Du mythe de l'automatisation au savoir-faire des petites mains : une histoire des datacenters par la panne

Guillaume Carnino, Clément Marquet

Du mythe de l'automatisation au savoir-faire des petites mains : une histoire des datacenters par la panne

Guillaume CARNINO (UTC) & Clément MARQUET (Telecom Paris)

Résumé : Cet article se propose de mettre au jour le processus historique de concentration des serveurs, initié dans les plus anciennes salles informatiques et aboutissant au *nec plus ultra* des centres de données (*datacenters*) sécurisés contemporains. Dans un univers pourtant conçu pour les supprimer, les pannes persistent de façon paradoxale en raison d'un phénomène de récursivité sécuritaire. Enfin, la permanence de l'action technique et du savoir-faire humain dans un univers industriel prétendument automatisé est frappante, à tel point que l'article rattache cette sociographie des infrastructures du numérique à une histoire globale de l'industrialisation, visant à montrer que loin des discours lénifiants sur l'innovation disruptive, les petites mains qui réparent et effectuent la maintenance quotidienne sont au cœur du déploiement des macro-systèmes techniques contemporains, offrant l'illusion d'une technique par nature fiable et disponible en permanence.

Mots-clés : panne, infrastructure numérique, travail invisible, automatisation, industrialisation

Abstract *: This article aims to uncover the historical process of server concentration, initiated in the oldest computer rooms and leading to the ultimate contemporary secure datacenters. In a world designed to eliminate them, failures persist paradoxically due to a phenomenon of security recursion. Finally, the permanence of technical action and human know-how in an allegedly automated industrial world is striking, to such an extent that the article links this sociography of digital infrastructures to a global history of industrialization, aiming to show that far from soothing discourses on disruptive innovation, the little hands that repair and carry out daily maintenance are at the heart of the deployment of contemporary large technical systems, offering the illusion of reliable and permanently available technologies.*

Keywords *: breakdown, digital infrastructure, invisible labor, automation, industrialization*

Le 9 novembre 2017, Octave Klaba, PDG de l'hébergeur OVH, tweete à 9h15 : « Nous avons un souci d'alimentation de SBG1/SBG4 [deux des quatre datacenters d'OVH à Strasbourg]. Les 2 arrivées électriques EDF sont down (!!) et les 2 chaînes de groupes électrogènes se sont mis[es] en défaut (!!!). L'ensemble de 4 arrivées élec[triques] n'alimentent plus la salle de routage. Nous sommes tous sur le problème. En plus du souci sur SBG, nous avons le souci sur le réseau optique en Europe qui interconnecte RBX [Roubaix] et GRA [Graveline] avec les POP [Point Of Presence, points d'interconnexion des réseaux internet régionaux]. Il est down (!!). »

Quelques heures plus tard, il commente dans un billet de synthèse : « Ce matin, nous avons eu 2 incidents séparés qui n'ont rien à voir l'un avec l'autre. Le 1er incident touche notre site de Strasbourg (SBG) et le 2e Roubaix (RBX). Sur SBG nous avons 3 datacentres en fonctionnement et 1 en construction. Sur RBX, nous avons 7 datacentres en fonctionnement. »

Conséquence directe de cette panne, plusieurs milliers de sites – petits ou gros, voire gouvernementaux – inaccessibles, mais également de nombreux autres services (téléphonie, Cloud, VPS, mails, serveurs de jeux, etc.) sont indisponibles plusieurs heures durant, ce qui pour certains constitue un véritable manque à gagner, notamment en période de soldes. Un client analyse l'incident quelques temps plus tard : « Le souci avec ces deux incidents est qu'en arrivant en même temps, ils ont créé le pire des scénarii. […] C'est la double peine : vos serveurs sont HS, mais vous ne pouvez même pas rediriger les requêtes vers d'autres serveurs. »

Les pannes et autres accidents constituent un point d'accès privilégié pour saisir le fonctionnement des infrastructures sur lesquelles repose l'organisation de nos sociétés occidentales[1]. L'accès quotidien à l'eau potable, à l'électricité, au gaz et maintenant au réseau internet nous fait prendre pour acquis que ces ressources sont disponibles, invisibilisant en retour la complexité des systèmes techniques sur lesquels reposent les orientations politiques qui les gouvernent et les formes de travail nécessaires à leur pérennité. La panne joue ainsi un rôle heuristique devenu classique dans les *Science and Technology Studies* : elle rend visibles des pans entiers de l'organisation sociotechnique.

Il est remarquable que, parmi ces systèmes techniques, les technologies de l'information et de la communication aient pris une place considérable au cours des vingt dernières années, notamment avec le développement d'internet. Parmi les composantes de ce gigantesque système technique, les datacenters, bâtiments qui regroupent les systèmes informatiques des organisations et permettent l'accès aux données à distance, jouent un rôle considérable : les pannes qui les affectent peuvent maintenir au sol les avions d'une flotte pendant plusieurs heures[2], interdire toute transaction bancaire[3] ou paralyser le système judiciaire d'un pays entier[4]. Ce ne sont donc pas uniquement les opérations que nous effectuons sur le web ou par l'intermédiaire de nos applications smartphones qui sont affectées, mais la plupart des actions quotidiennes qui reposent sur la bonne gestion des bâtiments abritant les systèmes informatiques, ainsi que sur l'intégrité des réseaux qui les relient à nos appareils[5].

Longtemps passés inaperçus dans les études sur l'internet et le développement de nos sociétés numériques qui se sont essentiellement concentrées sur la part virtuelle de ces technologies (forums, sites en lignes, e-commerce, bases de données, progiciels de gestion intégrée, etc.), les centres de données font depuis quelques années l'objet d'analyses, profitant notamment d'un tournant matériel des études sur les *media*[6]. Ces études ont mis en évidence l'abondance des ressources énergétiques en jeu dans l'organisation de l'internet[7] et le poids des datacenters dans l'organisation des territoires[8]. La raison d'être de ces assemblages – la sécurité des données – est régulièrement mentionnée : elle nécessite une protection physique de l'accès à l'information, avec la présence de vigiles, de systèmes de reconnaissance et d'autorisation d'entrée, mais aussi une garantie de disponibilité des données par l'intermédiaire du réseau internet la plus continue possible, 24 heures sur 24, 7 jours sur 7, toute l'année.

Si ces travaux donnent à voir les mondes dans lesquels les datacenters s'implantent et les manières dont ils les reconfigurent autour de leurs besoins, il reste très difficile de comprendre ce

---

[1] Susan L. Star, « The Ethnography of Infrastructure », *American Behavioral Scientist*, Vol.43, No. 3, 1999, p. 377-391.
[2] « US airlines temporarily ground flights after AeroData glitch », https://www.datacenterdynamics.com/news/us-airlines-temporarily-ground-flights-after-aerodata-glitch [1er avril 2019].
[3] « Widespread Wells Fargo issues blamed on datacenter outage, cause disputed », https://www.datacenterdynamics.com/news/widespread-wells-fargo-outage-blamed-data-center-fire [7 février 2019].
[4] « UK justice system brought to a standstill by datacenter network issue », https://www.datacenterdynamics.com/news/uk-justice-system-brought-standstill-data-center-outage [25 janvier 2019].
[5] Nicole Starosielski, *The Undersea Network*, Durham & London, Duke University Press, 2015.
[6] Jean-François Blanchette, « A Material History of Bits », *Journal of The American Society for Information Science and Technology*, 62(6), 2011, p. 1042-1057 ; Shannon Mattern, *Code and Clay, Data and Dirt. Five Thousands Years of Urban* Media, Minneapolis & London, University of Minnesota Press, 2013 ; Lisa Parks,& Nicole Starosielski (dir.), *Signal Traffic. Critical Studies of Media Infrastructures,* Chicago, University of Illinois Press 2015.
[7] Mél Hogan, « Data Flows and Water Woes: The Utah Data Center », *Big Data & Society* 2015, N° 2, p. 1-12. ; Julia Velkova, « Data that warms: Waste heat, infrastructural convergence and the computation traffic commodity », *Big Data & Society* 2016, juillet-décembre, p. 1-10 ; Guillaume Carnino, Clément Marquet, « Les datacenters enfoncent le cloud : enjeux politiques et impacts environnementaux d'internet », *Zilsel*, 2018/1 (n° 3), p. 19-62.
[8] Asta Vonderau, « Scaling the Cloud: Making State and Infrastructure in Sweden », *Ethnos*, 2018 ; Clément Marquet, « Ce nuage que je ne saurais voir. Promouvoir, contester et réguler les data centers à Plaine Commune », *Tracés*, Vol. 2, N° 35, 2018, p. 75-98 ; Cécile Diguet & Fanny Lopez (dir.), *L'impact spatial et énergétique des datacenters sur les territoires*, Rapport Ademe, 2019.

