d'imaginer le développement de villes et de territoires connectés dès lors que ceux-ci bénéficient d'équipements permettant une meilleure gestion et maîtrise des politiques publiques locales. Ces services ont vocation à automatiser la gestion d'un territoire, le rendre plus simple, plus transparent, plus résilient, plus attractif, plus durable et plus inclusif.

ARRAS POTENTIALISE SON ATTRACTIVITÉ TOURISTIQUE PAR LA DATA

Les services de la commune d'Arras sont aujourd'hui capables, grâce à l'essor des outils numériques, de connaître le parcours des visiteurs, leur panier moyen, le temps consacré, etc. Tant de données qui sont importantes pour les collectivités pour adapter leurs politiques et innover et qui invitent à réfléchir sur l'organisation à adopter. Ces outils d'analyse plus performants peuvent en effet permettre de mieux connaître le territoire, de mieux identifier les besoins des habitants, de mieux mesurer l'impact des politiques locales.

Les élus locaux ont désormais la possibilité de repenser le modèle opérationnel de leur territoire pour concilier données et démocratie. En intégrant la donnée comme élément structurant dans la définition et le déploiement des politiques publiques territoriales, ils doivent par ailleurs prendre garde à respecter un cadre éthique et déontologique. Dans le cadre de la crise sanitaire, certaines villes étrangères ont pu s'appuyer sur leurs infrastructures pour lutter contre le virus. On peut citer la Corée du Sud qui a utilisé la donnée présente au sein du hub mis à disposition par le ministère des Territoires, des Infrastructures et des Transports, au service du Centre coréen de contrôle et de prévention des maladies. Cela a permis aux épidémiologistes de détecter les voies de transmission et ainsi limiter la propagation du virus[16].
Si — et seulement si — le contrat social est respecté entre l'administration et les administrés, et si la gestion des données est transparente, traçable et auditable, alors l'acceptabilité de ces infrastructures numériques devient possible.

Une infrastructure de confiance ne peut fonctionner qu'à travers la qualité des rapports entre le capteur et le capté, et dans le renforcement de la coopération entre territoires pour permettre une gestion des données qui profite à tous. C'est l'ambition des dataspaces territoriaux et

[16] *"Smart city technology reinvents contact tracing method", MOLIT, 26 mars 2020.*

des standards communs de partage des données dans une objectif de compétitivité, mais aussi l'établissement d'un cadre de coopération plus large entre le monde économique et la sphère publique.

Les nouveaux usages de la donnée et l'intégration de nouvelles données pour le pilotage des politiques publiques nécessitent une adaptation des systèmes d'information des collectivités. Les données doivent facilement être extraites et circuler, tout en garantissant un haut niveau de sécurité. Ces évolutions passent par l'intégration de priorités nouvelles dans le développement des outils informatiques et l'intégration d'exigences nouvelles dans les cahiers des charges :

- Existence d'interfaces pour accéder aux données (les « APIs ») ;
- Apparition de nouveaux modes de stockage adaptés aux données massives, comme les écosystèmes de partage de données décentralisés ;
- Choix de logiciels garantissant le contrôle public de l'utilisation des données et la possibilité de publier des données en open data ;
- Recours possible à l'open source ;
- Exigence de formats favorisant l'interopérabilité pour pouvoir croiser et exploiter au mieux les données sur un territoire ou entre territoires.[17]

La libre circulation des données appelle implicitement l'émergence d'une multitude d'acteurs dans l'élaboration de nouveaux usages et donc d'une nouvelle forme de décentralisation. La confiance de tous envers chacun est fondamentale pour le développement harmonieux des infrastructures numériques et pour ce nouvel acte de décentralisation.

2. ÉVITER LA CENTRALISATION DES POUVOIRS VIA LA MULTITUDE

L'effet de réseau, cœur de la révolution numérique, fait de la gestion de la confiance le nouveau paradigme politique, et de la décentralisation son meilleur allié. En jouant la multitude contre les monopoles, la décentralisation contre la plateformisation, nous pouvons inverser l'asymétrie qui existe entre les Big Tech et nos organisations politiques.
L'heure est donc à la confiance par la multitude ; cela passe par la prise de conscience par les citoyens de leur pouvoir en tant qu'internautes et par la création de cadres de gouvernance adaptés.

LA CONFIANCE ASSURÉE PAR LES COMMUNS NUMÉRIQUES

D'après Sébastien Broca, chercheur en sociologie au Centre d'études des techniques, des connaissances et des pratiques de la Sorbonne et auteur d'*Utopie du logiciel libre* (2013), la fin de l'urgence pandémique a entraîné *« le retour de l'idée que seul l'État peut être le garant de l'intérêt général (…). La crise avait pourtant montré le contraire : dans l'urgence, ces communs en étaient, eux aussi, devenus les garants. Il s'est joué là un peu plus qu'un bricolage en temps de crise dont on pourrait se passer ensuite. Il y a beaucoup à apprendre de cette mobilisation, y compris pour des temps moins tourmentés. L'État devrait être plus attentif à cette créativité et à ces forces venues de la société civile.*[18]»

[18] *"Après la crise, les communs numériques en quête de reconnaissance", Claire Legros, Le Monde, 31 juillet 2020.*

La société civile s'est en effet remarquablement emparée de la crise sanitaire et des confinements en construisant ou en aménageant des solutions numériques de continuité des activités, dont le foisonnement témoigne de l'inventivité des internautes.

FRAMASOFT, UN COMMUN NUMÉRIQUE EN QUÊTE D'AUTONOMIE

Les services en ligne de l'association d'éducation populaire Framasoft, qui milite pour des logiciels libres, ont été pris d'assaut par des télétravailleurs en quête d'outils de partage et de visioconférence efficaces, transparents et respectueux des données personnelles. Framasoft propose par ailleurs des infrastructures techniques alternatives, comme le projet de CHATONS, le Collectif des Hébergeurs Alternatifs, Transparents, Ouverts, Neutres et Solidaires. Lancé en 2016, ce collectif cherche à développer des réseaux d'acteurs locaux, qui s'engagent à fournir des services équivalents mais décentralisés et autonomes par rapport aux GAFAM : hébergement de sites web, outils collaboratifs, services mails... Autant de leviers dont l'objectif est de permettre aux usagers de reprendre la main sur des outils du quotidien, dans une logique à rebours des entreprises américaines.

Ces solutions contributives et solidaires (logiciels, hébergements de sites, clients email) sont des communs numériques, c'est à dire des ressources ouvertes, coproduites et maintenues par une communauté qui définit ses règles de gouvernance. Il s'agit, en résumé, de revenir à l'ambition initiale portée par *« les « Pères fondateurs » de l'Internet, les ingénieurs qui ont conçu ce réseau, avaient une ambition majeure : créer un réseau solide, ouvert, coopératif et garantissant l'horizontalité et la liberté d'expression »*, note Hervé Le Crosnier, enseignant-chercheur à l'université de Caen.[19]

LES COMMUNS NUMÉRIQUES, UNE CONTRE-CULTURE INFORMATIQUE

Dès le milieu des années 1970 les États-Unis ont commencé à faire protéger les logiciels par le droit d'auteur, encourageant indirectement des communautés d'utilisateurs à s'auto-organiser afin de continuer à produire, gérer et faire circuler des ressources numériques librement. Aujourd'hui, les exemples les plus connus de communs numériques s'appellent Linux, Wikipédia, Open Food Fact ou encore OpenStreetMap, et parviennent à survivre voire dans certains cas à faire davantage autorité que certains services proposés par les GAFAM.

Vincent Bergeot, co-président OpenStreetMap France et chercheur associé UMR Passages, affirme que *« le modèle communautaire, comme OpenStreetMap (OSM) est la solution pour créer la confiance dans les infrastructures*[20]*»*. La confiance envers les infrastructures se construit ici sur des « données de confiance » : les données issues des communs numériques sont à jour et fiables car transmises par des utilisateurs qui sont légitimes. Aujourd'hui, il y a plus de 2 millions de personnes qui contribuent à cette base de données. Ce chiffre augmente tous les jours. 2 à 3 millions de données sont modifiées tous les jours dans le monde. Ces interactions permettent d'avoir une base de données de 8 milliards de points utilisable et utilisée par tous, y compris par les GAFAM – hormis Google.

[19] *Ibid.*
[20] *Audition de Vincent Bergeot par le comité de pilotage du rapport.*

La confiance se trouve dans la multitude des contributeurs[21]. Chaque modification apportée par l'un d'entre eux est dupliquée et renvoyée à différents endroits. C'est également un gage de qualité pour la donnée car plus les internautes utilisent cette donnée, plus nombreux sont ceux en mesure de percevoir les erreurs et de les corriger. En ce sens, pouvoir ajouter une donnée et savoir qu'elle est visible quasi-directement est un élément important du succès d'OSM.

Cette « démocratie numérique contributive » s'appuie sur une dynamique de co-construction, la technologie utilisée étant transparente, libre et open source. Elle est portée par des communautés de développeurs aussi bien à l'intérieur des administrations qu'à l'extérieur, et suppose que les acteurs publics acceptent de produire des infrastructures en collaboration avec des communautés d'utilisateurs mobilisés qui s'impliquent dans la construction partagée des politiques publiques à travers des expériences de co-design. Cela étant, le déploiement de ce type de démocratie soulève des enjeux en termes de contrôle des infrastructures informationnelles et de gouvernance partagée.

LES PLATEFORMES DE PARTICIPATION CITOYENNES À L'ÉCHELON LOCAL

Le cas de la création de Decidim par la Ville de Barcelone est éclairant. La volonté de la collectivité était de disposer d'une infrastructure numérique lui permettant de co-construire son action avec les citoyens et tous les échelons territoriaux. De fait, Decidim s'apparente moins aujourd'hui à une plateforme numérique qu'à un projet social et politique dont la pérennité passe nécessairement par la combinaison d'une diffusion open source et une gouvernance ouverte et participative.

Cette combinaison est une réussite puisque Decidim est utilisé à l'international et notamment en France. En effet, plus d'une trentaine d'organisations utilisent Decidim dans l'Hexagone pour des processus participatifs ponctuels, réguliers ou pérennes. Ce modèle de commun numérique tente de répondre à des défis sociétaux nouveaux, à mutualiser la conception de solutions qui évoluent au gré des besoins des utilisateurs[22].

Decidim n'est pas la seule plateforme de participation citoyenne. Cap Collectif ou encore Make.org ont également pour ambition de développer une méthode de consultation massive, capable de toucher plusieurs millions de personnes.

Ces démarches s'inscrivent dans la volonté des citoyens de participer aux processus de construction des politiques publiques, en lien avec leurs aspirations pour le territoire dans lequel ils vivent ou travaillent, mais aussi de renforcement du sens qu'ils souhaitent donner à leur participation dans les entreprises et/ou organisations au sein desquelles ils sont engagés.

La multitude apparaît comme une réponse face à la crise de confiance des citoyens à l'encontre des géants du numérique et des institutions. Elle est en ce sens le garant d'un renouveau démocratique dans l'usage des outils numériques et rejoint l'idée première des « fondateurs d'Internet » de disposer d'un réseau dont l'esprit reposait sur la liberté, la transparence, et le partage.

[21] *voir L'âge de la Multitude. Entreprendre et gouverner après la révolution numérique, Nicolas Colin et Henri Verdier, Armand Colin, Paris, 2015.*
[22] *"Decidim, un commun numérique pour la participation citoyenne", Labo Société Numérique.*

BLOCKCHAIN, PROTOCOLE DE LA CONFIANCE DÉCENTRALISÉE

Près d'un demi-siècle après la mise en service du réseau de l'Agence des projets de recherche du département de la défense américain (ARPA), la blockchain est le protocole qui transpose le mieux technologiquement cet esprit pionnier et son mode de gouvernance. Née d'une méfiance envers les « Big Banks » et leur rôle dans la crise financière de 2008, la blockchain se veut aujourd'hui une véritable alternative aux Big Tech.

À l'image des premiers universitaires à avoir travaillé pour l'ARPA en développant les premiers sites web en toute indépendance des constructeurs et des grands opérateurs de télécommunications de l'époque grâce au partage des logiciels, des données et des ressources humaines, la blockchain permet aujourd'hui d'obtenir un certain niveau de confiance par la transparence grâce à la multitude d'acteurs qu'elle convoque dans le cadre d'une transaction. Dès 2018 *Digital New Deal* publiait une note expliquant la nécessité de saisir cette chance de rentrer dans « L'âge du web décentralisé » afin d'éviter le phénomène de centralisation des pouvoirs aux mains de quelques géants du net. Nous y renvoyons le lecteur en quête de précisions.

