DANGER 5G

27/9 et 17/10/2019

AU SOMMAIRE

1) 27/09/2019 : « Résister à la mise sous surveillance totale de nos villes et de nos vies »

Article du Monde Diplomatique

https://www.monde-diplomatique.fr/2019/06/TREGUER/59986

Mardi 17 septembre 2019.

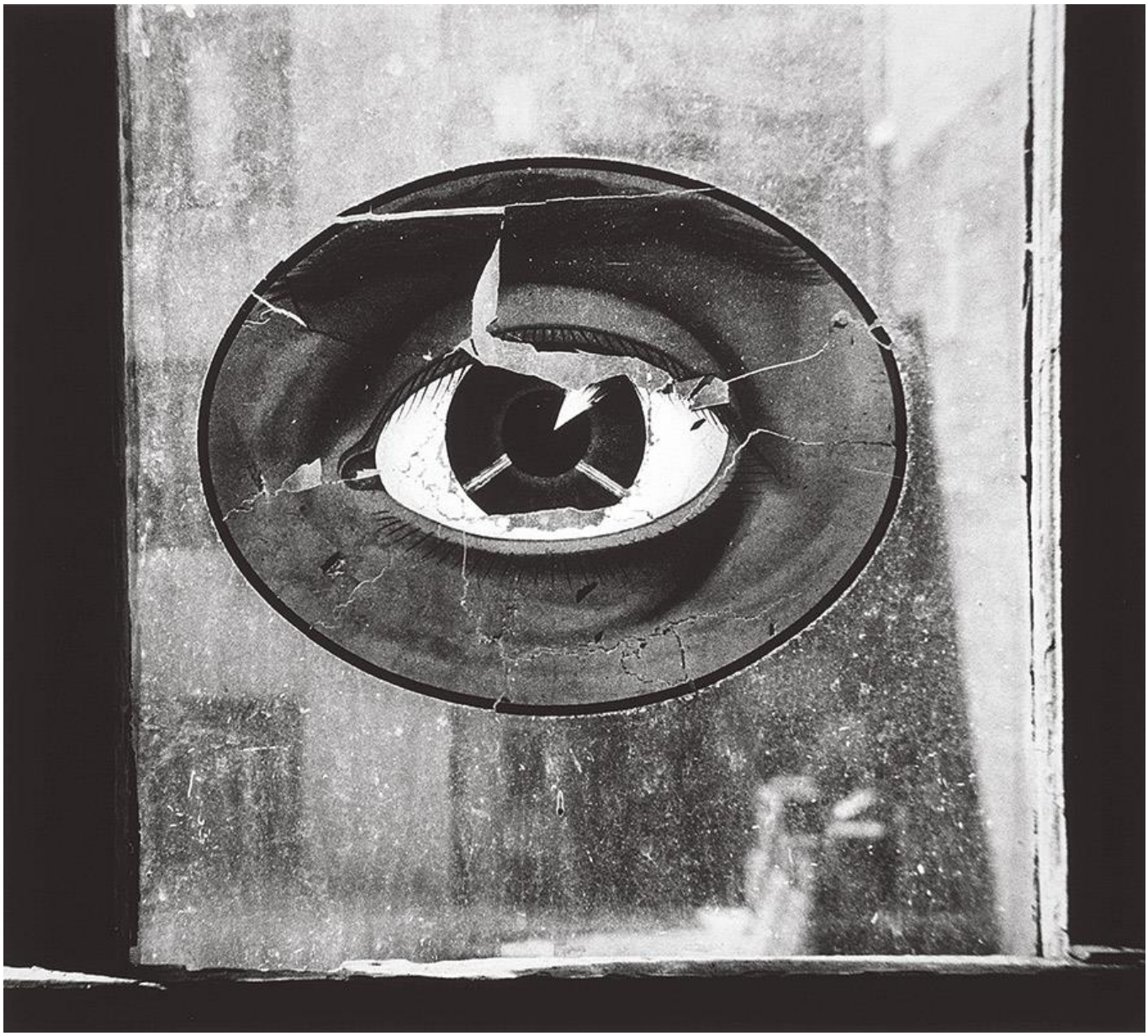
« Résister à la mise sous surveillance totale de nos villes et de nos vies » : c'est l'ambition de la plate-forme Technopolice, lancée par plusieurs associations de défense des droits humains afin de documenter les projets de villes dites « intelligentes ». Pour mieux s'y opposer collectivement. En juin dernier, Félix Tréguer, membre de La Quadrature du Net, décrivait quelques-unes de ces « villes sûres », pointant la *« privatisation sans précédent des politiques de sécurité »* qu'elles favorisent, et fustigeant le *« laisser-faire indolent »* de la CNIL, la Commission nationale de l'informatique et des libertés *(lire aussi Louis Joinet, « Les pièges "liberticides" de l'informatique »).*

Surveiller, analyser, prédire, contrôler

La « ville sûre » ou la gouvernance par les algorithmes

Les outils policiers fondés sur le big data et l'intelligence artificielle se déploient dans de nombreuses villes françaises. À travers des expérimentations pilotées par des groupes privés qui cherchent à se hisser au niveau de la concurrence américaine ou chinoise, la « ville intelligente » révèle son vrai visage : celui d'une cité sous surveillance.

par Félix Tréguer



Nathan Lerner. — « Eye on Window » (L'œil à la fenêtre), 1943

En ce 28 décembre 1948, dans *Le Monde*, le logicien Dominique Dubarle publie l'un des tout premiers articles consacrés aux nouveaux calculateurs mis au point aux États-Unis durant la seconde guerre mondiale. D'emblée, il tente d'anticiper les effets politiques de ce qu'on appellera bientôt l'informatique. La cybernétique balbutie, et le capitalisme de surveillance n'est pas encore d'actualité (1), mais il comprend

déjà que, à terme, cette technologie est appelée à muter en une *« machine à gouverner »* : *« Ne pourrait-on imaginer,* écrit-il, *une machine à collecter tel ou tel type d'informations, les informations sur la production et le marché, par exemple, puis à déterminer, en fonction de la psychologie moyenne des hommes et des mesures qu'il est possible de prendre à un instant déterminé, quelles seront les évolutions les plus probables de la situation ? »* Dubarle prédit que, au gré de l'accroissement des capacités de stockage et de traitement des données, l'informatique conduira au *« surgissement d'un prodigieux Léviathan politique »*.