qui se passe en leur sein. Des photographies mettent en scène de mystérieux espaces dépourvus d'humains, illuminés par d'étranges lumières bleutées et traversés de câbles colorés[9], mais ces clichés sont surtout des expériences artistiques réalisées à des fins de communication, et non la matière de travaux ethnographiques[10]. En raison du caractère critique de l'information qui y est stockée et des engagements de continuité, les datacenters sont des installations très difficiles d'accès et leurs propriétaires s'avèrent bien souvent peu enclins à répondre aux demandes d'entretiens. Néanmoins, comme l'indique l'extrait en ouverture, les pannes constituent des moments de visibilité singuliers des infrastructures, qui non seulement leur octroient une grande couverture médiatique, mais donnent aussi un aperçu du fonctionnement de ces installations et de la multitude de circuits techniques et d'expertises qui y interviennent. Cette visibilité tient en partie aux engagements que les opérateurs ont vis-à-vis de leurs clients : la panne constitue une rupture de leurs contrats de continuité de service, rupture qui occasionne des dommages et intérêts mais aussi et surtout des justifications et démonstrations de la capacité de l'opérateur à identifier l'origine du sinistre en vue d'y remédier.

Nous présenterons ici en trois temps, respectivement à partir de trois principaux ensembles de sources primaires, la façon dont la panne met en évidence le fonctionnement technique d'internet. À partir d'entretiens avec des acteurs du domaine et d'une ethnographie des salons professionnels[11], nous tenterons de mettre au jour le processus historique de concentration des serveurs, initié dans les plus anciennes salles informatiques et aboutissant au nec plus ultra des datacenters sécurisés contemporains, classés en fonction de leur garantie contre les pannes. C'est ensuite grâce aux sources écrites que constituent les *workflows* (bien souvent disponibles en ligne) que nous exposerons la permanence paradoxale des pannes dans un univers pourtant conçu pour les supprimer[12]. Enfin, nos entretiens ethnographiques *in situ*, au sein des datacenters que nous avons eu l'occasion de visiter[13], nous permettront de mettre au jour la permanence de l'action technique et du savoir-faire humain dans un univers industriel prétendument automatisé. Nous espérons ainsi rattacher cette sociographie des infrastructures du numérique à l'histoire globale de l'industrialisation en montrant que loin des discours lénifiants sur l'innovation disruptive, les petites mains qui réparent et effectuent la maintenance quotidienne sont au fondement et au centre du déploiement des macro-systèmes techniques contemporains, offrant l'illusion d'une technique par nature fiable et disponible en permanence.

Rationaliser les infrastructures pour lutter contre les pannes

Les datacenters sont avant tout des bâtiments, carapaces physiques de l'accumulation des données informatiques. Répartis aux quatre coins de la planète, sur des sites plus ou moins exotiques, tels que des fjords finlandais, des barges dans la baie de San Francisco, des grottes dans

[9] A.R.E Taylor, « Data Centers as Technological Wilderness », *Culture Machine*, Vol. 18, 2018.

[10] Jennifer Holt & Patrick Vondereau, « Where the Internet Lives. Data Centers as Cloud Infrastructures », in Lisa Parks & Nicole Starosielski, *op. cit.,* 2015.

[11] Nous avons ethnographié les éditions 2016, 2017 et 2018 du salon Datacenter World, et l'édition 2016 du salon Datacenter Solution Management. Ces salons permettent d'observer les sujets qui préoccupent les acteurs d'une année sur l'autre, mais aussi d'avoir de nombreux échanges informels dans les stands des entreprises participantes au cours desquels nous pouvons évaluer la pertinence de nos orientations de recherche. Par ailleurs, nous avons réalisé des entretiens approfondis avec un consultant et un architecte spécialisé dans la conception de datacenters, et la responsable de formation de l'IUT Villetaneuse.

[12] Nous nous sommes essentiellement appuyés sur OVH Tasks, site web accessible au public sur l'état des serveurs et les opérations de maintenance planifiées [http://travaux.ovh.com].

[13] Les opérateurs de datacenters sont rarement enclins à faire visiter leurs installations par des individus avec lesquels ils n'ont pas relation commerciale. Néanmoins, au cours de notre enquête, nous sommes parvenus à visiter les centres de données de trois acteurs privés, soit par quiproquo (les agents commerciaux de l'opérateur pensaient que nous venions louer de l'espace informatique) soit au travers de visites pédagogiques organisées pour les étudiants de l'UTC. Ces visites ont été complétées par trois visites de datacenters universitaires, dont l'un d'entre eux, de dernière génération, était très similaire aux installations des acteurs privés.

le Loiret ou d'anciennes bases de lancement de missiles, c'est avant tout dans les banlieues des grandes métropoles et en zones urbaines qu'ils se multiplient[14]. Le point commun entre ces différents lieux nous semble tenir à l'effort industriel de rationalisation des espaces de stockage des données informatiques en vue d'obvier à la survenue de pannes. Un commercial nous explique avec fierté : « On est un peu la cave de l'Internet, et si la cave s'effondre, tout s'effondre[15]. »

Dès les débuts de l'informatique, la taille des ordinateurs impose de gérer des contraintes industrielles en termes de bâti qui s'apparentent fortement à celles que connaissent les datacenters aujourd'hui. Sur le système IAS testé en 1951 afin d'effectuer un calcul (de 60 jours !) indispensable à la réalisation de la première bombe thermonucléaire, l'humidité estivale de Princeton eut pour conséquence de faire geler les unités de climatisation – un incident tout à fait comparable à l'averse dans le datacenter de Facebook à Prineville en août 2011, quand le différentiel de température couplé à la forte hygrométrie circonstancielle aboutit à la formation d'une véritable bruine à l'intérieur des bâtiments[16]. Ainsi, toutes les premières machines informatiques (considérées, principalement pour des raisons militaires, comme des infrastructures critiques) posent invariablement la question de la sécurisation de leur environnement direct afin d'éviter les pannes, ce qui amène presque toujours à la construction d'un bâtiment spécifique, doté de critères de sécurité propres : l'ENIAC américain de 1946[17], tout comme le MINSK et le BESM soviétiques de 1959[18], les AN/FSQ-7 utilisés après 1958 pour le projet de défense antiaérienne étasunienne SAGE[19], les IBM 705 de la BNP en 1957[20] ou le système de réservation de billets d'avion SABRE en 1960[21], sont établis sur des étages, voire des immeubles entiers.