Selon Hervé Bonazzi, CEO d'Archipels, *« le protocole et le design, par eux-mêmes, créent la confiance (…). Personne n'a intérêt à tricher dans un protocole blockchain. Tout le monde est obligé de valider les transactions et du coup d'y faire attention à ce qu'il y est écrit[23]».*

Cette technologie offre une résilience optimale face à d'éventuelles pertes ou corruption des données : toutes les informations échangées sont dupliquées et disponibles sur chaque ordinateur du réseau. Elles ne peuvent pas être modifiées ou encore supprimées sans l'accord unanime des autres ordinateurs. Une machine corrompue peut être mise en « quarantaine » sans que le réseau principal — c'est-à-dire la majorité des autres machines — n'ait besoin d'être mis hors ligne ou en maintenance pour ses utilisateurs, à l'instar d'Internet où un ordinateur ne peut pas interrompre le réseau.

Toute transaction présente dans la blockchain s'appuie sur une validité reconnue au moment de son exécution — puisque l'inclusion dans un bloc de transactions puis dans la blockchain est conditionnée par cette validité — et par sa dimension infalsifiable, y compris par des acteurs malveillants qui participeraient au réseau. D'un point de vue strictement matériel et physique, une blockchain ne représente qu'un réseau d'ordinateurs qui s'échangent des informations et des données. C'est donc moins l'infrastructure matérielle de cette technologie qui est révolutionnaire que son protocole et ses algorithmes, puisque ces derniers dictent aux ordinateurs qui s'y connectent une façon inédite de s'échanger des informations. Il s'agit d'une innovation radicale comparable à celle de l'invention du Web.

Si l'essor de la blockchain est si décisif, c'est qu'elle vient transformer deux ordres de fait d'une importance considérable pour la société. La première transformation, économique, est celle des modes matériels de transaction. Dans le cas du Bitcoin par exemple, nul besoin de faire confiance aux banques pour effectuer une transaction d'un compte à un autre : il suffit de faire fonctionner l'architecture de consensus décentralisé pour authentifier la requête et effectuer la transaction entre les comptes. Plus besoin de banques traditionnelles ni de garantie par la puissance publique.

[23] *Audition d'Hervé Bonazzi par le comité de pilotage du rapport.*

La seconde transformation, politique, est celle qui voit des réseaux privés — ou plutôt communautaires — se substituer aux réseaux des institutions, qui auparavant proposaient une régulation à la fois publique et centralisée. Or cette décentralisation radicale peut aussi être une occasion pour la puissance publique de trouver un nouveau rôle en faisant un pas de côté pour se positionner comme partie prenante tierce ; sa légitimité propre s'ajouterait à celle de l'architecture en créant un effet cumulatif de légitimité, qui alimenterait en retour la confiance.

Il est possible aujourd'hui d'imaginer une ville « blockchainée » : un sujet peut être discuté lors d'un conseil municipal (ou régional), avec des décisions prises démocratiquement, en toute transparence ; ces décisions pourraient être validées par la technologie blockchain. Si une collectivité utilisait une technologie blockchain pour certains de ses besoins, elle pourrait si elle le souhaitait venir porter sa voix dans un comité de gouvernance d'infrastructures dès lors qu'elle opèrerait un nœud elle-même. Hervé Bonazzi indique à ce titre que la collectivité peut *« participer à l'infrastructure techniquement, c'est-à-dire investir, mettre un coût en face d'opération d'un nœud et participer au réseau de confiance en le décentralisant finalement, en gardant copie du registre pour renforcer la résilience et la confiance ».*[24]

Depuis 2016, le droit français reconnaît une existence juridique – certes, principalement financière – aux « Dispositifs d'Enregistrement Électronique Partagé (DEEP) », davantage connue par le grand public sous son appellation anglophone de « blockchain technology ». Cette reconnaissance normative témoigne de l'intérêt ainsi que de l'adoption progressive de cette nouvelle technologie, qui révolutionne techniquement le partage d'informations numériques, et théoriquement, son approche par le marché.

Les smart contracts constituent l'un des usages innovants qu'offre la blockchain pour sécuriser les transactions contractuelles à condition que les acteurs impliqués disposent d'une parfaite connaissance sur les tenants et aboutissants de cette technologie. Dans les smart contracts, le caractère numérique et automatisé du contrat permet à deux partenaires de nouer une relation commerciale sans qu'ils aient besoin de se faire confiance au préalable, sans autorité ou intervention centrale.

En somme, la blockchain fonctionne comme une circulation technologique de la preuve. L'architecture décentralisée permet la multiplication par distribution authentifiée des preuves en dépôt dans un réseau physique d'ordinateurs. La transparence des algorithmes utilisés et leur auditabilité[25] impliquent un accès ouvert et permet de rendre des comptes aux parties prenantes de la chaîne. Les technologies internes de cryptographie ajoutent de la sécurité, tandis que la résilience du système général est rendue possible par la duplication des informations sur les postes et l'éventualité prévue de l'isolement d'un poste corrompu.

Cette distribution technologique de la preuve se décline dans trois types d'algorithmes : Proof-of-Work, Proof-of-Stake et Proof-of-Authority.

L'algorithme de Proof-of-Work (PoW) est la principale méthode de validation de la blockchain à ce jour, grâce à la construction centrale du Bitcoin qui introduit le protocole en 2009. Cette méthode consiste à utiliser la preuve de travail[26] comme algorithme de consensus pour valider les transactions et construire de nouveaux blocs dans la chaîne. Ce consensus sécurise par

[24] *Audition d'Hervé Bonazzi par le comité de pilotage du rapport.*
[25] *Que l'on peut vérifier ou évaluer par un audit. L'auditabilité indique la possibilité d'être vérifié par un tiers, et partant une possibilité de transparence et d'ouverture.*
[26] *Travail effectué par le miner pour deviner un nombre pseudo-aléatoire, qui doit produire un résultat correspondant à diverses conditions ; une fois le résultat trouvé, les autres nœuds doivent en vérifier la validité. Chaque bloc validé contient un bloc comprenant lui-même le travail effectué par le miner, d'où le terme de "Proof-of-Work". "La preuve de travail", 6 décembre 2018, Binance Academy.*

lui-même le réseau contre les attaques, car il faudrait une immense puissance de calcul dont le coût serait supérieur au bénéfice. En revanche, le consensus par PoW est très énergivore : le *mining* demande un matériel informatique coûteux, et une quantité d'électricité considérable pour la capacité de calcul comme pour le refroidissement des moteurs.

C'est pour répondre aux limites de la Proof-of-Work que l'algorithme de consensus « Proof-of-Stake » (PoS) a été construit. Les chaînes en Proof-of-Stake ne dépendent plus directement du mining, mais d'un système de mise en jeu : *« Les validateurs PoS sont sélectionnés en fonction du nombre de coins qu'ils s'engagent à mettre en jeu*[27]*»*. Plus la mise des validateurs est importante, plus grande est leur chance d'être choisis comme validateurs du bloc. Moins énergivore et moins coûteux, cet algorithme ne nécessite qu'un investissement indirect et un engagement du validateur. Ethereum, deuxième crypto-monnaie en popularité, déploie actuellement cet algorithme, avec les difficultés posées par l'échelle de sa blockchain et le nombre de contributeurs.
La preuve de mise en jeu peut aussi être déléguée via le Delegated Proof-of-Staking (DPoS), qui construit un système de tiers de confiance dans l'algorithme. Le DPoS permet ainsi à des utilisateurs simples de signaler leur soutien via d'autres participants plus importants dans le réseau, qui prennent un statut de dépositaires de la confiance des utilisateurs simples, *« qui effectuent les actions au nom des utilisateurs lors d'événements décisionnels »*, à la manière d'un trust.
Les validateurs délégués — qui constituent les nœuds — sont les « gros » usagers qui gèrent les opérations majeures ainsi que la gouvernance globale du réseau blockchain. Ces usagers ont une participation décisive aux processus construction du consensus et définissent les modalités de gouvernance. Étant donnée la moindre centralité du *mining* dans la PoS, cette évolution algorithmique tend à abaisser les barrières à l'entrée des écosystèmes de blockchain et de crypto-monnaies.

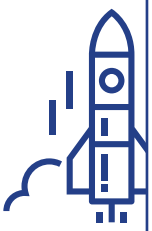
Le troisième mécanisme de consensus, le Proof-of-Authority (PoA), en cours d'expérimentation, repose sur la réputation. L'algorithme de Proof-of Authority ne met plus seulement en jeu les fonds (coins) de l'usager, mais la validité de son identité ; la sécurisation se fait alors par les nœuds (gros usagers) qui sont sélectionnés lorsqu'ils ont déjà fait la preuve de leur identité et sont donc déjà considérés comme dignes de confiance. En mettant en jeu la validité de l'identité de l'usager, cet algorithme pose la question de la légitimité des gros usagers de la blockchain. Ainsi, *« Le modèle de preuve d'autorité repose sur un nombre limité de validateurs de blocs, ce qui en fait un système hautement scalable. Les blocs et les transactions sont vérifiés par des participants pré-approuvés, qui jouent le rôle de modérateurs du système.*[28]*»*

Des réserves émergent à propos du PoA : cet algorithme est-il un renoncement à la décentralisation, esprit fondateur de la blockchain ? En effet, l'exigence d'identité réelle et authentifiée, les obstacles (fonds et réputation) pour devenir validateur et les normes d'approbation sont autant de critères qui orientent le PoA vers une certaine centralisation vers des acteurs ayant les moyens de dépasser ces obstacles, acteurs institutionnels ou grandes entreprises. De fait, le faible nombre de nœuds dans une chaîne en PoA est adapté à l'échelle des réseaux d'entreprises et autres réseaux privés, dans lesquels un certain niveau de confiance existe déjà parmi les membres. Autrement dit, l'algorithme de PoA est déjà adapté pour des solutions d'entreprise fonctionnant déjà sur une blockchain privée, ou pouvant se mettre à niveau avec leur Intranet[29].

[27] *"Qu'est-ce que le staking ?" 22 septembre 2019, Binance Academy .*

D'autres y voient des cas d'usages moins restreints. C'est le cas d'Olivier Dion, CEO de Onecub et cofondateur de aNewGovernance, qui discerne par exemple dans le mécanisme de Proof-of-Authority un support technique pour les *digital territories* (villes, régions ou États), c'est à dire des projets d'écosystèmes de données numériques des instances démocratiques locales. La sécurité et l'authenticité apportées par cet algorithme pourraient servir à élire des représentants, à multiplier les scrutins, et prendre en compte la demande persistante de démocratie fluide et directe.

L'évolution des algorithmes vers la distribution des preuves de confiance souligne le caractère crucial de la gouvernance des infrastructures. En effet, il est question de traduire technologiquement les principes de neutralité, d'égalité des voix, de consensus et de décision unanime dans le cas de l'exécution d'une transaction ou la suppression de données. Centralité de la gouvernance donc, mais aussi des architectures algorithmiques qui, en exécutant les requêtes produites par une gouvernance décentralisée et transparente, permettent par exemple l'émergence de services publics citoyens.



ENCOURAGER/ACCÉLÉRER LA MISE EN PLACE DE « DIGITAL TERRITORIES » POUR OUVRIR, FLUIDIFIER ET PROTÉGER LE PARTAGE DES DONNÉES LOCALES ENTRE POUVOIRS PUBLICS, ENTREPRISES ET CITOYENS

Les « digital territories » sont des projets d'écosystèmes de données liés à un territoire. Leur fonction est d'aider à la création de valeur en aménageant le partage de données des écosystèmes locaux, en protégeant les droits numériques des citoyens, et en empêchant la constitution de monopoles dans les affaires. Cette modalité de partage et de protection des données pourrait s'appliquer à l'amélioration de la politique de RSE des entreprises.

Autre cas d'usage, la mise en place d'un jumeau numérique des structures démocratiques locales pourrait oeuvrer à ramener les usagers vers l'activité démocratique et participative en servant de support régulier pour les consultations locales. La sécurisation et la légitimité du processus pourraient par exemple se faire sur une blockchain en algorithme de Proof-of-Authority.