Au cours des années 1950, des chercheurs du Stanford Research Institute créent un système informatique à destination des banques (Electronic Recording Method of Accounting computer processing system, ou ERMA), révélé au public en 1955, testé sur des comptes bancaires réels en 1956 et mis en service pour la Bank of America en 1959[22]. Dans les années 1960, la majorité des banques internationales s'équipent d'ordinateurs massifs assistant la gestion des comptes. En Angleterre, Barclays ouvre son premier centre informatique bancaire en 1961, où l'on installe un imposant IBM 1401[23]. Ces machines de calcul occupent au fil des années des espaces de plus en plus importants et sont regroupées dans d'immenses Centres de traitement de l'information (CTI). Cependant, les grèves du personnel des années 1970 soulignent la fragilité de ces espaces critiques pour le fonctionnement des banques[24], qui vont alors opérer un double mouvement de dispersion des sites de traitement de l'information et de mise en circulation de copies des bandes informatiques d'un site à l'autre. Certains sites, tels le CTI de Dinand, sont soumis à des mesures

---

[14] Concentrant les données et les systèmes informatiques qui les stockent, les traitent et les font circuler, les opérateurs sont de grands consommateurs d'électricité et déploient des stratégies variées (architecturales, technologiques mais aussi géographiques) pour limiter leur consommation électrique. Pour une étude sur leur conséquence pour les systèmes énergétiques des territoires, voir Cécile Diguet et Fanny Lopez (dir.), *L'impact spatial et énergétique des datacenters sur les territoires*, Rapport Ademe, 2019. Pour une étude globale sur l'impact environnemental des technologies numériques, voir Hugues Ferreboeuf (dir.), *Lean ICT. Pour une sobriété numérique,* Rapport The Shift Project, 2018.

[15] Entretien du 12 novembre 2014.

[16] Everest Pipkin, « It was raining in the datacenter », 12 juin 2018 [https://medium.com/s/story/it-was-raining-in-the-data-center-9e1525c37cc3].

[17] Kent C. Redmond & Thomas M. Smith, *Project Whirlwind*, Digital Press, 1980.

[18] Rihards Balodis & Inara Opmane, « History of Data Centre Development », in Arthur Tatnall (dir.). *Reflections on the History of Computing: Preserving Memories and Sharing Stories*, Springer, 2012, p. 180-203.

[19] David F. Winkler & Julie L. Webster, *Searching the skies: the legacy of the United States Cold War defense radar program*, Headquarters Air Combat Command, 1997.

[20] Pierre Mounier-Kuhn, *Mémoires vives. 50 ans d'informatique chez Bnp Paribas*, Paris, Bnp Paribas, p. 57.

[21] « (Short) Data center history » [http://opticalcloudinfra.com/index.php/what-why-and-how/short-data-center-history].

[22] Balodis & Opmane, *op. cit.,* p. 194.

[23] *Ibid.*, p. 194.

[24] Mounier-Kuhn, *op. cit.*, p. 106.

de sécurité qui constituent les prémices des datacenters actuels : « alimenté par trois groupes électrogènes en cas de coupure EDF, avec les cuves à mazout et le refroidissement nécessaire par l'eau puisée dans la nappe phréatique, il peut fonctionner en autonomie complète pendant plusieurs semaines[25] ». Au fil des années, les espaces sont de plus en plus standardisés : « on a entrepris de dissocier les opérateurs et les techniciens[26] ».

Alors que se développent ces gigantesques *mainframes*, on voit apparaître les premiers réseaux locaux (LAN, local area network, dont le premier – ARCnet – est établi à la Chase Manhattan Bank en 1977 pour interconnecter 255 machines). Le PC (Personal Computer) est introduit en 1981 et marque le début de la microinformatique, mais c'est seulement après le développement du protocole NFS (Network File System) par Sun microsystems en 1984 qu'un ordinateur client est en mesure d'accéder à un fichier sauvegardé sur un serveur distant : dès le début des années 1990, on voit les anciennes salles des *mainframes* colonisées par ces plus petits « serveurs » et parfois renommées *datacenters*[27]. L'arrivée du web dans les années 1990 pousse à articuler ces réseaux intranet avec l'internet naissant, ce qui aboutit à la multiplication des salles machines, indispensables à l'hébergement de données et de sites sans cesse plus nombreux. À mesure que se développe l'économie numérique, les entreprises se doivent de maintenir leur infrastructure informatique opérationnelle jour et nuit, chaque jour de l'année. Si certains espaces abritant des *mainframes* ou des réseaux de télécommunications ont conservé des systèmes d'alimentation ou de climatisation robustes[28], les salles informatiques des années 1990 étaient bien souvent bricolées avec les moyens du bord. Deux informaticiens travaillant aujourd'hui dans un datacenter dernière génération nous avouent avoir un souvenir ému de ces années de bricolage, où les pannes étaient gérées au coup par coup[29] : on passait l'aspirateur pour enlever les poussières accumulées sur les ventilateurs des serveurs, les fenêtres étaient ouvertes manuellement en hiver afin de refroidir les salles qui surchauffaient, etc.

Ces mouvements de rationalisation des infrastructures ne rendent cependant pas compte du mouvement de concentration des sites autour des villes. Bien souvent, les datacenters privatifs – qu'ils appartiennent aux sociétés de la grande distribution, aux banques ou aux grands noms de l'internet – se situent dans les campagnes, profitant d'hectares de terrains peu chers. Dans les années 1990, avec le développement de l'internet, sont apparus de nouveaux acteurs dans l'immobilier urbain. Internet est un réseau de réseaux dont le fonctionnement repose entre autres sur les espaces dans lesquels les réseaux s'interconnectent. Par souci d'économie, plutôt que de développer des compétences internes en informatique et gestion des données, de nombreuses entreprises ont recours à des hébergeurs assurant la maintenance des serveurs et la qualité de la connexion aux réseaux. Ces hébergeurs tendent à se situer dans les mêmes locaux que les opérateurs de télécommunication, de sorte à garantir à leur client une circulation de données au plus haut débit possible. Avec la multiplication des serveurs dans les années 1990, ces espaces souvent situés en ville prennent le nom d'« hôtel télécom ». Pour éviter la dépendance trop forte à un opérateur en particulier, des acteurs tiers développent un marché appelé « colocation neutre » garantissant aux clients l'égal accès à l'ensemble des réseaux[30]. Les enjeux d'accès au réseau et de rapidité dans l'échange de données participent à la concentration des infrastructures dans les zones urbaines, les différents acteurs s'installant souvent à proximité les uns des autres. Par ailleurs, comme les plus gros opérateurs ont besoin de gigantesques puissances de calcul, ils

[25] *Ibid.*, p. 107.
[26] *Ibid.*, p. 106.
[27] « The evolution of the datacenter: Timeline from the Mainframe to the Cloud » [https://siliconangle.com/2014/03/05/the-evolution-of-the-data-center-timeline-from-the-mainframe-to-the-cloud-tc0114].
[28] Mastertel & Cineminers, *The Internet Architecture. Data Center* [https://www.youtube.com/watch?v=hg5zWg0kNkI, 8 avril 2019].
[29] Entretien du 17 février 2017.
[30] Pour un récit plus détaillé, voir Bruno Moriset, « Les forteresses de l'économie numérique. Des immeubles intelligents aux hôtels de télécommunications », *Géocarrefour*, n° 78(4), 2003, p. 375-388.

s'avèrent progressivement en mesure de louer celle-ci. On voit alors se développer ce que les professionnels nomment l'IaaS (Infrastructure as a Service), qui correspond peu ou prou à l'émergence dans le grand public de l'idée de *cloud*, l'informatique délocalisée « dans les nuages » (mais en réalité tout à fait matérielle et consommatrice d'énergie). Comme un commercial nous l'expose à plusieurs reprises : « le *cloud*, c'est juste le datacenter de quelqu'un d'autre ».

Selon un consultant senior[31], le datacenter se situe à la croisée de ces deux histoires, celle des espaces de stockage d'information au fonctionnement peu à peu ultra-rationalisé, et celle de la mise en réseau de machines nécessitant d'avoir à disposition une multiplicité d'accès télécom. Aux exigences de sécurité s'ajoutent les attentes en termes de gain économique grâce à la concentration des infrastructures. Le marché des datacenters se divise ainsi selon plusieurs modalités, des services de *cloud computing* à l'hébergement du système d'information d'entreprises clientes.

Dès le début des années 2000, il y a donc un marché pour la colocation neutre, qui propose des services sécurisés, principalement les infrastructures assurant le bon fonctionnement des baies de serveurs – alimentation électrique, climatisation, dispositifs anti-incendie, sécurité physique des bâtiments. Autrement dit, *ce que vend un datacenter, c'est une assurance contre les pannes*. D'autres garanties de sécurité peuvent être contractualisées : certains sites proposent des clauses de type « *disaster recovery* » ou « *business continuity* », classiquement à destination de la finance ou des forces armées. Le datacenter offre alors des espaces permettant de recréer en quelques dizaines de minutes, grâce aux données sauvegardées et aux postes préinstallés, l'entièreté d'un environnement de travail préétabli (la salle de gestion boursière d'une grande banque parisienne, par exemple). Ainsi, en cas de sinistre, une équipe du client peut migrer directement vers l'espace sécurisé du centre afin de ne pas mettre en péril la continuité de son activité. Un commercial nous avoue néanmoins, l'œil complice, qu'il ne faudrait pas que tous ses clients revendiquent au même moment l'accès à une solution de *business continuity*, car il ne pourrait alors pas tous les satisfaire[32].

L'ensemble de ces contraintes et préoccupations se voit normalisé et explicité par un classement en différents *tiers* (« couches », en anglais) : le Tier I renvoie à une simple salle des machines avec climatiseur (ou sans !), là où le Tier IV correspond au *nec plus ultra* en matière de sécurité et de redondance des installations. Un datacenter Tier III est censé offrir contractuellement une continuité de service annuelle de 99.984 %. Dans cette configuration, on doit pouvoir gérer des périodes de maintenance sans impact sur la disponibilité des serveurs, bien qu'il soit théoriquement possible qu'adviennent des coupures en cas d'incidents importants (pas de redondance garantie sur la totalité de la chaîne). Le Tier IV est le plus haut niveau de garantie qu'un datacenter puisse offrir avec une disponibilité de 99.995 % (soit environ vingt-six minutes de panne dans l'année : ce qui serait, aux yeux d'un commercial, « inadmissible pour [se]s clients[33] »), et une redondance intégrale au niveau des circuits électriques, de refroidissement et du réseau. Cette architecture doit permettre de pallier les pires scénarios d'incidents techniques sans jamais interrompre la disponibilité des serveurs en place. Dans la pratique, le Tier IV implique des contraintes si coûteuses qu'elles ne sont nécessaires qu'en cas de besoins spécifiques, essentiellement dans le monde de la finance et des établissements bancaires.

Officiellement, l'organisme international en charge de la certification Tier est l'Institut Uptime[34], un consortium d'entreprises créé en 1993 dont l'objectif revendiqué est de maximiser l'efficacité des datacenters. Cette certification s'effectue en trois étapes, relatives à l'étude des documents du projet de construction, à l'inspection des infrastructures finalisées, puis à l'audit des processus de fonctionnement en situation réelle. Dans les faits, si la nomenclature « Tier » est utilisée par l'ensemble de la profession, rares sont les centres à pousser jusqu'à son terme la

[31] Entretien du 29 avril 2016.
[32] Entretien du 12 novembre 2014.
[33] Entretien du 26 mai 2016.
[34] L'Uptime Institute est parfois surnommé « The Global datacenter Authority » [https://uptimeinstitute.com].

certification : si 86 datacenters sont certifiés Tier II ou plus aux États-unis et 42 en Arabie saoudite, seuls 19 d'entre eux le sont en Chine et seulement 3 en France (soit moins de 1 % du parc[35]). Certains marchés nationaux ne prennent en effet pas la peine de faire classer officiellement leurs installations par l'Uptime Institute. Dans le cas hexagonal, le marché mobilise ainsi la dénomination en *tiers* tout en s'appuyant sur un autre ensemble normatif, le système des normes ISO.

On peut supposer que la « *tierification* » fournit un raccourci qui simplifie et synthétise la complexité et la diversité des normes auxquelles les opérateurs cherchent à se conformer. Se présenter Tier III ou Tier IV, c'est donner au client une indication de ce qu'il peut être en droit d'attendre, avant d'aller observer plus précisément les certifications que l'opérateur a effectivement obtenu. De nombreux commerciaux insistent d'ailleurs sur le fait qu'ils sont « de Tier III+, presque IV [36] » et que la certification serait une perte de temps et d'investissement. À l'inverse, un commercial nantais s'énerve dès que nous lui posons la question de la tierification de son datacenter : « C'est de la flûte tout ça ! Ce qui compte c'est le sérieux des équipes. On n'a jamais eu de gros plantage[37]. »

Au-delà de l'effet d'annonce commercial, et donc d'une réalité probablement parfois enjolivée, il est probable qu'à la manière des corporations artisanales d'Ancien Régime[38], l'intrication des acteurs et intérêts au sein du marché participe à la production d'une réputation quant à la qualité des produits et services vendus, réputation dont le poids suffit à écarter la majorité des fraudes.

Automatiser pour lutter contre la panne, ou la récursivité sécuritaire

Une panne est un arrêt accidentel et subit du fonctionnement d'un appareil ou d'une installation. Maîtriser la panne implique de pouvoir l'anticiper afin de pallier de la façon la plus fluide qui soit les dysfonctionnements qu'elle entraîne : la stratégie mise en œuvre est bien souvent celle du couplage en temps réel entre capteurs et redondance matérielle, l'ensemble étant géré par des automates, censés garantir l'opérateur contre la faillibilité humaine. Mais le recours à l'automatisation permet-il réellement de se prémunir contre les pannes ?

Le mythe d'une machinerie autorégulée, totalement efficiente et dont les pannes ne relèveraient jamais de sa nature propre bat son plein[39]. « 67 % des *outages* [pannes] sont dus à des fautes humaines, donc si on peut enlever cette couche-là[40]… », suggère un communiquant en fin de conférence au forum Datacenter World : l'automatisation totale serait la panacée face aux problèmes posés par les humains gérant les infrastructures technologiques actuelles. Un directeur ironise lourdement sur le PFH, acronyme « sociologique » (sic), renvoyant au « putain de facteur humain », source de tous les maux. Le moins d'opérations de maintenance il y a à faire, le moins de risque il y aurait : tout doit donc être réduit au minimum, cloisonné, découplé. À cette réduction drastique du matériel et des opérations répond le doublement de tout : chaque salle doit être autonome, c'est-à-dire que chaque salle doit posséder ses propres batteries, générateurs électriques, systèmes de climatisation, tableaux électriques, etc. L'optimisation est faite en vue de l'autonomie maximale de chaque client, au sens où ses erreurs ne risquent pas d'affecter le matériel des autres.

---

35 Chiffres valables au 6 mai 2017.

36 Ce que l'Uptime Institute n'hésite pas à dénoncer comme étant dépourvu de sens *via* sa page wikipedia.

37 Entretien du 29 mars 2018.

38 Steven L. Kaplan, Philippe Minard (dir.), *La France, malade du corporatisme ? XVIII^e^- XX^e^ siècles*, Paris, Belin, 2004.

39 Sur l'utopie d'une technique par nature étrangère aux dysfonctionnements, voir notamment Jean-Baptiste Fressoz, *L'Apocalypse joyeuse. Une histoire du risque technologique*, Paris, Seuil, 2012, chap. VI : « La Mécanique de la faute ».

40 Forum Datacenter world, 15 novembre 2017. Un autre intervenant martelait le chiffre plus marquant encore de 90 % : de là à imaginer qu'il s'agit surtout d'un discours performatif, bien peu fondé sur des chiffres réels et mobilisant des ordres de grandeur visant à convaincre (deux tiers, neuf dixièmes, etc.), il n'y a qu'un pas.