L'ÉMERGENCE DES SERVICES PUBLICS CITOYENS

Le confinement et la pandémie ont aussi permis la consécration de services publics citoyens dans un esprit de délégation de l'innovation grâce à l'open data. Des projets citoyens comme ViteMaDose, CovidTracker et Covidliste ont vu le jour à partir du printemps 2020 grâce à la politique d'ouverture des données du gouvernement.

Le cas de Covidliste est éloquent puisqu'outre le tweet du Président de la République du 6 mai 2021 faisant la promotion du site, le gouvernement a attribué une subvention de 35 000 euros à ce service. En mai 2021, Covidliste était utilisé par 2 100 centres de vaccination grâce entre autres à la publicité réalisée par le gouvernement. Si elles n'ont pas vocation à remplacer

[28] *"Qu'est-ce que la preuve d'autorité ?", 8 décembre 2018, Binance Academy.*
[29] *"Proof of Authority explained", Dimitar Bogdanov, 3 août 2021, Limechain.*

l'action de la puissance publique, ces innovations citoyennes la complètent et témoignent de l'importance de disposer d'infrastructures adaptées permettant le développement de telles initiatives numériques. Certains considèrent d'ailleurs que si *« de tout temps, il existait un engagement citoyen, ce qui est nouveau avec les outils numériques, c'est qu'une personne dans son salon peut toucher rapidement des millions de personnes.*[30]»

Les innovations venant souvent du privé, l'État doit en revanche veiller à favoriser leur création et leur diffusion en mettant à disposition des ressources et infrastructures, en premier lieu les données publiques utiles à l'innovation d'intérêt général, des espaces d'expérimentation ou encore des partenariats de distribution de l'innovation à travers les services publics traditionnels.

LES SERVICES PUBLICS CITOYENS DU COVID

Figure de proue de cette lame de fond, Guillaume Rozier, le cofondateur des services CovidTracker (open data sur la pandémie) et ViteMaDose (outil de recherche de créneaux de vaccination) incarne cette nouvelle génération d'entrepreneurs citoyens.

D'autres alchimistes de la data ont émergé durant la crise sanitaire, comme Germain Forestier (site éponyme) et Guillaume Saint-Quentin (Meteo-Covid), dont le succès de leurs sites amateurs n'aurait pas été possible sans la politique d'ouverture des données menée par le ministère de la Santé. En ouvrant plusieurs jeux de données, comme celui des eaux usées, l'administration a permis de développer ces outils innovants, utiles pour tous.[31]

Notre think-tank a été précurseur sur ces questions en publiant dès 2018 *"Le Service Public Citoyen"* avec Paul Duan.

Cofondateur de Bayes Impact, une ONG qui utilise l'intelligence artificielle et le Big data afin de répondre à des problématiques sociales, Paul Duan confirme que : *« l'ère post-Covid a été un catalyseur de confiance via les services publics citoyens. Il y a un grand décalage entre la volonté de sens, la capacité entrepreneuriale, et de l'autre côté la capacité des institutions à savoir utiliser la multitude*[32]*».*

Ce constat n'est pas sans rappeler le débat sur l'agilité et la rapidité des citoyens à s'organiser pour répondre à des problématiques de société. La période que nous venons de vivre a été révélatrice de la façon dont nous faisons confiance aux différents interlocuteurs dans le cadre de la transmission d'informations : de manière générale, les citoyens ont davantage fait confiance aux chiffres de CovidTracker qu'à ceux de l'État, alors que dans les deux cas les données collectées, analysées et publiées sont issues de Santé Publique France. Cet exemple renvoie une nouvelle fois à la méfiance que peuvent inspirer les institutions. Une méfiance liée le plus souvent à l'inertie dont ces institutions sont accusées de faire preuve sur des sujets pourtant cruciaux.

[30] *"Citoyens-Covid : la puissance de la société civile numérique", La Net Scouade, 22 mai 2021.*
[31] *L'ouverture des jeux de données par les administrations est l'objet de la pour une République numérique , dite loi Lemaire https://www.vie-publique.fr/eclairage/20301-loi-republique-numerique-7-octobre-2016-loi-lemaire-quels-changements*
[32] *Audition de Paul Duan par le comité de pilotage du rapport.*

L'ÈRE POST-COVID A ÉTÉ UN CATALYSEUR DE CONFIANCE VIA LES SERVICES PUBLICS CITOYENS. IL Y A UN GRAND DÉCALAGE ENTRE LA VOLONTÉ DE SENS, LA CAPACITÉ ENTREPRENEURIALE, ET DE L'AUTRE CÔTÉ LA CAPACITÉ DES INSTITUTIONS À SAVOIR UTILISER LA MULTITUDE"

Paul Duan, *fondateur de Bayes Impact.*

UN SERVICE PUBLIC CITOYEN DE LA JUSTICE ?

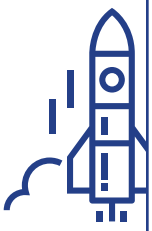
Aux États-Unis, une ONG a développé au début des années 2010 une plateforme nommée Callisto, visant à répertorier les plaintes des victimes d'agressions sexuelles sur les campus, mais aussi et surtout à mettre ces victimes en relation avec des avocats, et si elles le souhaitent entre elles.

L'objectif affiché : éviter « l'effet pingouin », ou le principe d'inertie excessive qui se traduit par l'incapacité de prendre une initiative si personne n'est allé dans ce sens auparavant. Callisto fonctionne comme une plateforme construite sur un système de « hashs cryptographiques », qui fait que chaque déclaration est scellée, et ne peut être décryptée que par une personne qualifiée (conseiller légal, avocat assigné au cas), de manière confidentielle ; soit lorsque deux déclarations mentionnent le même agresseur présumé.

Tant qu'il n'y a pas « match » entre plusieurs plaintes et un agresseur présumé, les déclarations sont totalement cryptées, et donc garanties secrètes. Cette méthode, qui ne repose pas sur la blockchain, permet de savoir si deux contenus sont identiques sans avoir à les décrypter a priori.

Dans ce cas de figure, la multitude — en l'occurrence les personnes victimes d'agressions sexuelles — comble technologiquement un déficit de confiance envers les autorités publiques : en l'occurrence deux institutions régaliennes qui devraient naturellement inspirer la confiance, la police et la justice. Aux États-Unis, lors du lancement de Callisto, une étudiante sur cinq déclarait avoir déjà subi une agression sexuelle, alors que seulement 11 % d'entre elles l'avaient rapportée aux autorités éducatives ou à la police.

Le succès de telles plateformes est toutefois tributaire de la reconnaissance d'une autorité perçue comme légitime par le plus grand nombre. Comme l'explique Paul Duan, *« il faut qu'il y ait un acteur qui soit en mesure de garantir un certain nombres de principes (neutralité, universalité). La notion de confiance est indissociable de la notion de principes qu'il faut définir en fonction de l'enjeu. Il est nécessaire que les gens aient confiance en cette expertise pour la rendre concrète via la dimension participative, la multitude. Cela implique les notions de transparence, de mise en commun.*[33]»



FÉDÉRER LA MULTITUDE ET LES TIERS DE CONFIANCE PUBLICS

La plateforme d'éveil d'enfants 1001 mots dans l'éducation, qui rassemble chercheurs en neurosciences cognitives et en santé publique, orthophonistes, psychologues, mais aussi le secteur public, ou encore de Covidom, plateforme de télésurveillance de patients suspectés d'avoir contracté le Covid-19 élaborée en collaboration avec l'AP-HP, sont autant d'exemples qui montrent la pertinence d'un travail conjoint entre la multitude et un tiers de confiance public.

Ce constat pourrait d'ailleurs être amené non pas à devenir la norme, mais du moins à s'accélérer dans les années à venir pour répondre au grand défi de nos sociétés démocratiques occidentales, à savoir la perte de confiance dans nos institutions, notamment régaliennes.

Faire confiance à l'énergie de la multitude et à la légitimité des tiers de confiance publics pour construire ensemble des infrastructures de confiance apparaît comme une solution de ré-oxygénation à la fois sur le plan économique et opérationnel, mais aussi du point de vue de l'évolution des régimes démocratiques au XXIe siècle. Par ailleurs, ouvrir la gouvernance des architectures minimise le risque de dépendance à des gestionnaires extérieurs, et participe donc résolument à l'autonomie stratégique des infrastructures numériques. En d'autres

[33] *Audition de Paul Duan par le comité de pilotage du rapport.*

termes, la gouvernance multipartite apparaît comme une solution de souveraineté partagée des architectures. Mais cette solution d'ouverture dans la politique numérique ne saurait faire l'économie d'une défense active de nos intérêts : défense technologique et cyber, mais aussi défense économique de nos acteurs nationaux et leur implantation territoriale.

II. DÉFENDRE NOS INTÉRÊTS

1. DÉFENDRE, C'EST SÉCURISER TECHNOLOGIQUEMENT

La dimension numérique a considérablement transformé la défense de nos systèmes. La menace est devenue plus diffuse, et plus difficile à identifier : qu'il s'agisse d'une attaque intérieure ou extérieure, d'un particulier ou d'un État, la réponse sera différente. Dans les deux cas, les cibles doivent être capables de résilience, en particulier s'il s'agit d'une infrastructure dont dépendent de nombreux services essentiels à la continuité de nos activités.

Un élément déterminant de la résilience d'une infrastructure numérique demeure dans la capacité à protéger les données qui circulent sur les nouvelles autoroutes de l'information[34]. À l'instar du fonctionnement des infrastructures routières, il est important qu'il y ait des règles claires et des protections pour les utilisateurs pour permettre une utilisation par tous, dans une logique visant à instaurer un climat de confiance.

Les menaces sur un réseau numérique sont moins palpables, mais les conséquences sont bien réelles : rançongiciels, programmes malveillants, attaques par déni de service, ou encore hameçonnages. Ces cyberattaques peuvent causer le piratage de données, le gel d'activité, voire dans certains cas la destruction d'une activité en captant des données sensibles (brevets, contrats) ou en sabotant l'infrastructure même. Comme l'explique Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), si les infrastructures physiques sont des cibles, il est également nécessaire de prendre garde aux structures purement numériques comme le cloud, qui est l'archétype de l'infrastructure numérique qui crée un effet systémique très fort en cas d'attaque[35].

Chaque année dans le monde, près d'un milliard de personnes sont concernées par une cyberattaque. 9 français sur 10 ont déjà été confrontés à un acte de cybermalveillance[36] et entre 2019 et 2020, il y a eu quatre fois plus de victimes qui ont fait appel à l'ANSSI par rapport à l'année précédente[37]. Aussi, les cyberharceleurs ne visent plus directement leurs cibles mais recherchent des moyens de les atteindre indirectement par les services intermédiaires.

Avec la crise sanitaire et le confinement, les manières de consommer et de travailler ont été bouleversées, avec un usage renforcé des outils numériques ; cette période a définitivement convaincu les dirigeants d'entreprises de la pertinence du digital dans la bonne conduite dans leurs affaires.

L'accélération de la digitalisation des entreprises, des nouvelles habitudes de consommation et le développement des projets de smart territoires nécessitent d'appréhender la cybersécurité comme un défi majeur. Plusieurs organes publics assurent déjà ce type de missions, que ce soit l'ANSSI pour celles relevant de la défense des systèmes d'information de l'État et de conseil et de soutien aux administrations et aux opérateurs d'importance vitale, ou bien le groupement d'intérêt public Action contre la Cybermalveillance (GIP ACYMA), issu de la Stratégie numérique du Gouvernement.

Cette volonté de territorialiser la cybersécurité rencontre une volonté politique souhaitant

[34] *Audition de Fabrice Koszyk et de Margot Corréard par le comité de pilotage du rapport.*
[35] *Audition de Guillaume Poupard par le comité de pilotage du rapport.*
[36] *https://www.cyberocc.com/sinformer/quelques-chiffres/*
[37] *"Quatre fois plus de cyberattaques en un an en France selon l'Agence nationale de la sécurité des systèmes d'information", France TV Info, 10 juin 2021.*

faire de chaque territoire un territoire attractif en combinant intelligence territoriale, inclusion sociale, valeurs écologistes et innovation technologique par la mise en œuvre de nouveaux usages et services numériques nécessaires à leur développement.

L'ambition portée par les élus, notamment régionaux et départementaux, est de proposer aux établissements publics de coopération intercommunale (EPCI) et aux villes moyennes de les accompagner vers leur transition numérique, en plaçant la Région et le Département comme renfort d'ingénierie. Il s'agit également de mobiliser les réseaux d'initiative publique THD comme leviers du développement de projets numériques structurants et innovants pour les territoires.

LE PROJET "SMART'EST"

Avec le programme « Smart'Est », la Région Grand Est et la Banque des Territoires souhaitent évaluer simplement le degré de maturité numérique d'une collectivité à partir d'un questionnaire en ligne interactif à compléter et modifier à tout moment de manière sécurisée. Il est aussi question de recenser, partager des projets numériques portés par une collectivité et accéder à un référentiel d'initiatives développées par d'autres collectivités ou acteurs (publics ou associatifs) du territoire ou à l'échelle régionale, dans une logique d'échange de bonnes pratiques et de mise en réseau des acteurs impliqués en région Grand Est.

La nécessaire sécurisation des technologies numériques doit donc s'accompagner d'un renforcement de la concertation entre les différents acteurs publics et privés impliqués sur ces enjeux et conduire à des réflexions sur les contraintes opérationnelles concernant l'hébergement des données, notamment les données sensibles.

LA CYBERSÉCURITÉ, DÉFI MAJEUR

La notion d'infrastructure numérique critique doit être étendue à plusieurs domaines. Préalablement aux enjeux de sécurité de l'ANSSI, il existait déjà une formalisation des secteurs d'activités d'importance vitale qui étaient identifiés. Cette liste répondait à des raisons de sécurité nationale face à des menaces classiques à laquelle ont été ajoutées de nouvelles exigences visant à prendre en compte le risque cyber.

La France a été le premier État européen à en poser les principes dans l'article 22 de la loi de programmation militaire de 2013, qui impose désormais aux opérateurs d'importance vitale (OIV) de renforcer la sécurité des systèmes d'information qu'ils exploitent. Cette règle s'est depuis généralisée au niveau européen avec la directive Network and Information System Security (NIS) qui poursuit un objectif essentiel : assurer un niveau de sécurité élevé et commun pour les réseaux et les systèmes d'information de l'Union européenne.

La directive est aujourd'hui en révision dans le cadre de la stratégie européenne en matière de cybersécurité pour la décennie numérique, laquelle a pour ambition de *« façonner l'avenir numérique de l'Europe »*, en même temps que la Commission européenne a adopté une proposition de directive sur la résilience des entités critiques. La Commission européenne souhaite élargir le champ d'application de la directive NIS (énergie, transport, banques,

infrastructures financières de marché, santé, eau potable et infrastructures numériques) en ajoutant de nouveaux secteurs d'activité en fonction de leur importance pour l'économie et la société compte tenu de leur taille. La proposition de directive NIS 2 complète les exigences de sécurité imposées aux entreprises « essentielles » et « importantes ».

Faire de la cybersécurité un défi majeur implique de mobiliser un ensemble d'acteurs hétéroclites et de travailler de façon transverse. Pour Jean-Guy de Ruffray, avocat-associé chez Altana, « *être capable d'assurer cette cybersécurité est un enjeu fondamental pour les territoires et pour la création d'infrastructures de confiance. Cela passe par une nécessaire concertation des acteurs*.»[38] Les grands groupes, les start-ups et les administrations ont certes des besoins différents, mais ont en commun cette impérieuse nécessité de cybersécurité.

Pour Guillaume Poupard, si la France veut être dans le premier cercle des États forts en matière de cybersécurité, il est nécessaire de fédérer les actions pour être souverain. La France ne peut pas rivaliser avec des pays comme les États-Unis d'un point de vue budgétaire, mais dispose en revanche d'une multitude de ressources qualifiées pouvant travailler à un but commun. Cette action peut être une caisse de résonance dans l'espace européen et s'inscrit dans une logique de politique publique visant à renforcer la notion de souveraineté européenne.

La certification est un autre chemin permettant de répondre aux nouvelles exigences de cybersécurité. En pratique, il est impossible pour n'importe quel acteur privé de savoir qui est compétent et digne de confiance ; des mécanismes d'évaluation et de certification par des autorités publiques légitimes permettent de transférer la confiance. En certifiant, l'État français se porte ainsi garant du service. La certification a également été européanisée avec des schémas à l'échelle continentale pour éviter un morcellement qui serait préjudiciable à tous, à commencer par les industriels qui proposent des solutions et des services, mais également pour les usagers qui en bénéficient.

L'ANSSI a de son côté fait part de son souhait que les offres de cloud qualifiées en France intègrent l'immunité au droit américain. La volonté affichée ici est de protéger l'espace européen face aux ambitions intrusives de certains acteurs étrangers. En parallèle de cette action à l'échelle nationale, l'Agence travaille également sur le plan européen afin de mettre en place une certification cloud européenne. La certification apparaît ainsi comme un instrument incontournable pour aider les citoyens, les entreprises et les pouvoirs publics à identifier les organisations et les services les plus fiables en termes de sécurité.

Il s'agit d'un dispositif d'autant plus pertinent aujourd'hui que l'augmentation des usages numériques liée à la crise sanitaire s'est accompagnée d'une hausse de la cybercriminalité. Refondue début 2020, la plateforme cybermalveillance.gouv.fr a connu une forte hausse de sa fréquentation (+155 % par rapport à 2019) avec plus de 1,2 million de personnes qui ont visité ses contenus et ses alertes. Lors des premières semaines de confinement au printemps 2020, les visites ont même atteint un pic de près de 600 %. Comme les années précédentes, les particuliers ont représenté plus de 90 % du public en recherche d'assistance.[39]

Outre le hameçonnage, le piratage de compte en ligne (12 %) et les arnaques au faux support technique (11 %) complètent le podium des recherches d'assistance effectuées par les particuliers sur la plateforme cyber du gouvernement. Les demandes provenant de publics

[38] *Audition de Jean-Guy de Ruffray par le comité de pilotage du rapport*
[39] *Quatre fois plus de cyberattaques en un an en France, selon l'Agence nationale de la sécurité des systèmes d'information, France TV Info, 10 juin 2021.*

“ÊTRE CAPABLE D'ASSURER CETTE CYBERSÉCURITÉ EST UN ENJEU FONDAMENTAL POUR LES TERRITOIRES ET POUR LA CRÉATION D'INFRASTRUCTURES DE CONFIANCE. CELA PASSE PAR UNE NÉCESSAIRE CONCERTATION DES ACTEURS.”

Jean-Guy de Ruffray, *avocat-associé chez Advant Altana*

professionnels (entreprises, collectivités, administrations etc.) ont également progressé de 20 % pendant cette période.[40]

Ce constat est à mettre en parallèle avec le principe de « privacy by design », soit la protection des données dès la conception. Cela signifie que l'entreprise ou n'importe quelle autre structure comme une collectivité, doit désormais intégrer la protection des données à caractère personnel dès la conception de projets rattachés à leur traitement. L'application de ce principe permet donc, dans l'architecture même, de mettre en œuvre des mesures préventives permettant de limiter les risques.

Enfin, selon le GIP ACYMA, 159 collectivités locales ont été la cible d'un piratage en 2020, soit une augmentation de plus de 50% par rapport à l'année 2019. Des chiffres qui peuvent s'expliquer par le manque d'acculturation en matière de cybersécurité au niveau des collectivités territoriales, en dépit de l'obligation de désigner un délégué à la protection des données (DPO), inscrite dans le RGPD. Spécialiste des enjeux de protection des données, l'avocat Jean-Guy de Ruffray a toutefois précisé lors de son audition qu'il était difficile de trouver le bon profil car un DPO est autant un juriste qu'un technicien, même s'il existe des formations qui s'ouvrent spécifiquement pour cela.[41] La CNIL a d'ailleurs beaucoup servi de fournisseur de DPO pour de nombreux acteurs privés ou publics, et met de plus en plus à disposition des "sand box" (accompagnement renforcé pour les écosystèmes) mettant à disposition des profils de la CNIL pour les sujets data d'intérêt général les plus innovants.

Enfin, plus les traitements de données se multiplient, plus les surfaces sont grandes et donc plus les points d'entrée sont importants. Cette multiplication des failles évolue en parallèle avec le caractère essentiel de certains services publics qui concernent la circulation, l'éclairage public ou encore les écoles et les hôpitaux.

LES HÔPITAUX, CIBLES DES CYBERATTAQUES DURANT LA CRISE SANITAIRE

Les hôpitaux ont été largement frappés en 2020. Le CHU de Rouen, celui de Dax, le groupement hospitalier de territoire de Dordogne ou encore l'hôpital de Villefranche-sur-Saône dans le Rhône ont été totalement paralysés pendant plusieurs semaines du fait d'attaques par rançongiciels. Alors que la pandémie du Covid-19 a définitivement démontré que les hôpitaux sont des opérateurs de service essentiels (OSE), 135 groupements hospitaliers français ont été rajoutés à la liste des OSE. Cette désignation intervient au moment où plusieurs dizaines de laboratoires médicaux ont été frappés par une cyberattaque et qu'un fichier contenant 500 000 données de patients a été mis en vente sur le darkweb à la fin 2020[42]. De nombreuses informations sensibles sont disponibles dans ce fichier : le numéro de sécurité sociale, le groupe sanguin, la date de naissance, l'adresse, le numéro de téléphone portable ou encore le médecin prescripteur.

À la lecture de ces éléments, des *« approches sectorielles et régionales sont nécessaires »*, selon Guillaume Poupard, lequel milite pour trois maillages de cybersécurité en France : national, régional et départemental. Pour une meilleure coordination des actions, ces différents niveaux devront travailler ensemble, être interconnectés alors que devrait être centralisé ce qui doit l'être. Ces entités œuvrent dans un but commun de cybersécurisation, certes à des niveaux différents mais les conséquences sont également communes. Si demain un territoire est

[40] https://www.cyberocc.com/sinformer/quelques-chiffres/
[41] Audition de Jean-Guy de Ruffray par le comité de pilotage du rapport.
[42] Fuite de données médicales de 500 000 Français : la CNIL n'a pas été alertée", Numerama, 24 février 2021.

touché par une cyberattaque causant un dysfonctionnement des infrastructures numériques, la réponse devra être collective pour assurer une résilience des services.

L'approche sectorielle permettrait de mettre autour de la table des acteurs de terrain différents quand l'approche régionale s'effectuerait en collaboration avec les conseils régionaux. L'idée ici serait de développer les Computer Emergency Response Team (CERT), c'est à dire des équipes opérationnelles qui gèrent les vulnérabilités à l'échelle régionale.

PROPOSITIONS

CRÉER UN SERVICE INTERCOMMUNAL DE CYBERSÉCURITÉ (SIC) SUR LE MÊME MODÈLE QUE LE SERVICE DÉPARTEMENTAL D'INCENDIE ET DE SECOURS (SDIS)

Présent dans chaque département, le service d'incendie et de secours est chargé de la prévention, de la protection et de la lutte contre les incendies. Il concourt, avec les autres services et professionnels concernés, à la protection et à la lutte contre les autres accidents, sinistres et catastrophes, à l'évaluation et à la prévention des risques technologiques ou naturels ainsi qu'aux secours d'urgence. Alors que la plupart des élus locaux et des chefs d'entreprises ne sont pas acculturés aux risques de cybersécurité et à leur conséquence, la création d'un SIC viserait à répondre aux besoins de cybersécurité des territoires les plus démunis. Celui-ci s'appuierait sur le schéma directeur territorial d'aménagement numérique (SDAN) qui viendrait structurer ses missions et son périmètre d'intervention en lien avec la feuille de route numérique élaborée par l'intercommunalité. Enfin, les conseillers numériques pourraient être mobilisés le cas échéant pour ce type de mission, en plus de celles qui leur incombent déjà (inclusion numérique et sobriété numérique). La mise en place de ce type de service, qui serait coordonné par les Régions, cheffes de file en matière de cybersécurité et dans une logique de péréquation entre les territoires, pourrait par ailleurs permettre une plus grande entraide entre les communes.

ACCOMPAGNER LES ÉLUS PAR UN PROGRAMME DE FORMATION CONTINUE SUR LA CYBERSÉCURITÉ

L'Institut des Hautes Études de Défense Nationale (IHEDN) a récemment mis sur pied un module de formation intitulé « Souveraineté numérique et cybersécurité ». Celui-ci a pour objectif de sensibiliser et former les auditeurs à ces sujets qui sont un facteur de préoccupation grandissante pour les pouvoirs publics et les acteurs économiques. Alors que les collectivités doivent s'adapter pour faire face à la multiplication de menaces de plus en plus sophistiquées, la diffusion des bonnes pratiques implique des efforts de formation. En effet, l'élaboration d'une vision stratégique « cyber » est désormais une nécessité, tant pour les élus que pour les services concernés au sein des collectivités.