La mythologie de l'efficacité et de la sécurité totales engendrées par la procéduralisation et l'automatisation existe depuis deux siècles au moins[41], et elle se porte étonnamment bien[42] alors même qu'elle entre en contradiction avec les faits. L'institut Ponemon donne en effet des chiffres tout à fait différents dans son étude consacrée aux « *unplanned outages* » (arrêts critiques imprévus) des datacenters, puisque seulement 22 % à 24 % des pannes auraient une origine humaine[43] :

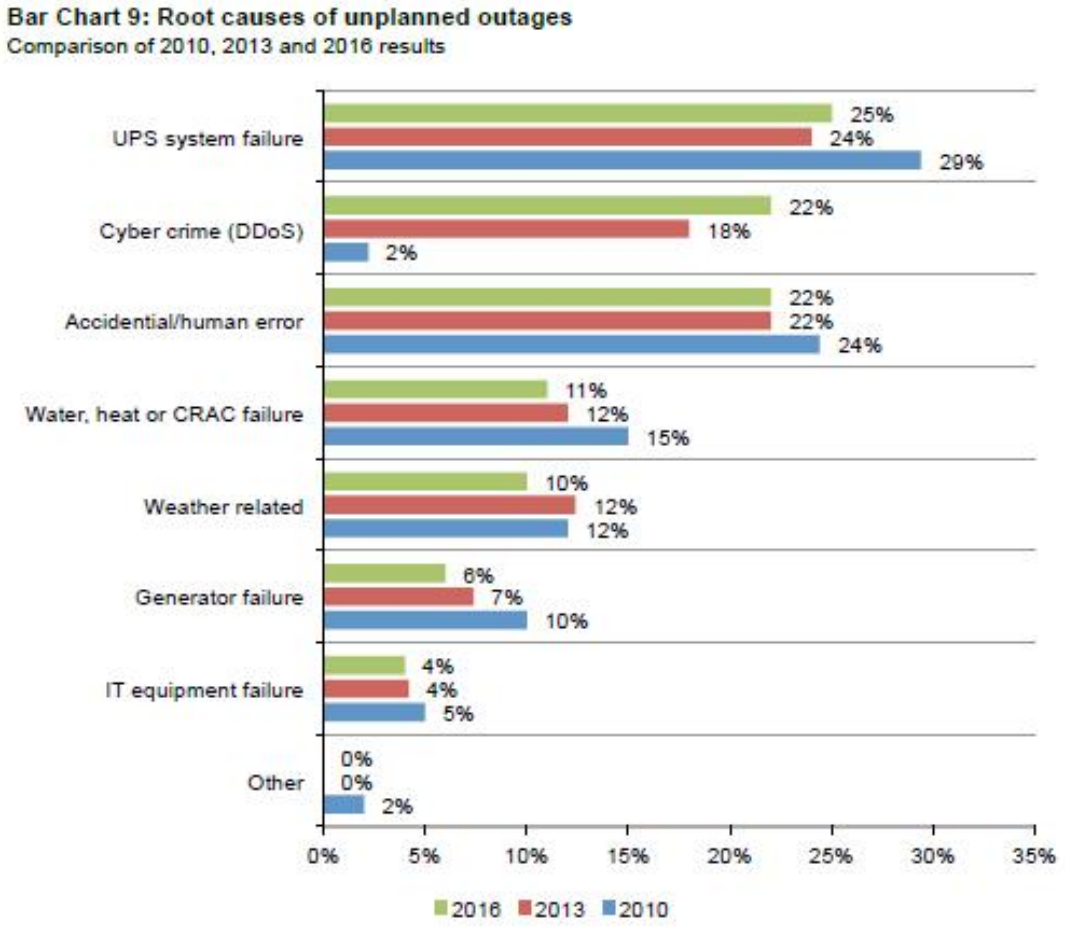

Figure 1. Cause des arrêts critiques imprévus des datacenters. Graphique comparant les chiffres de 2010, 2013 et 2016. D'après Ponemon Institute, Cost of Data Center Outages, *Janvier 2016, p. 16.*

En réponse à un arrêt critique survenu dans un datacenter parisien en juin 2017, un superviseur explique :

> Nos datacenters sont équipés de diverses sondes. L'une d'entre elles est capable de détecter la présence de liquide dans une baie. Les alertes levées par ces sondes sont transmises aux techniciens présents dans le datacenter via différents canaux de communication. L'un d'eux est un

[41] Pour un florilège de cette mythologie, voir notamment l'anthologie réalisée par François Jarrige, « Face au luddisme : quelques interprétations », in Cédric Biagini, Guillaume Carnino (dir.), *Les Luddites en France. Résistances à l'industrialisation et à l'informatisation*, Paris, L'Échappée, 2010, p. 287-334.

[42] Pour une version enchantée, voir par exemple le rapport du McKinsey Global Institute, *Disruptive technologies. Advances that will transform life, business and the global economy*, 2013, p. 42-43. Pour une approche plus critique, mais relevant de la même posture de sidération devant les discours technologiques, voir Bernard Stiegler, *La Société automatique*, Paris, Fayard, 2015 ou Carl Benedikt Frey, Michael A. Osborne, *The Future of employment. How susceptible are jobs to computerization ?*, 2013
[http://www.oxfordmartin.ox.ac.uk/downloads/academic/The_Future_of_Employment.pdf, 22 mai 2017].

[43] Ponemon Institute, *Cost of Data Center Outages*, janvier 2016, p. 16.

> outil baptisé MARCEL (l'acronyme de Monitoring Audio des Réseaux, Composants, Équipements et Locaux), qui permet de diffuser un message audio dans nos datacenters grâce à une voix de synthèse et à des haut-parleurs disposés dans chaque salle. C'est un moyen très efficace de prévenir nos techniciens d'un événement anormal présentant un caractère d'urgence, quand bien même ceux-ci sont déjà occupés sur une intervention telle qu'un remplacement de disque. Ils n'ont ainsi pas besoin de retourner en salle de contrôle pour s'apercevoir qu'un incident est en cours dans un autre endroit du datacenter. Un précieux gain de temps.
>
> Dans le cadre de l'implantation à l'international de nouveaux datacenters, ce système de monitoring audio était en cours de mise à jour, afin que la voix de synthèse puisse diffuser les messages d'alerte dans plusieurs langues. En raison d'une malfaçon dans cet upgrade, réalisé le même jour, l'alerte audio n'a pas fonctionné correctement, retardant sa prise en charge. Au lieu d'intervenir immédiatement, comme c'est le cas habituellement, le premier technicien est arrivé dans la salle 3 onze minutes après la détection de la fuite. Ce retard a très certainement accentué l'impact de l'incident[44].

On constate alors que le recours aux automates ne prémunit aucunement contre les pannes : la mise à jour d'un dispositif de prévention automatisé (le fameux MARCEL) a accru un problème à l'origine potentiellement bénin.

Courant novembre 2017, les infrastructures d'OVH à Strasbourg et Roubaix sont victimes d'incidents critiques engendrés par les automates en charge des protocoles de redondance :

> Ce matin, le système de bascule motorisée [d'un datacenter de Strasbourg] n'a pas fonctionné. L'ordre de démarrage des groupes n'a pas été donné par l'automate. Il s'agit d'un automate NSM (Normal Secours Motorisé), fournit par l'équipementier des cellules haute-tension 20 kV. Nous sommes en contact avec lui, afin de comprendre l'origine de ce dysfonctionnement. […] La base de données avec la configuration est enregistrée 3 fois et copiée sur 2 cartes de supervision. Malgré toutes ces sécurités, la base a disparu. Nous allons travailler avec l'équipementier pour trouver l'origine du problème et les aider à fixer le bug. […] Les bugs ça peut exister, les incidents qui impactent nos clients non. Il y a forcement une erreur chez OVH puisque malgré tous les investissements dans le réseau, dans les fibres, dans les technologies, nous venons d'avoir 2 heures [153 minutes] de downtime sur l'ensemble de nos infrastructures à Roubaix[45].

Se profile alors un véritable vertige épistémologique, puisque toute source de sécurisation est aussi potentiellement une source de panne ; d'où un cercle vicieux fonctionnel, véritable *récursivité sécuritaire*, où à chaque automate peut être adjoint un automate de contrôle, qui à son tour peut se trouver à l'origine d'un dysfonctionnement, et qu'il faut donc sécuriser et contrôler, *ad nauseam*. Il semble donc impossible d'éradiquer le spectre de la panne sans en recourir à nouveau à l'humain.

[44] https://blog.ovh.com/fr/blog/hebergements-web-post-mortem-incident-29-juin-2017/
[45] http://travaux.ovh.net/?do=details&id=28244&edit=yep [14 novembre 2017].

Ainsi, le progiciel de gestion intégré d'OVH[46] – dont le fil des tâches relatives aux datacenters est consultable en libre accès – mentionne, pour la période 2005-2018, 628 incidents, dont très peu concernent réellement un arrêt critique et d'ampleur de nombreux serveurs, précisément grâce au monitoring humain des machines, d'où la récurrence systématique de la mention « Nous avons des difficultés à joindre les serveurs de la baie. Nous investiguons. » – invariablement suivie de « Intervention terminée. Tous les serveurs sont à nouveau en ligne. »

Les incidents sont ainsi traités directement par des humains censés prendre la bonne décision quant à leur résolution. Les superviseurs indiquent par exemple que « Nous avons détecté un défaut sur la partie de distribution électrique de la baie, nous procédons au remplacement de celle-ci. Aucun impact prévu. » (24 octobre 2018, 19h36) Quand la panne est trop complexe pour être gérée par les techniciens sur site (habituellement en rotation sur le mode des 3 x 8), les constructeurs sont mis à contribution (les contrats de maintenance délimitant le cadre de ce genre d'intervention), comme pour cette panne d'onduleur (23 octobre 2018, 23h39) : « Nous avons détecté un dysfonctionnement sur l'UPS6B, nous investiguons. […] Le fournisseur a été contacté, un technicien spécialiste est sur place. »

Par ailleurs, au sein de cet univers ultraconnecté où les chaînes d'alimentation peuvent se trouver impactées en cascade, certains incidents mineurs deviennent parfois sources de pannes majeures, comme en témoigne cette longue description d'une série de dysfonctionnements et des mesures prises à son encontre ayant abouti à une interruption de service dans le datacenter parisien d'OVH :

> À 18h48, le jeudi 29 juin 2017, dans la salle 3 du datacenter P19, en raison d'une fissure sur un tuyau en plastique souple de notre système de *watercooling*, une fuite de liquide de refroidissement entraîne la présence de fluide dans l'une des deux baies de stockage propriétaires, lesquelles n'étaient pas refroidies par ce procédé mais se trouvaient à proximité immédiate. Cela a eu pour conséquence directe la détection d'un défaut électrique entraînant l'arrêt complet de la baie. […]
>
> À 21h25, l'ensemble des personnels d'astreinte sont mobilisés, et les équipes techniques sont restées pour leur prêter main forte. Il est décidé de mener deux actions en parallèle :
>
> – plan A : poursuivre les tentatives de récupération des données sur la baie de stockage avec l'aide du constructeur ;
> – plan B : lancer la procédure de restauration des données depuis les sauvegardes réalisées quotidiennement. […]
>
> La procédure d'urgence, servant à exécuter cette série d'opérations existait et avait été testée. Mais pas industrialisée. Autrement dit, restaurer une table à partir du backup est trivial. Restaurer un très grand volume de tables, initialement réparties sur 99 VM [machines virtuelles], nécessitait davantage d'automatisation, sans quoi la restauration aurait nécessité plusieurs journées.
>
> L'équipe en charge des *backups* a scripté, durant la nuit, la procédure, afin de pouvoir l'industrialiser. À 3h du matin, le clonage des VM à partir d'un *template* source était lancé et les données étaient en cours de restauration. […]
>
> À 23h40, la restauration de la 99e instance prend fin, et l'ensemble des utilisateurs retrouvent un site fonctionnel, à l'exception de quelques

[46] Voir http://travaux.ovh.net/?project=11&PHPSESSID=51f7a9b303cce6ae257f04194f130990 [consulté le 19 décembre 2018]. Si le fil n'est pas nécessairement complet, notamment sur les débuts de son implémentation en 2005, la proportion d'incidents varie néanmoins très peu sur le long cours.

> utilisateurs, dont la base était hébergée sur des instances sous MySQL 5.1 et a été restaurée sous MySQL 5.5. Un effet de bord rapidement résolu.
>
> Un geste commercial sera accordé aux clients pour l'indisponibilité de leur service durant près d'une journée. Il nous est apparu légitime de dédommager nos clients, au-delà de la clause limitative de responsabilité présente dans nos conditions générales de service. Le geste commercial consistera à prolonger gracieusement l'offre d'hébergement web des utilisateurs concernés de deux mois.[47]

Comme on peut le constater, tout problème est susceptible d'engendrer un problème à son tour, dont l'aboutissement peut être l'arrêt des machines (ici une fuite de liquide de refroidissement aboutissant à un défaut d'alimentation électrique). La complexité des dispositifs autorise alors plusieurs chemins critiques visant à la résolution des pannes (ici le plan A – réparer la machine – et le plan B – réinstancier les sauvegardes sur d'autres machines), et les spécialistes sont alors indispensables pour qualifier la faisabilité et quantifier la durée de telle ou telle solution envisagée – d'où les multiples recours aux constructeurs des divers matériels, puisqu'il n'existe aucun individu, aussi compétent soit-il, en mesure de maîtriser l'ensemble des composants de toute la chaîne de fonctionnement des infrastructures.

On comprend alors l'intérêt de dispositifs automatisés permettant de détecter tout problème et d'établir un autre chemin fonctionnel autorisant à poursuivre les processus critiques. Mais le souci est que ces chemins alternatifs, aussi efficients soient-ils, impliquent toujours une maintenance humaine, qui peut être source d'erreur et de dysfonctionnements. Si un technicien chez Céleste, fournisseur français de solutions *cloud* à destination des entreprises, nous explique lors d'un entretien que « les maintenances préventives limitent les pannes[48] », le principal datacenter de l'entreprise a paradoxalement subi un arrêt critique le 12 décembre 2013 suite à une maintenance antérieure du groupe électrogène : le technicien envoyé par le constructeur avait oublié de rouvrir, après ses tests, le robinet d'alimentation provenant de la cuve principale des groupes électrogènes, qui ont donc cessé de fonctionné après que leur réservoir courant (environ 300 L, soit quelques minutes d'autonomie) fut vidé lors d'une coupure EDF.

Une armée d'invisibles petites mains

La réalité du terrain met en évidence l'action humaine indispensable au bon fonctionnement des dispositifs : « *Ça s'entend au son* » (ce qui permet de savoir quand il y a besoin d'intervenir), nous signifie un opérateur observant lors d'une visite un *cluster* de serveurs qui entre en phase de calcul intensif[49]. Même au plus haut niveau de la *high-tech*, là où les processus électroniques sont censés échapper aux perceptions humaines, les travailleurs développent une habileté, un savoir-faire, typique des métiers techniques[50], qui les rend aptes à comprendre les variations les plus minimes et les causes possibles des dysfonctionnements auxquels ils sont confrontés[51]. Un superviseur nous expose la sécurité drastique qui entoure l'armoire à clefs : en plus du badge, il faut des clefs, mais pour obtenir les clefs, il faut un badge, et un code, qui permettent d'ouvrir et de savoir qui a ouvert – les données sont conservées trente jours – pour enfin libérer magnétiquement les trousseaux que la personne est habilitée à utiliser ; « si on essaie de prendre

[47] https://blog.ovh.com/fr/blog/hebergements-web-post-mortem-incident-29-juin-2017/
[48] Entretien du 9 novembre 2018.
[49] Entretien du 17 février 2017.
[50] Richard Sennett, *Ce que sait la main : la culture de l'artisanat*, Paris, Albin Michel, 2009.
[51] Pour un autre exemple de savoir-faire incorporé relatif à la réparation informatique, voir Blanca Callén, « Donner une seconde vie aux déchets électroniques. Économies informelles et innovation sociotechnique par les marges », *Techniques & culture* n° 65-66, 2016, p. 206-219.

une clef à laquelle on n'a pas droit, un message d'alerte est envoyé[52] ». Dans l'instant qui suit cette déclaration d'inviolabilité du système, le voici qui s'empare sans autorisation d'une clef dont il a besoin pour la poursuite de la visite, et sourit en disant qu'une alerte a probablement été émise, mais qu'il n'a ni son portable ni son ordinateur sur lui… Dans une veine similaire, un directeur de centre nous confie au détour d'un couloir : « Si j'applique les consignes du Ministère, plus personne ne bosse[53]. » Dans les faits, c'est l'écart entre la règle et la réalisation effective de la tâche qui rend possible la maintenance de ces infrastructures : là où le discours commercial vante une fiabilité et une sécurité totale passant par des dispositifs indépendants de toute action humaine, la réalité de l'activité semble plus nuancée, comme le confirme un client et commentateur acerbe de ces dispositifs :

> On pourrait naïvement croire que ces choses-là sont automatisées et qu'à la moindre étincelle ou petite volute de fumée, PAF, les bouteilles se vident. Eh bien non. D'une part, dans beaucoup de datacenters, il faut que deux détecteurs se déclenchent avant qu'un humain soit averti qu'il y a peut-être le feu, mais en plus, le déclenchement du système d'extinction est manuel. Quand on voit que dans certains bâtiments, les personnes sur place mettent parfois 20 minutes à se rendre compte que les salles d'hébergement n'ont plus d'alimentation électrique, ça fait peur[54].