CRÉER UNE PLATEFORME DE MISE EN RELATION ENTRE INSTITUTIONS PUBLIQUES ET/OU PRIVÉES AYANT SUBI UNE CYBERATTAQUE, GARANTISSANT LEUR ANONYMAT

Sur le même modèle que Callisto aux États-Unis, il s'agit de créer une plateforme via un système de "hashs cryptographiques", qui fait que chaque déclaration est scellée, et ne peut être décryptée uniquement par une personne qualifiée de manière confidentielle ; soit, lorsque deux déclarations mentionnent le même type de cyberattaque. Cette personne qualifiée pourrait ainsi être le service local de cybersécurité. Pour mémoire, lorsqu'une institution publique ou privée est victime de cyberattaque, il est toujours difficile pour elle de reconnaitre cette intrusion, au regard des dégâts en termes de notoriété que cela peut engendrer.

LE NÉCESSAIRE RENFORCEMENT DE LA SÉCURITÉ DES SITES (PYLÔNES, DATACENTERS, ETC.)

La sécurisation des technologies numériques doit s'accompagner d'un renforcement des sites stratégiques. Cet impératif de sécurisation est formalisé dans l'arrêté du 2 juin 2006 qui désigne les télécommunications parmi les secteurs d'activité d'importance vitale. Or les réseaux numériques participent désormais pleinement à la production et à la distribution de biens ou services indispensables à l'économie et à la sécurité de la Nation.[43]

LES ANTENNES 5G ET LES PYLÔNES PRIS POUR CIBLES

Les dégradations volontaires des pylônes en Europe occidentale se multiplient, notamment en France : 70 antennes relais ont été vandalisées sur le territoire national en 2020[44]. Dans un autre registre, l'incendie du site OVH à Strasbourg et ses conséquences sur certains services essentiels en période de pandémie (certaines écoles et universités ont eu du mal à assurer leurs cours à distance) témoigne de la nécessité pour les pouvoirs publics de se saisir de cet enjeu autour des installations matérielles.

Cette assertion prend d'autant plus de sens que la pandémie liée au Covid-19 a vu se multiplier ce type d'attaques sur fond de théories complotistes. Nombre de pétitions en ligne continuent de faire la promotion d'une lubie affirmant que les symptômes du coronavirus sont causés par des antennes 5G.

En France, près d'une centaine d'incendies de sites de réseau 5G ont été déclarés en 2020, entraînant l'interpellation d'une trentaine de personnes par les forces de l'ordre. D'autres types d'antennes sont également la cible d'activistes à l'instar de l'émetteur TNT TDF de Limoges-Les Cars qui a été incendié au mois de décembre 2020[45]. Dans ce cas précis, la conséquence principale n'a eu aucun impact sur le ralentissement du déploiement de la 5G — dont le développement est embryonnaire en Haute-Vienne —, mais a privé de télévision et de radio 1,4 million d'habitants.

Jean-Baptiste de Scorraille, adjoint au maire de Toulouse en charge des antennes radio et de téléphonie, concède sur ce sujet qu'*« il ne faut rien laisser passer au regard de l'importance que relève ces infrastructures »*, indiquant que *« sur ce sujet, on ne peut pas dire que l'État abandonne les collectivités »*. L'élu s'interroge par ailleurs sur la possibilité d'envisager des infrastructures de nouvelle génération qui soient inatteignables et milite pour cette *« logique sur laquelle nous devons nous orienter »*. Que l'aléa provienne d'un groupe d'individus ou d'une avarie matérielle, la sécurité des sites devient un enjeu pressant à mesure que nous dépendons des services qui y sont abrités.

L'incendie du site OVH de Strasbourg (printemps 2021) a en effet démontré toute la nécessité de repenser la sécurité et la vulnérabilité de ces infrastructures, en intégrant la possibilité de leur disparition physique.
L'incident d'OVH n'est pas resté sans conséquences puisque les appels d'offres portant sur la colocation d'espaces de centre de données requièrent désormais des informations sur l'assurance de l'infrastructure, mais aussi des certifications d'assemblée plénière de sociétés d'assurances dommages (dite certifications APSAD) ; ces certifications imposent des exigences précises en termes de détection d'incendie (certification APSAD R7) et d'extinction automatique (certification APSAD R13).

[43] *"La protection des réseaux numériques en tant qu'infrastructures vitales", Bertrand Warusfel, Sécurité et stratégie, 2010.*
[44] *"L'inquiétant boom des destructions d'antennes relais", Europe 1,19 janvier 2021.*
[45] *"L'incendie du relais des Cars revendiqué par des anti-5G auprès du Populaire du Centre", Jean-Louis Mercier, Le Populaire du Centre, 12 janvier 2021.*

Cette actualité a enfin soulevé deux sujets sous-jacents jusqu'ici peu pris en compte par les principaux concernés que sont les acteurs du cloud computing et les utilisateurs : d'une part la localisation de l'endroit où sont stockées les données, notamment pour des considérations sécuritaires et de souveraineté ; d'autre part, l'impact environnemental qu'implique l'installation de telles infrastructures numériques.

Les datacenters apparaissent également comme des sites dont la sécurité doit être renforcée au regard de l'importance stratégique qu'ils revêtent. Là encore, l'actualité de ces derniers mois est venue nous rappeler à quel point ces datacenters sont devenus incontournables dans la gestion et la circulation de nos données, publiques ou privées, sensibles ou non.

Une vigilance à mettre en parallèle avec l'interrogation de Jean-Guy de Ruffray sur la capacité de la France et de l'UE d'être en mesure de préserver la souveraineté et la sécurité des données traitées par une entité publique ou privée alors que son prestataire est une entreprise de nationalité extra-européenne, quand bien même les données sont hébergées en France ou en Europe. D'après Sébastien Duré, directeur général d'Hoppen (solutions connectées pour les établissements de santé), c'est la raison pour laquelle beaucoup d'acteurs du secteur de la santé hébergent leurs données au sein de leurs propres structures. Ce choix est motivé par des contraintes opérationnelles où certains systèmes sont déjà présents dans les hôpitaux, mais aussi par la volonté des directeurs des systèmes d'information (DSI) de conserver ces données au sein de l'hôpital : *« Avec un cloud extérieur, les DSI considèrent perdre le contrôle sur la donnée car elle serait moins sécurisée. Il est nécessaire d'apporter de la confiance à ces interlocuteurs car le cloud apporte plus d'efficacité que les serveurs internes[46]».*

LE CAS HUAWEI

Le cas de Huawei et de façon générale des BATX chinois est particulièrement éclairant, car le passage à la 5G implique un renouvellement des équipements de réseau avec des antennes adaptées. L'opérateur chinois est actuellement le 1er équipementier en 5G et possède 40 % des parts de marché en Europe. Ses marchés ne se limitent pas à la production et à la vente de téléphones portables mais couvrent l'ensemble des équipements nécessaires pour faire fonctionner les réseaux mobiles, depuis les antennes et les serveurs jusqu'aux objets connectés, en passant par les solutions industrielles (cloud, réseaux d'entreprise, solutions pour la gestion énergétique).

Ecarté par la France du cœur des réseaux nationaux de télécommunications et de ses sites sensibles, Huawei fait face depuis des années à des accusations sur sa gouvernance et ses liens supposés avec l'Etat chinois, avec en toile de fond, des soupçons d'espionnage.

A Toulouse, Jean-Baptiste de Scorraille relève que « l'organisation du festival des Lanternes à Blagnac par exemple a été récupérée par une société chinoise47». Le lieu d'implantation de l'évènement, à proximité de l'aéroport de Toulouse-Blagnac, haut lieu de l'écosystème aéronautique français et européen, n'est sans doute pas étranger à cet intérêt.

De fait, si rien ne permet d'affirmer que ni Huawei, ni aucune entreprise chinoise évoquée ici ne participe à de l'espionnage industriel, force est de constater qu'il existe toutefois une crainte liée au déploiement des infrastructures numériques.

[46] *Audition de Sébastien Duré, Cédric Messina et Cédric Denoyel par le comité de pilotage du rapport.*
[47] *Audition de Jean-Baptiste de Scoraille par le comité de pilotage du rapport.*

DES INFRASTRUCTURES DURABLES

L'autre sujet soulevé par la sécurisation des infrastructures numériques concerne leur impact environnemental. D'après l'étude de l'Agence de la transition écologique (Ademe), les datacenters et autres infrastructures de réseau représentent aujourd'hui 53 % des émissions de gaz à effet de serre (GES) générées par le numérique (lui-même représentant 4 % des émissions de GES[48]). Un constat qui implique une mobilisation importante de la part des acteurs du numérique afin de relever les défis du changement climatique. Nos choix en matière d'alimentation des infrastructures conditionnent notre aptitude à respecter les engagements que nous avons pris en adoptant l'Accord de Paris sur climat. Rappelons que l'accélération du déploiement des infrastructures numériques depuis le début des années 2000 s'est accompagnée d'un doublement de la production d'aluminium, alors que l'extraction des métaux rares nécessaires à la production des batteries augmente de façon exponentielle.

C'est donc en s'emparant aussi de cette problématique que la notion de confiance deviendra consubstantielle du numérique, à l'heure où l'impératif écologique entre en tension avec le développement de nos activités, y compris économiques.

À ce titre, alors que les projets d'infrastructures sont de plus en plus efficients énergétiquement et que les opérateurs d'infrastructures souhaitent mutualiser au mieux leurs services de manière à minimiser leur impact environnemental et énergétique, les autorités publiques poussent également vers l'établissement d'un nouveau modèle qui s'inscrit dans l'objectif de durabilité.

C'est le cas de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP), dont la présidente Laure de la Raudière a annoncé dès sa prise de fonction en janvier 2021 vouloir faire de l'environnement le 4e pilier de la régulation des télécoms. C'est aussi le cas des parlementaires, à travers la proposition de loi visant à réduire l'empreinte environnementale du numérique en France est en cours d'examen ; et enfin du Gouvernement via la feuille de route « Numérique et environnement ».

Cette feuille de route, publiée le 23 février 2021, donne un référentiel pour cadrer les actions des acteurs du numérique dans les prochaines années. Elle s'appuie sur 3 piliers :

- Le développement de la connaissance de l'empreinte environnementale numérique pour agir efficacement ;
- Le soutien au numérique plus sobre en réduisant l'empreinte environnementale du numérique ;
- Le numérique comme levier de la croissance écologique.

Ce dernier point est peut-être le plus significatif puisqu'il annonce la volonté des pouvoirs publics de s'appuyer sur les infrastructures numériques pour s'orienter vers une croissance responsable. L'horizon du numérique comme levier de croissance écologique sous-entend entre autres une accélération du déploiement des réseaux énergétiques connectés.

Le déploiement des réseaux électriques intelligents apparaît en effet comme un des facteurs d'une transition énergétique réussie. Les smart grids, qui permettent l'intégration massive des énergies renouvelables et le développement de nouveaux usages individuels et collectifs en matière de consommation d'énergie, ont pour corollaire une réduction des émissions de CO2,

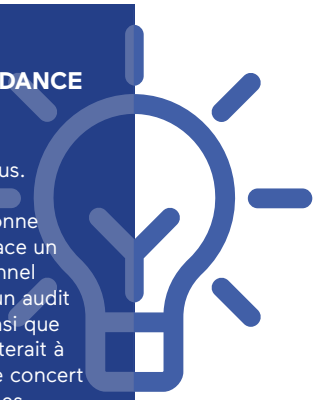
[48] *"La face cachée du numérique", Ademe.*

produites en grande majorité par les villes, particulièrement énergivores. Aussi, les smart grids seront désormais éligibles aux aides du fait de leur intégration au sein de la taxonomie verte. Ainsi le développement des infrastructures numériques doit aller de pair avec une industrialisation durable et permettre de rationaliser la production énergétique pour lutter contre le réchauffement climatique. Il offre ainsi plusieurs éléments de réponse aux objectifs de développement durable énoncés à la fois par les Nations unies dans le cadre de l'Agenda 2030, et de façon plus concrète par le gouvernement à travers la feuille de route « numérique et environnement».