Non seulement les automates ne sont pas exempts de dysfonctionnements, mais en plus leur impénétrabilité structurelle (puisque fonctionnant à la vitesse de l'électron, et donc imperméables aux perceptions humaines) rend tout problème difficile à diagnostiquer. Lors de nos entretiens, deux techniciens insistent d'ailleurs à plusieurs reprises sur la faible fiabilité de l'électronique et donc de l'automatisation[55] : « Saloperie d'électronique. […] Sur le papier ça marche. […] Dans la vraie vie, ça a ses limites. » ; « Des alimentations bourrées d'électronique, ce sont des sources à emmerdement. » ; « Des PDU intelligents [multiprises électriques informatisées], on veut pas en entendre parler. » ; « Moi, j'suis mécanicien, j'ai pas confiance dans l'électronique. […] Les composants électroniques, c'est sensible à la température, à l'humidité, c'est pas fiable. » Ces techniciens revendiquent ainsi, dans leurs propres termes, la nécessité d'un accès *technique* et *non technologique* aux dispositifs dont ils ont la charge. Nous n'entendons pas ici technologique au sens étymologique (*tekhnè-logos*, discours sur les techniques, *i.e.* compréhension procédurale), mais au sens contemporain plus commun de techno-science, renvoyant à l'idée de processus alliant savoirs scientifiques et procédés industriels de grande ampleur, des machineries complexes et potentiellement opaques aux perceptions humaines[56]. Autrement dit, l'enjeu, pour ces immenses infrastructures, est de maintenir la possibilité d'un accès aux processus à l'échelle des opérateurs, indispensables à la maintenance quotidienne des systèmes. Techniques et technologies sont par nature faillibles, mais les premières, à la différence des secondes, permettent davantage de maîtrise humaine face à leurs dysfonctionnements. On peut alors inverser la vulgate managériale en la matière et considérer que si certaines pannes prennent leur source dans l'action de

[52] Entretien du 5 novembre 2015.
[53] Entretien du 17 février 2017.
[54] http://blog.spyou.org/wordpress-mu/2010/08/12/dis-papa-cest-quoi-un-datacenter-44-le-reste [22 avril 2019].
[55] Entretien du 9 novembre 2018.
[56] Sur les différents sens de la technologie, voir notamment Guillaume Carnino. « Les Transformations de la technologie. Du discours sur les techniques à la "techno-science" », *Romantisme. Revue d'histoire du XIX^e siècle*, n° 150, 2010, p. 75-84 ; Guillaume Carnino et Liliane Hilaire-Pérez, « Qu'est-ce que la technologie ? Jalons pour l'histoire longue d'un concept oublié », in Guillaume Carnino, Liliane Hilaire-Pérez et Jochen Hoock (dir.), *La technologie générale. Johann Beckmann, Entwurf der algemeinen Technologie/Projet de technologie générale (1806)*, Rennes, Presses universitaires de Rennes, 2017, p. 13-36. Sur la distinction entre technique et technologie contemporaine, voir Cédric Biagini & Guillaume Carnino. « On arrête parfois le progrès », Biagini & Carnino. *Les Luddites en France*, *op. cit.*, p. 5-59.

l'Homme, la totalité des situations de bon fonctionnement des infrastructures est en réalité intégralement de son fait !

Si un datacenter emploie peu de personnel fixe, le recours à la sous-traitance implique néanmoins la mobilisation de nombreux acteurs lors de la prévention ou de la résolution d'un problème, ce qui a pour vertu de rendre visible les multiples compétences et réseaux humains sollicités pour le maintien du système. Derrière le discours clinquant de l'automatisation, certains opérateurs de datacenters prennent les devants pour créer localement des filières de formation spécialisées dans la gestion et la maintenance de leurs infrastructures. Ainsi, l'opérateur Telecity Group (racheté depuis par l'entreprise Equinix) s'est rapproché en 2010 de l'Université de Villetaneuse pour élaborer un cursus datacenter au sein du Diplôme universitaire de technologie génie électrique et informatique industrielle (DUT GE2I). Cette initiative vient répondre à un double problème pour l'opérateur : d'abord, il s'agissait de répondre aux critiques qui s'inquiétaient de l'importante occupation foncière des centres de données sans pour autant prendre part pleinement à l'économie locale[57]. Ensuite, les techniciens issus des formations classiques ne possédaient pas les compétences nécessaires à la maintenance de ces infrastructures : spécialisés par type de technologie (génie électrique ou réseaux), ils n'étaient pas en mesure de prendre en compte la complexité des relations entre les différents équipements qui composent le centre de données.

Le nouveau cursus se différencie ainsi des formations existantes en n'étant « pas orienté vers un domaine mais vers un outil industriel ». Ouverte en 2012, la formation articule trois domaines de compétence : la partie réseau, demandant aux techniciens des savoirs manuels, notamment épissurer les fibres optiques, mais aussi connaître les bases de la configuration des routeurs, la gestion des adresses IP et la topologie des réseaux. La partie électrique, cruciale pour assurer une distribution en énergie la plus propre possible, c'est-à-dire régulière, nette et sans coupure, demandant notamment de savoir gérer les systèmes automatiques et d'assurer manuellement les prises de relais entre les différents systèmes électriques (batteries, groupes électrogènes) en cas d'échec des automates. À cela s'ajoute des cours de climatique pour assurer la régulation thermique et hygrométrique des salles.

Ces formations techniques permettant la gestion des infrastructures de réseau ne reposent pas sur des technologies particulièrement neuves, mais sur l'agencement d'un ensemble de techniques bien maîtrisées. Lorsque l'on visite un datacenter, on constate rapidement que si l'essentiel de la valeur économique est produite par le fonctionnement des ordinateurs, le temps passé dans la salle informatique est relativement faible vis-à-vis de celui consacré à l'exposition des autres installations. La surface occupée par les serveurs ne représente généralement que la moitié, au plus, de celle destinée au reste des équipements (armoires électriques, transformateurs, batteries, groupes électrogènes, bonbonnes de gaz inerte en cas d'incendie, groupes froids, sans compter une salle de réunion, quelques salles de repos ou de travail, et un espace pour les services de sécurité, les humains aussi ayant des besoins à respecter pour veiller au bon fonctionnement des machines).