PROPOSITION

ENCOURAGER LA MISE EN PLACE D'AUDIT AUTOUR DE LA FRAGILITÉ DES INFRASTRUCTURES THD ET DE LEUR DÉPENDANCE TECHNOLOGIQUE À DES PAYS TIERS

La crise sanitaire mondiale et le premier confinement ont créé un choc et confirmé, si besoin était, la nécessité d'une connexion numérique pour tous. Sur tout le territoire, pour conserver un lien social, télétravailler, maintenir l'activité économique etc., il est désormais essentiel de disposer d'une bonne connectivité. Alors que le gouvernement a pour ambition de mettre en place un service universel du très haut débit, à l'image du service universel traditionnel des télécommunications, celui-ci pourrait s'accompagner au préalable d'un audit autour de la fragilité des infrastructures THD (pylônes, réseaux filaires) ainsi que de la dépendance technologique à des pays tiers. Cette démarche consisterait à organiser avec des règles et une réglementation adaptée, et à travailler de concert avec les opérateurs concernés, sans dimension contraignante au regard des lourdeurs administratives pouvant en résulter. Elle s'inscrirait enfin dans l'ambition portée par le Président de la République de maîtriser des technologies numériques souveraines et sûres, d'autant que ce sont près de 6 milliards d'euros qui vont être investis pour disposer de composants physiques et électroniques sécurisés, visant à créer les conditions de possibilité pour atteindre ces objectifs. L'accès aux composants électroniques étant présenté comme une priorité, avec pour objectif de « *doubler notre capacité électronique d'ici 2030* ».



2. DÉFENDRE, C'EST PROTÉGER ÉCONOMIQUEMENT

S'intéresser aux infrastructures de confiance revient aussi à appréhender la façon de potentialiser les infrastructures numériques pour protéger le tissu économique national et la cohésion sociale dans les territoires. En bâtissant un écosystème de confiance, nous créons aussi les conditions d'une croissance locale durable.

COMPÉTITIVITÉ DES TERRITOIRES ET DES ENTREPRISES

L'implantation d'une entreprise repose sur un ensemble de critères, parmi lesquels le bassin d'emploi, mais aussi les infrastructures et les équipements, raison pour laquelle un territoire ne peut se développer et rester autonome et attractif s'il ne se modernise pas. La notion d'écosystème est centrale : elle désigne la capacité d'une entreprise à interagir avec son environnement proche au sein d'un même espace. Le Plan France Très Haut Débit participe au renforcement de ces écosystèmes avec l'objectif de *« renforcer la compétitivité de l'économie française et l'attractivité de la France par le raccordement prioritaire en fibre optique des zones d'activités économique[49]».*

Les démarches innovantes liées à la complétude du déploiement numérique du territoire ont pour ambition de repenser son développement en permettant d'une part l'émergence de nouvelles

[49] *Garantir du Très Haut Débit pour tous, Agence nationale de la cohésion des territoires.*

méthodes de co-construction entre les acteurs économiques, et d'autre part de s'orienter vers une croissance économique plus responsable, plus inclusive. La dématérialisation des services publics, l'automatisation des réseaux énergétiques et de transports publics représentent certes un coût pour les élus, mais aussi une opportunité de relancer l'économie en créant de nouveaux emplois et en attirant les télétravailleurs. Tous les territoires sont concernés.

Fabrice Koszyk, directeur général de Serenicity (entreprise de cybersécurité), insiste sur les bienfaits du déploiement des infrastructures numériques dans la Loire, soulignant que le réseau d'initiative publique (RIP) local met à disposition de l'écosystème territorial des infrastructures qui répondent aux besoins des collectivités mais également du tissu économique[50]. Ces infrastructures sont des conditions de l'innovation.

Jean-Michel Mis, spécialiste des questions numériques et député de la deuxième circonscription de la Loire, en est bien conscient d'autant que son département a été précurseur dans la mise en place d'infrastructures numériques. Il existait dans ce territoire un syndicat en charge du réseau électrique qui a su migrer vers le numérique car les élus locaux ont su anticiper les besoins futurs, *« bien que ces actions ne sont pas forcément appréciées à leur juste valeur par les administrés au moment de leur lancement.»*[51] Ce déploiement permet d'attirer des entreprises qui ont des besoins numériques (comme des datacenters) mais également de conserver des entreprises locales qui auraient pu chercher ce besoin ailleurs.

LES INFRASTRUCTURES DE CONFIANCE, FACTEUR D'ATTRACTIVITÉ DES TERRITOIRES

Plusieurs collectivités font la promotion de leur territoire en plaçant la fibre comme un atout majeur pour attirer de nouvelles entreprises et de nouvelles populations, à l'instar du Val d'Oise, l'un des départements bénéficiant d'un des plus importants taux de couverture. Il s'agit d'un avantage comparatif important, que ce soit pour les pouvoirs publics, mais aussi pour le tissu économique local. La fibre demeure en ce sens un critère largement mis en avant, que ce soit par les agences de développement économique territoriales ou les acteurs privés comme les agences immobilières. Dans le cas du Val d'Oise, la Chambre de commerce et d'industrie départementale capitalise sur ce niveau de couverture, au même titre que sur la situation géographique – du fait de la proximité avec Paris – et la connexion qu'offre le territoire avec le reste du monde avec la présence du premier aéroport français et deuxième européen en termes de trafic, l'Aéroport Roissy Charles de Gaulle.

La mise en place d'infrastructures numériques de confiance permet par ailleurs le déploiement de « hubs de l'employabilité », à condition que les pouvoirs publics accompagnent les entreprises et les salariés sur les nouveaux usages. Le modèle qui consiste à se déplacer pour se rendre sur son lieu de travail pourrait évoluer avec la création de lieux intermédiaires, d'autant que le télétravail a créé des contraintes comme la gestion de la vie domestique, la perte de repères mais également l'isolement des télétravailleurs.

Des tiers-lieux à proximité d'infrastructures de transport permettraient de dédier des immeubles de manière polyvalente à plusieurs acteurs. C'est le cas par exemple à Longwy, ville française à la frontière belge et luxembourgeoise, qui crée un « Hub des compétences » pour accompagner les travailleurs transfrontaliers via un programme de formation dans des locaux adaptés à la situation de mobilité sociale et professionnelle de ces habitants.
Cette solution intermédiaire de partage de postes de travail dans un lieu dédié et qui n'est pas

[50] *Audition de Fabrice Koszyk et de Margot Corréard par le comité de pilotage du rapport.*
[51] *Audition de Jean-Michel Mis par le comité de pilotage du rapport.*

un lieu privé a l'avantage de faciliter la vie sociale, de répondre à des enjeux d'infrastructures et de protection des réseaux puisque le télétravail pose une question sur la cybersécurité. La relative nouveauté de l'ampleur du télétravail en France ne permet pas d'affirmer si cette voie sera privilégiée par les entreprises. Certains grands groupes réfléchissent toutefois à une architecture en toile d'araignée plutôt qu'en silos, permettant de moins concentrer les ressources au même endroit.

Malgré la volonté d'appréhender le territoire comme créateur de valeurs, dans certaines régions le manque d'infrastructures affecte la production. Si *« dans le territoire ligérien, les entreprises restent dans le département car il y a des connexions et des réseaux*[52]*»* à l'inverse en Centre-Val de Loire — et plus particulièrement dans le département du Cher — certains territoires perdent de leur population chaque année du fait du manque de services publics et d'infrastructures, y compris numériques.

Deux paramètres sont importants ici : le premier tient effectivement aux infrastructures, l'autre à la sociologie des territoires. Une étude établit que 13 millions de Français sont aujourd'hui éloignés du numérique[53], et que la moitié des non-internautes résident dans des communes de moins de 20 000 habitants. La réalité de la fracture numérique au sein de la population française ne doit pas être éludée. La dématérialisation des services publics et des démarches administratives ne rencontre pas nécessairement le même accueil à Paris et dans une commune de moins de 1000 habitants où les services publics physiques sont déjà rares.

Une situation qui crée une rupture d'égalité entre les populations mais aussi entre les territoires, entre ceux disposant d'individus capables d'utiliser le numérique de façon proactive en milieu professionnel ou autre et ceux bénéficiant d'une culture numérique limitée. L'accélération du déploiement des infrastructures numériques nécessite l'accélération de l'aménagement du territoire pour les besoins de tous.

La création du Fonds d'aménagement numérique des territoires (FANT), équivalent du Fonds d'amortissement des charges d'électrification (FACE), avait pour objet de contribuer au financement de certains travaux de réalisation des infrastructures et réseaux. Il répondait à un objectif de péréquation sur les raccordements les plus difficiles, en général en zone rurale.

Jean-Luc Sallaberry (Fédération Nationale des Collectivités Concédantes et Régies) préconise un fonds du même type pour le déploiement de la fibre avec un modèle de financement pérenne, à l'instar de ce qu'Orange a mis en œuvre pour le cuivre avec un fonds annuel de raccordements, d'évolution de 500 millions d'euros. Une somme équivalente pourrait selon lui permettre l'entretien du réseau compte tenu d'un nombre quasiment équivalent d'adresses entre la fibre et le cuivre et du coût équivalent de la fibre d'un point de vue technique. Un mode de financement pour les 30 à 40 prochaines années doit être prévu, jusqu'à ce qu'une technologie supplante la fibre. C'est un enjeu de pérennisation structurelle de ce réseau.

En revanche, défendre la compétitivité des territoires et des entreprises ne pourra se faire sans que les pouvoirs publics accordent une place préférentielle aux solutions locales dans les choix des solutions numériques utilisées. Conditionner les appels d'offres à certains paramètres relevant d'une dimension de souveraineté apparaît dès lors nécessaire pour assurer cette ambition.

[52] *Audition de Jean-Michel Mis par le comité de pilotage du rapport.*
[53] *"13 millions de français en difficulté avec le numérique", Société numérique.*

QUELLES CONDITIONS DE PRÉFÉRENCES LOCALES DANS LA CONCURRENCE ?

LES JO, TREMPLIN ENTREPRENEURIAL

Les Jeux Olympiques 2012 de Londres ont permi à la ville de se transformer et à la Grande-Bretagne d'accueillir de nombreux investisseurs. Levier de croissance et de création d'emplois, l'organisation de cet évènement a également permis le développement de solutions numériques par des acteurs privés soutenus par les pouvoirs publics. C'est le cas du système de vidéo-surveillance de la capitale britannique amélioré par des innovations logicielles dans le cadre d'une menace terroriste croissante. Par ailleurs, le complexe média, renommé Here East, est devenu un centre du digital et de l'innovation. L'exemple londonien illustre la volonté politique des gouvernements de s'appuyer sur l'organisation de ces évènements pour encourager le développement de solutions innovantes en soutenant le tissu économique local. Ce bilan ne s'applique malheureusement pas encore en France où l'Euro 2016 de football a engendré un impact entrepreneurial bien moins structurant.

Gageons qu'il en sera autrement pour 2024...

Cédric Messina, président-fondateur de MyCoach (plateforme gratuite de gestion d'équipe) et ancien président de la French Tech Côte d'Azur, prend pour exemple un appel d'offre organisé il y a quelques mois pour déterminer la plateforme numérique qui accompagnera les athlètes français aux JO de Paris. L'appel d'offre a été remporté par un acteur américain, les organisateurs reprochant à MyCoach son manque d'expérience internationale, bien que la solution ait été utilisée par l'équipe de France de football championne du monde, et par près d'un tiers des fédérations sportives professionnelles en France.[55]
Cet exemple parmi tant d'autres illustre l'incompréhension des personnes en charge des appels d'offres sur les enjeux de développement et de compétitivité internationale de nos acteurs positionnés dans le secteur du numérique, et la façon dont l'organisation à domicile d'évènements à portée internationale doit être synonyme de renforcement de notre ossature entrepreneuriale et économique.

Ceci est d'autant plus dommageable que derrière ces considérations apparaissent des problématiques relevant de sujets en lien avec la souveraineté, et l'ordonnance du 26 novembre 2018 — qui permet de faire du gré-à-gré pour protéger les acteurs numériques français — n'a encore jamais été utilisée. Le sujet est donc aussi celui de l'utilisation des lois existantes, car cette non-utilisation des leviers disponibles impacte les structures françaises.
Sans le soutien d'une puissance publique sensibilisée, la montée en puissance des acteurs numériques français pourrait être remise en cause : l'attribution des marchés aux géants étrangers est pour l'heure perçue comme plus sécurisante pour les pouvoirs publics, qui apportent en retour légitimité et présence sur le sol français à des géants au détriment de nos acteurs.

Pour Cédric Messina (MyCoach) *« le numérique a besoin de décisions rapides qui s'inscrivent sur le long terme, et non de décisions lentes avec des résultats rapides comme le souhaiteraient des décideurs publics[56]».*

[54] *C'est à dire de redistribution du financement de l'État parmi les collectivités territoriales.*
[55] *Audition de Sébastien Duré, Cédric Messina et Cédric Denoyel par le comité de pilotage du rapport.*
[56] *Audition de Sébastien Duré, Cédric Messina et Cédric Denoyel par le comité de pilotage du rapport.*

LE NUMÉRIQUE A BESOIN DE DÉCISIONS RAPIDES QUI S'INSCRIVENT SUR LE LONG TERME, ET NON DE DÉCISIONS LENTES AVEC DES RÉSULTATS RAPIDES COMME LE SOUHAITERAIENT DES DÉCIDEURS PUBLICS."

Cédric Messina, *président-fondateur de MyCoach.*

Sébastien Duré, directeur général de Hoppen (solutions connectées pour les établissements de santé), complète cette analyse, arguant la crainte pour les décideurs publics que peut susciter l'appel à une entreprise n'ayant pas encore fait la preuve de son concept, ou ne disposant pas d'une expérience jugée suffisante par les autorités compétentes.
Le fait que ces achats soient portés par des personnes mettant en jeu leur propre responsabilité et devant rendre des comptes sur le marché attribué en cas d'échec est un élément à prendre en considération. Toujours selon S. Duré, *« ces personnes ne prendront aucun risque pour leur carrière personnelle et privilégieront les leaders présumés étrangers aux potentielles start-ups françaises qui présentent un plus gros risque ».*[57]

Il est donc nécessaire de dépasser cette aversion au risque, ce blocage psychologique sur la capacité des entrepreneurs à apporter des solutions viables et pérennes aux acteurs privés nationaux. C'est ce blocage que Digital New Deal avait déjà identifié dans sa publication "*Sortir du Syndrome de Stockholm numérique*" en 2018. C'est pour cette raison que notre think-tank soutient l'initiative « IT50+ » qui regroupe les acteurs s'engageant à investir plus de 50% des nouveaux budgets IT auprès des acteurs français et européens.

SENSIBILISER LES DÉCIDEURS PUBLICS SUR L'ATTRIBUTION DES MARCHÉS

Véritable outil territorial au service des entrepreneurs du numérique né de la volonté de la FrenchTech, H7 est aujourd'hui un des principaux incubateurs français regroupant plus de 70 start-ups. Cédric Denoyel, son président, et ses équipes, ont formé l'ensemble des acheteurs de la métropole de Lyon aux solutions innovantes. Pour lui, les décideurs doivent utiliser le message politique provenant d'en haut comme un bouclier pour justifier des choix axés sur des entreprises françaises, tout en respectant le droit de la concurrence européen, qui n'est pas immuable. Il est également possible dans certains domaines de privilégier des acteurs locaux, comme pour la politique RSE.

Se passer de la mise en concurrence du marché public revient de facto à choisir un acteur qui a un monopole d'exploitation sur un élément, notamment via un brevet d'invention. Jean-Guy de Ruffray propose par exemple la mise en place d'une contrainte basée sur des garanties juridiques en termes de souveraineté des données. Ainsi, un acteur national comme OVH serait mis en avant face à un acteur étranger soumis à la juridiction de son pays d'origine.

[57] *Ibid.*

PROPOSITIONS

FAVORISER LES ENTREPRISES FRANÇAISES EN DEMANDANT DES GARANTIES JURIDIQUES SUR LA SOUVERAINETÉ DES DONNÉES.

Si le droit européen ne permet pas de choisir une entreprise dans le cadre de l'attribution de marché public en fonction de sa nationalité, d'autres moyens existent. Aussi, la France pourrait s'appuyer sur des dispositions techniques particulières afin de valoriser ses entreprises, d'autant que les pouvoirs publics et les collectivités ont largement pris conscience de leur rôle dans la transformation de l'économie au regard des impératifs sociaux, environnementaux et sociétaux à l'œuvre. Les collectivités territoriales ont d'ailleurs aujourd'hui la possibilité, pour tous leurs achats de fournitures, de services et de travaux, d'intégrer dans leurs cahiers des charges et dans les procédures de passation de marchés des objectifs de développement durable, sous la forme de clauses liées aux conditions d'exécution et/ou sous la forme de critères de jugement des offres. Il s'agirait donc, à partir du système de labellisation, de réserver un quota des marchés publics en fonction du degré de maturité atteint, en prenant en compte les efforts réalisés par les entreprises en fonction de leurs ressources internes.

RÉACTUALISER LA LOI DE BLOCAGE DE 1968 POUR CONTRER LA PORTÉE EXTRATERRITORIALE DU DROIT DE PAYS TIERS, NOTAMMENT NON-EUROPÉENS.

Cette loi de blocage interdit, sous peine de sanctions pénales à toute personne physique de nationalité française ou résident habituellement sur le territoire français et à tout dirigeant, représentant, agent ou préposé d'une personne morale y ayant son siège ou un établissement, de communiquer à des autorités étrangères une information ou des documents d'ordre économique, commercial, industriel, financier ou technique. Elle est toutefois très rarement convoquée pour contrer l'extraterritorialité du droit américain, en raison de son caractère très peu dissuasif et du faible nombre de sanctions mises en oeuvre. Le législateur français a tenté, avec la loi Sapin 2, de renforcer son efficacité en confiant à l'Agence française anticorruption (AFA) la mission de veiller au respect de ses dispositions. Une réforme de la loi au niveau national pourrait consister en une augmentation des sanctions pour la rendre plus dissuasive — les sanctions actuelles étant souvent jugées dérisoires —, en modifier le champ d'application pour qu'elle puisse concerner de façon certaine les opérateurs de cloud détenant les informations et ainsi « contrer » les effets du Cloud Act. En d'autres termes, rééquilibrer le rapport de force dans le conflit entre loi française et loi américaine. En attendant qu'un texte européen renforce un tel dispositif.

IMAGINER UN LOCAL DIGITAL ACT VISANT À RÉSERVER UNE PARTIE DES APPELS D'OFFRES PUBLICS À DES ENTREPRISES LOCALES DANS LE CADRE DE GRANDS PROJETS STRUCTURANTS POUR LE TERRITOIRE.

L'ordonnance n° 2018-1074 du 26 novembre 2018 et du décret n° 2018-1075 du 3 décembre 2018 ont permis d'instituer le code de la commande publique. Afin de répondre à l'objectif de simplification et d'accessibilité du droit, le code fait ressortir « les principes directeurs de la commande publique et [établit], de manière cohérente, les régimes de passation et d'exécution des contrats ». Pour autant, sur le même modèle de ce qui est mis en place dans certaines collectivités, il conviendrait de laisser une plus grande marge d'expérimentation dans le cas de la commande publique, notamment auprès des TPE-PME positionnées dans le secteur du numérique.

UNE CROISSANCE ÉCONOMIQUE PLUS RESPONSABLE, PLUS INCLUSIVE

Enfin, aborder le sujet des infrastructures de confiance nécessite de s'attarder sur la façon dont elles participent à ce que Jeremy Rifkin définit comme la Troisième révolution industrielle (TRI), à savoir le passage à une convergence des technologies de la communication (Internet/satellitales notamment) et des énergies renouvelables, propres et sûres. En liant protection de l'environnement et soutien aux innovations digitales, les politiques publiques menées en France s'inscrivent dans cette volonté de faire du numérique un levier de croissance écologique.

Le développement des smart territoires répond à cet impératif en plaçant le numérique comme un puissant levier d'optimisation des systèmes énergétiques, notamment dans le pilotage

« durable » écologique et économique des villes de demain. Si la transition numérique a besoin d'innovations techniques, l'impératif environnemental qui doit désormais orienter les perspectives de croissance s'accompagne d'un engagement renforcé de la part des acteurs économiques dans une démarche favorisant la transition écologique.

Cette mutation du cadre de la croissance est appelée à structurer les évolutions socio-économiques du XXIe siècle. Le numérique outille en effet la mesure et la compréhension des phénomènes en lien avec le bouleversement climatique et permet, à travers ses applications, une montée en puissance des solutions destinées à affronter ce défi.

Que ce soit à travers le déploiement de capteurs sur les réseaux d'eau visant à repérer les fuites, le développement de formes partagées de mobilité ou de consommation ou encore l'avènement de projets open source et low tech en matière d'énergie, le numérique et ses infrastructures sont porteurs de promesses au service d'une croissance responsable.
Des *« actions en faveur de l'écologie ont beaucoup à gagner à s'appuyer sur le numérique en matière d'information, d'implication des citoyens et des parties prenantes, de collaboration, d'organisation, de passage à l'échelle… »*[58]

L'orientation vers le développement durable est désormais un impératif compris par la plupart des parties prenantes, et cet impératif s'immisce de plus en plus dans les politiques publiques territoriales, d'autant que les collectivités locales ont un rôle clé à jouer pour soutenir et intégrer les innovations du numérique les plus profitables à la transition écologique de leur territoire.

Les collectivités sont en effet le premier maillon pouvant soutenir les expérimentations locales pour les orienter vers des objectifs de croissance verte et donner aux entreprises qui innovent la possibilité de tester leurs innovations. Les solutions numériques, permises par la couverture en infrastructures d'un territoire, représentent à ce titre un réservoir d'innovations dans lequel les pouvoirs publics peuvent puiser pour renouveler leurs services publics.

Les projets d'expérimentation ne manquent pas, sous des formes parfois hétérogènes, mais qui ont en commun d'optimiser la gestion des données dans le but d'améliorer les services aux usagers : transports, énergies, déchets, habitat.

Cette décentralisation de l'infrastructure, représentée par l'émergence de l'Internet of Things (IoT) promet la rationalisation et l'optimisation de la production et de la consommation de l'énergie. Exploiter plus efficacement est une nécessité dans les énergies renouvelables, d'avantage soumises aux variations et aléas naturels que les hydrocarbures dans leurs pipelines enterrés. L'Internet of Things est déjà utilisé dans divers secteurs industriels comme la smart city, le ferroviaire, la fabrication industrielle et médicale, l'automobile ou encore l'aéronautique[59].

La synergie espérée entre numérique et développement durable ne peut advenir sans le consentement de tous sur des usages clairs et transparents dans la gouvernance des données. La confiance du public envers les acteurs chargés de construire et faire fonctionner les projets d'infrastructures et de territoires intelligents est indispensable, car la méfiance, l'incompréhension et l'opacité peuvent faire échouer les projets.

[58] *"Faire converger les transitions numérique et écologique", Damien Demailly, Renaud Francou, Daniel Kaplan et Mathieu Saujot, Annales des Mines - Responsabilité et environnement, 2017.*
[59] *"L'Internet des objets, le futur de l'énergie ?", La Tribune de l'Énergie, octobre 2015.*

L'ÉCHEC DE GOOGLE À TORONTO, UN CAS D'ÉCOLE

L'abandon du projet porté par Sidewalk Labs (Google) à Toronto a fait événement. La province de l'Ontario et l'État Fédéral canadien ont lancé en 2001 une opération pour transformer 800 hectares de friches industrielles au bord du lac Ontario. L'appel d'offre cherchait « un partenaire innovant » mais aussi un mécène pour l'opération. Google et sa filiale Sidewalk Labs, remporte le marché et se félicite de pouvoir *« donner vie à notre vision du quartier du futur »*. En 2018, Ann Cavoukian, consultante du projet et commissaire à protection de la vie privée de la province s'alarme et se retire du projet en apprenant que des « tierces parties » pourraient accéder à des informations non anonymisées des habitants. À la suite de ces accusations publiques, un mouvement citoyen, #BlockSidewalk, s'organise. L'année suivante Sidewalk Labs publie son plan d'aménagement portant sur 77 hectares au lieu des 5 initialement prévus, un affront pour les dirigeants locaux et les habitants. Face au colossal projet des habitants dénoncent la *« privatisation de ressources publiques »*, des conflits d'intérêts au sein du consortium, et surtout un *« risque de surveillance des citoyens »*.