Si le contenu de la formation universitaire « techniciens infrastructures » témoigne de la diversité des systèmes techniques qui sont articulés pour garantir la continuité de service, la spécificité du centre de données n'est cependant pas uniquement abordée sous sa dimension technique, mais aussi sous son aspect commercial. Le DUT fonctionne ainsi sur un principe de sélection, recrutant douze à quinze élèves parmi la promotion de première année composée de quarante à soixante cinq élèves. La sélection se fait en particulier sur les compétences dites de rigueur et de « savoir-être » en entreprise, qui font par ailleurs l'objet de cours lors de la suite de la formation, comprenant la ponctualité, la politesse, la gestion du stress et l'anglais. Autant de compétences sociales que la responsable de formation estime d'autant plus nécessaires que les

[57] Pour analyse de la polémique suscité par la présence de nombreux datacenters à Plaine Commune, au nord de Paris, voir Clément Marquet, *op. cit.*

étudiants du département, la Seine-Saint-Denis, peuvent être davantage attendus sur ces questions en raison des préjugés sur le 93. À la différence d'autres équipements techniques (centrales électriques, postes sources) et en dépit des efforts des architectes pour séparer les salles de serveurs des équipements d'infrastructures, le datacenter reste un espace partagé entre les différents métiers, c'est-à-dire entre les techniciens et les développeurs informatiques, qui sont bien souvent des clients de l'hébergeur. La criticité des installations, et notamment l'enjeu de la continuité de service, est là aussi mise en avant pour justifier le soin pris dans la sélection :

> Il y a une banque avec qui on travaille, si on prend les systèmes d'information des salles de marché, il ne faut pas une microseconde de coupure. Et quand on a un client au téléphone, en général le client n'appelle pas pour dire tout va bien mais pour dire qu'il a un souci, donc auquel cas il faut aussi savoir tenir le stress et ne pas se liquéfier[58].

Garantir la continuité de service passe aussi par des conditions de travail fatigantes, les techniciens sont aux trois huit et peuvent être d'astreintes en cas d'incidents. Lors des retours de stage, les étudiants font remarquer la longueur des couloirs des bâtiments : le caractère éprouvant de ce travail est aussi ce qui permet à la formation de tourner. Les 60 % à 70 % d'étudiants embauchés en CDI à la fin de chaque année (soit environ 8 élèves sur 12) reposent notamment sur l'important *turn-over* du métier : « Je pense que c'est un boulot assez physique, au bout d'un moment il y a une certaine usure, ça libère des places et ça fait vivre la formation. » Selon la responsable de formation, les techniciens font ce travail quelques années puis, soit montent en hiérarchie, soit s'orientent vers d'autres postes de techniciens dont les conditions de travail et notamment les horaires sont plus conciliables avec une vie de famille.

À titre d'exemple, la mégapanne qu'a connu OVH le 9 novembre 2017 sur ses datacenters de Roubaix et Strasbourg a demandé une disponibilité totale des équipes pendant plusieurs jours. Comme les conséquences sur l'infrastructure située à Strasbourg étaient plus importantes, OVH a affrété des jets privés afin d'accélérer la rotation des équipes entre Strasbourg et Roubaix (figure 2).

[58] Entretien avec Fabienne Floret, maîtresse de conférences en génie électrique à l'IUT de Villetaneuse et responsable du cursus datacenter (3 octobre 2016).

Figure 2 Tweet d'Octabe Klaba, P.-D.G. de l'hébergeur OVG, 12 novembre 2017. Source : https://twitter.com/olesovhcom/status/929654854267625472?lang=en

La disponibilité permanente du système implique une mise à disposition d'humains, qui doivent se soumettre au rythme et aux nécessités des flux numériques. Et si un datacenter emploie peu de personnel fixe, c'est toute une batterie de métiers rattachés à chaque équipement qui doit se tenir au garde-à-vous chez chaque sous-traitant de l'infrastructure.

Conclusion

Nous rencontrons finalement une certaine histoire des techniques et de l'industrie s'inscrivant notamment dans les travaux d'Hélène Vérin (qui voyait dans les innombrables activités de réparation – et non dans l'innovation, fût-elle de rupture – la dynamique première de l'industrialisation[59]), de Liliane Hilaire-Pérez (qui décrit les tâches multiformes et segmentées du milieu artisanal du luxe londonien au XVIII[e] siècle comme vectrices du processus d'industrialisation[60]), de Carlotta Benvegnù et David Gaborieau (qui montrent que loin d'engendrer un chômage massif par les algorithmes et le *big data*, la logistique, véritable envers du décor du e-commerce et de la grande distribution, est un univers excessivement consommateur de main d'œuvre, usée prématurément[61]) ou du programme de recherche de Jérôme Denis et David Pontille relatif à la maintenance industrielle contemporaine (qui proposent d'infléchir l'analyse des systèmes techniques pour ne plus insister sur le déploiement de dispositifs

[59] Hélène Vérin, *Entrepreneurs, entreprise. Histoire d'une idée*, Paris, Garnier, 2011.
[60] Liliane Hilaire-Pérez, *La Pièce et le Geste. Artisans, marchands et savoir technique à Londres au XVIII[e] siècle*, Paris, Albin Michel, 2013.
[61] Carlotta Benvegnù & David Gaborieau, « Produire le flux. L'entrepôt comme prolongement d'un monde industriel sous une forme logistique », *Savoir/Agir*, n° 39(1), 2017, p. 66-72.

prétendument autorégulés, mais bien pour faire réapparaître les innombrables « petites mains de la société d'information » rendues invisibles par le grand récit de l'innovation triomphante[62]). Autrement dit, l'analyse du datacenter par la panne nous semble inviter à déplacer, au même titre que ces autres travaux, le centre de gravité de l'histoire industrielle, qui apparaît en dernière instance comme l'œuvre de travailleurs et de travailleuses, dont l'activité est recomposée par la taille des dispositifs impliqués, et dont l'enjeu quotidien consiste à maintenir un accès à dimension humaine à ceux-ci, permettant de conserver un horizon minimal de sens et d'efficacité. L'industrialisation n'est dès lors plus tant une histoire d'invention et d'innovation que de croissance de la taille des processus et périmètres techniques, aboutissant à un contrôle accru du travail humain, toujours plus enchâssé au sein de ces gigantesques infrastructures. En d'autres termes, il s'agit de conserver une prise à taille humaine sur un système dont l'échelle et la complexité débordent sinon directement toute possibilité de contrôle.

On retrouve alors l'étymologie du terme panne (*i.e.* « mettre en panne »), c'est-à-dire orienter les vergues d'un navire de manière à arrêter sa marche – un arrêt maîtrisé, indispensable au contrôle du vaisseau, et qui a fini par signifier un arrêt de fonctionner tout court. Car pour stopper un galion et rester sur place, il ne faut pas se contenter de larguer les écoutes et d'attendre (sans quoi on perd le contrôle du bateau) ; il faut masquer ses voiles, c'est-à-dire régler la moitié d'entre elles pour avancer et border l'autre moitié « à contre », comme si l'on voulait faire reculer le navire. Le bâtiment reste alors stable et il peut reprendre sa course aisément. Originellement, la panne renvoie donc à l'action humaine indispensable pour conserver la maîtrise d'un dispositif.

À cet égard, un réseau hydraulique, une chaîne de production logistique ou un datacenter ne diffèrent guère d'une frégate de la Royale du grand siècle : l'humain reste central dans la gestion quotidienne et récurrente des incidents. Une inversion s'opère néanmoins à l'échelle des dispositifs contemporains : si ce travail incessant de l'Homme est plus que jamais indispensable au bon fonctionnement des macro-systèmes techniques[63], le rythme de l'activité est désormais cadencé par leur temporalité propre. Le tempo social est alors celui des machines qui forment système, et la propriété de ces systèmes assure désormais une puissance (économique, politique ou militaire) à la mesure du nombre d'invisibles petites mains enrôlées dans leur maintenance. On comprend que les détenteurs et bénéficiaires de ces infrastructures ont tout intérêt à faire croire que la source de leur pouvoir réside dans des machines et non dans l'exploitation d'un travail humain. Gageons que, depuis deux siècles au moins, une large part des discours sur l'automatisation a justement pour fonction de banaliser cette fiction politique et de minorer l'importance de l'activité de l'Homme, étonnamment persistante sur le long cours. En ce sens, un macro-système technique est un instrument de prescription opératoire et d'ordonnancement social, c'est-à-dire un artefact politique.

[62] Jérôme Denis et David Pontille, « Beyond breakdown: exploring regimes of maintenance », *Continent*, 2017, p. 13-17.

[63] Thomas P. Hughes, *Networks of Power: Electrification in Western Society, 1880-1930*, Baltimore : Johns Hopkins University Press, 1983.