Ces derniers, remarquablement informés et engagés, ont pointé l'opacité concernant les installations et le traitement de traitement des données : déploiement massif de caméras et autres capteurs, inexistence de consentement et même d'information des citoyens ciblés, ignorance de la nature des données nominales et du profil d'identité numérique individuel, du stockage, de la propriété des données, de leur accessibilité et leurs exploitations possibles, manque de transparence du projet public sur ces points : *« puis l'impression qu'on refusait d'en parler au cours des concertations et tables rondes citoyennes, ont transformé le flou en suspicion d'espionnage secret.*[60]»

Pour les membres de l'Observatoire Netexplo Smart Cities, *« s'il y a une leçon à tirer de cet échec, c'est que si les promoteurs des transformations urbaines s'appuient sur les données massives, alors ils ne peuvent faire l'économie d'une réflexion profonde sur leur politique. L'abandon du projet Quayside à Toronto est un échec qui doit être compris comme une alerte. On a négligé de définir les règles du jeu, l'éthique de cette modernité. C'est à ce genre d'excès que vont s'opposer des citoyens, comme à Toronto.*[61]»

Sébastien Missoffe, directeur général de Google France, explique cette mésaventure par le goût de l'innovation de l'entreprise et la prise de risque assumée, caractéristiques de sa culture : *« Google continue d'innover avec un système 70/20/10 (70% sur l'existant, 20% sur ce qui est en train de changer et 10% sur des paris plus fous) »*. Il rappelle d'ailleurs que les villes changeant à une telle vitesse aujourd'hui, *« on ne doit pas simplement agrandir les territoires mais revoir les infrastructures et repartir de zéro avec toutes les innovations actuelles comme le machine learning ou l'énergie.*[62]»

Le cas de Toronto est très riche d'enseignements : au-delà de l'aspect « David contre Goliath », il montre d'une part que les citoyens se sont appropriés l'usage du numérique et des nouvelles technologies en conformité avec leurs valeurs démocratiques. D'autre part, cet événement montre que l'absence de transparence dans des projets impliquant les technologies numériques et le traitement massif de données provoquent le rejet.

La défense active de nos infrastructures et des tissus économiques qui irriguent nos territoires est un premier acte pour retrouver la confiance. Mais celle-ci ne se limite pas à la sécurisation :

[60] *"Pourquoi Google abandonne son projet de smart city à Toronto", L'Usine Digitale, 8 mai 2020.*
[61] *"Google city de Toronto : les raisons d'un échec", Les Échos, 18 mai 2020.*
[62] *Audition de Sébastien Missoffe par le comité de pilotage du rapport.*

la confiance est aussi accoudée à une demande intense de transparence, de participation et de respect des valeurs démocratiques, qui nous enjoignent à penser une nouvelle gouvernance.

La méfiance des citoyens, que ce soit envers des infrastructures perçues comme instruments de surveillance de masse, envers les vaccins ou les institutions publiques, doit nous informer et nous instruire sur les impacts de la transformation numérique sur les sociétés. Cette méfiance, loin de caractériser des gaulois ou des torontois réfractaires, signale au contraire un remarquable niveau d'éducation citoyenne et d'acculturation numérique, des atouts fondamentaux pour construire un Internet éclairé et démocratique.

À la méfiance des citoyens, nous devons répondre par l'explication, la reddition de comptes et la gouvernance partagée.

CONCLUSION

À travers les auditions, puis la rédaction de ce rapport, nous avons réalisé que répondre aux questions liées aux infrastructures numériques de confiance, c'était finalement répondre à deux grands enjeux politiques : la subsidiarité, et l'aménagement du territoire.

La subsidiarité d'abord, car avec les infrastructures numériques se pose constamment la question de l'échelon de responsabilité et du bon niveau de compétence. Le numérique est de ce point de vue un vecteur de clarification puisqu'il répartit assez distinctement les rôles entre l'Union européenne, l'État, et les collectivités :

- L'Europe est l'échelon de la vision et des moyens financiers. De toute évidence on ne peut pas demander à une Région, ni même à un État, de financer et organiser seul un maillage infrastructurel capable de concurrencer les investissements des GAFAM ou la Route de la Soie… Une réponse continentale est nécessaire pour se mesurer à ces nouveaux grands ensembles économiques et géopolitiques. De tels investissements ne peuvent être l'apanage que de l'Union européenne qui a la taille critique pour installer un rapport de force avec ces Léviathans digitaux.
- L'État est le garant de la confiance. C'est lui qui va orchestrer cette nouvelle forme de décentralisation en répartissant les moyens, en coordonnant les investissements, en opérant les grandes lignes de son architecture. L'État a le pouvoir d'adapter la vision européenne aux attentes de son territoire, et a l'immense responsabilité de devenir le tiers de confiance qui va sécuriser les nœuds de décisions dans cette organisation politique qui sera, à l'image d'Internet, de plus en plus décentralisée.
- Les collectivités constituent l'échelon de la gouvernance. C'est au niveau local, au plus près de la réalité du terrain et des attentes des citoyens, que doit se jouer le processus de décisions collectives. A l'ère des réseaux sociaux il est urgent de concevoir une forme de démocratie participative de proximité qui permettra de remonter aux échelons supérieurs les besoins des territoires.

L'aménagement du territoire, avec une redéfinition de cette politique publique à l'ère d'Internet. Faut-il se servir du digital pour aménager nos territoires, ou bien doit-on s'inspirer de notre organisation politique pour aménager le numérique ?
Notre conviction, c'est qu'il faut répondre oui aux deux.

Pour digitaliser nos territoires, la question des infrastructures a été abordée dans ce rapport et fait écho à la politique de déploiement du gouvernement avec par exemple le programme du Très Haut Débit, et son corollaire, le plan de lutte contre l'illectronisme. La plupart de nos propositions vont d'ailleurs dans ce sens, en

avançant des pistes de réflexion tendant à accompagner cet effort politique.

Pour introduire nos principes politiques et nos valeurs humanistes dans le numérique, là en revanche tout reste à faire. Internet est encore très jeune, ce réseau décentralisé a déjà connu des mues importantes. D'un point de vue économique bien sûr avec un paradoxal phénomène de centralisation de la valeur par une poignée d'acteurs monopolistiques contre lequel le think-tank Digital New Deal se bat en proposant de nouvelles voies de régulation permettant de compenser ces distorsions concurrentielles. Mais aussi d'un point de vue démocratique, puisque l'opacité algorithmique dans laquelle nous enferment ces plateformes menace nos fragiles équilibres sociétaux.

Il est donc temps que ces nouveaux territoires virtuels, qui impactent tant nos vies réelles, soient aménagés selon nos principes démocratiques. Nous ne pouvons pas déléguer notre confiance à des forces étrangères, aussi amicales soient-elles.

DIGITAL NEW DEAL
LE THINK-TANK DE LA NOUVELLE DONNE

Digital New Deal accompagne les décideurs privés et publics dans la création d'un Internet des Lumières, Européen et Humaniste. Notre conviction est que nous pouvons offrir une 3eme voie numérique en visant un double objectif : défendre nos valeurs en proposant une nouvelle régulation contre la centralisation des pouvoirs ; et défendre nos intérêts en créant les conditions de la coopération face à la captation de la valeur par les « Big Tech ».

Notre activité de publication a pour vocation d'éclairer de manière la plus complète possible les évolutions à l'œuvre au sein de enjeux de « souveraineté numérique », dans l'acception la plus large du terme, et d'élaborer des pistes d'actions concrètes, voire opérantes via le Do tank, à destination des organisations économiques et politiques.

LE CONSEIL D'ADMINISTRATION

Olivier Sichel (président fondateur) et Arno Pons (délégué général), pilotent les orientations stratégiques du think-tank sous le contrôle régulier du conseil d'administration.

Forts de leur intérêt commun pour les questions numériques, les membres du Conseil d'administration ont décidé d'approfondir leurs débats en formalisant un cadre de production et de publication au sein duquel la complémentarité de leurs expériences pourra être mise au service du débat public et politique. Ils s'impliquent personnellement dans la vie de Digital New Deal, notamment dans le choix des rapports et de leurs rédacteurs. Il sont les garants de notre indépendance, académique et économique.

SÉBASTIEN BAZIN
PDG AccorHotels

NICOLAS DUFOURCQ
DG de Bpifrance

AXELLE LEMAIRE
Ex-Secrétaire d'Etat du Numérique et de l'Innovation

ALAIN MINC
Président AM Conseil

DENIS OLIVENNES
DG Libération

YVES POILANE
DG Ionis Education Group

ARNO PONS
Délégué général du think tank Digital New Deal

JUDITH ROCHFELD
Professeur agrégée de Droit, Panthéon Sorbonne

OLIVIER SICHEL
President Digital New Deal
DGA Caisse des Dépôts

ROBERT ZARADER
PDG Equancy

contact@thedigitalnewdeal.org

www.thedigitalnewdeal.org

CALIF

Cabinet de conseil fondé en 2010, CALIF est basé à la fois en Auvergne-Rhône-Alpes et à Paris. Il est l'un des rares membres de l'Association française des conseils en lobbying (AFCL) dont le siège social est en province (St Etienne). CALIF est inscrit sur les registres HATVP.

Leader et pionnier dans la défense des intérêts territoriaux, CALIF accompagne principalement des entreprises (toutes tailles : startups, PME, grands groupes), mais aussi des fédérations professionnelles et des associations dans leur démarche d'influence en établissant avec tous ses clients français et étrangers une relation de partenariat et de confiance. CALIF opère à la fois pour des acteurs nationaux ou internationaux qui cherchent à développer leur influence et leurs activités dans les territoires (métropoles, villes moyennes, zones rurales…), mais aussi pour des structures basées en régions qui souhaitent rayonner dans d'autres régions ou au niveau national.

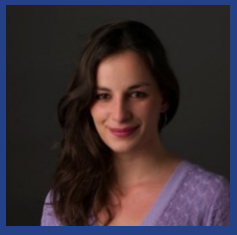
A l'échelle nationale, le cabinet assure des missions de lobbying auprès de toutes les parties prenantes : gouvernement, Parlement, agences de l'État, opérateurs, administrations, monde économique, académique, autres institutions etc.

Parmi les outils privilégiés par CALIF et qui s'inscrivent dans son savoir-faire : organisation d'évènements, de rendez-vous, mise en place de veilles, définition et pilotage de stratégies d'alliance etc.

Cabinet généraliste, intervenant dans de nombreux secteurs, CALIF a la confiance d'acteurs majeurs dans l'univers numérique (ETI, PME, start-up dont certaines au FT120, opérateurs d'infrastructures, leaders dans la e-santé, pionniers dans la cybersécurité…).

FRANÇOIS MASSARDIER
Président-fondateur

PIERRE-HENRI PICARD
Consultant senior



CAMILLE DUFIEUX
Consultante

MAGID BEN MAHMOUD
Consultant

CÉCILE DUFIEUX
Consultante

NOS PUBLICATIONS

Fiscalité numérique, le match retour
Vincent Renoux, *septembre 2021*

Défendre l'état de droit à l'ère des plateformes
Denis Olivennes et Gilles Le Chatelier, *juin 2021*

Cloud de confiance : un enjeu d'autonomie stratégique pour l'Europe
Laurence Houdeville et Arno Pons - *mai 2021*

Livres blancs : Partage des données & tourisme
Fabernovel et Digital New Deal - *avril 2021*

Partage de données personnelles : changer la donne par la gouvernance
Personal data sharing: governance as a game changer
Matthias de Bièvre et Olivier Dion - *septembre 2020*

Réflexions dans la perspective du Digital Services Act européen
Reflections in the perspective of the European Digital Services Act
Liza Bellulo - *mars 2020*

Préserver notre souveraineté éducative : soutenir l'EdTech française
Marie-Christine Levet - *novembre 2019*

Briser le monopole des Big Tech : réguler pour libérer la multitude
Big Tech Regulation: Empowering the Many by Regulating A Few
Sébastien Soriano - *septembre 2019*

Sortir du syndrome de Stockholm numérique
Jean-Romain Lhomme - *octobre 2018*

Le Service Public Citoyen
Paul Duan - *juin 2018*

L'âge du web décentralisé
Clément Jeanneau - *avril 2018*

Fiscalité réelle pour un monde virtuel
Vincent Renoux - *septembre 2017*

Réguler le « numérique »
Joëlle Toledano - *mai 2017*

Appel aux candidats à l'élection présidentielle pour un #PacteNumérique
janvier 2017

La santé face au tsunami des NBIC et aux plateformistes
Laurent Alexandre - *juin 2016*

Quelle politique en matière de données personnelles ?
Judith Rochfeld - *septembre 2015*

Etat des lieux du numérique en Europe
Olivier Sichel - *juillet 2015*

THINK-TANK
DIGITAL
NEW DEAL

novembre 2021

www.thedigitalnewdeal.org