Soixante-dix ans plus tard, les projets de « ville intelligente » *(smart city)* essaiment dans le monde. Après les États-Unis, la Chine, les pays du Golfe ou le Royaume-Uni, c'est en France que de grands groupes industriels se positionnent sur ces marchés en s'alliant à des élus locaux adeptes du solutionnisme technologique (2). Comme en écho aux prédictions de Dubarle, ils entendent faire proliférer les outils informatiques dans l'espace public urbain pour surveiller, analyser, prédire et contrôler les flux de personnes et de marchandises. Le gouvernement des villes passe ainsi à l'ère de la gouvernance algorithmique. Et, en dehors de quelques initiatives en matière de mise à disposition des données, de gestion « intelligente » de l'éclairage public ou des bennes à ordures, la « ville intelligente » se définit surtout par son volet sécuritaire. À tel point que les industriels parlent désormais de « ville sûre » *(safe city).*

Les documents administratifs liés à ces projets témoignent de la porosité entre la gouvernance urbaine et les doctrines issues du monde militaire. Ainsi, la convention d'expérimentation conclue en juin 2018 entre la mairie de Nice et un consortium de quinze entreprises dirigé par Thales part du constat d'une *« urbanisation galopante à la surface du monde »*. Évoquant des *« menaces de plus en plus importantes »*, elle met sur le même plan les *« risques naturels »*, qui peuvent être liés au dérèglement climatique, et les *« risques d'origine humaine »* (criminalité, terrorisme, etc.). Pas question de s'interroger sur les ressorts économiques, sociaux, politiques de ces phénomènes, et encore moins d'agir sur eux. Il importe avant tout d'*« évaluer chaque situation pour pouvoir anticiper les incidents et les crises »*, d'identifier les *« signaux faibles »* afin de fournir une *« aide à la planification »*, de proposer des *« prédictions sur base de scénarios »*, le tout dans le cadre d'une *« gestion en temps réel »* à travers l'exploitation du *« maximum de données existantes »* au sein d'un *« centre d'hypervision et de commandement »* (3).

Les « risques » sont ainsi réduits à un état de fait dont la puissance publique se contente de gouverner les effets. Chez les concepteurs de la « ville sûre », la police recouvre sa vieille fonction théorisée au XVIIIe siècle : produire un savoir sur la population, orienter sa conduite en agissant sur les variables qui la déterminent, assurer sa docilité et sa productivité. La nouveauté tient à l'abandon de l'horizon décidément trop fuyant de l'« ordre public ». On se contente désormais de gérer le désordre. Grâce à la surenchère technologique, les technocrates croient pouvoir repérer dans la nuée du chaos certaines caractéristiques ou régularités statistiques à partir desquelles on pourra catégoriser, trier, corréler et, in fine, anticiper, prévenir, préempter, ajuster — mais aussi, quand cela sera nécessaire, cibler et réprimer.

Pour ce faire, la « ville sûre » s'appuie sur deux grandes innovations technologiques. D'abord, la possibilité de réunir et d'analyser divers jeux de données, comme les fichiers de police, les informations personnelles glanées en ligne — et en particulier sur les réseaux sociaux —, etc., afin de produire des statistiques et de l'aide à la décision dans une logique de police prédictive. Les outils de surveillance expérimentés depuis dix ans par les grandes agences de renseignement se généralisent à l'ensemble des activités policières...

À Marseille, le projet d'observatoire big data de la tranquillité publique, confié depuis novembre 2017 à l'entreprise Engie Ineo, vise à intégrer des sources issues des services publics municipaux (police, régie de transport, hôpitaux, etc.), mais aussi des *« partenaires externes »*, tels que le ministère de l'intérieur, qui centralise de nombreux fichiers et données statistiques, ou les opérateurs télécoms, dont les données relatives à la localisation des téléphones portables permettent de cartographier en temps réel les *« flux de population »*.

Détection des expressions faciales

Par ailleurs, les citoyens seront appelés à contribuer en fournissant directement des informations (textos, vidéos, photographies, vitesse de déplacement, niveau de stress…) à travers *« une application sur smartphone ou des objets connectés »*. La surveillance des conversations sur les réseaux sociaux comme Twitter ou Facebook est aussi de mise, que ce soit pour *« récupérer les publications dont les thèmes ont un intérêt pour la sécurité de la ville »*, pour *« anticiper la menace »* et évaluer le *« risque de rassemblements dangereux par analyse des tweets »*, ou encore pour procéder à *« l'identification des acteurs »* en repérant *« qui parle, qui agit, qui interagit avec qui »* (4). Pour héberger et traiter ces immenses volumes de données, la ville de Marseille a acquis plusieurs serveurs auprès de l'entreprise Oracle. Elle dispose désormais d'un espace de stockage de six cents téraoctets, soit une capacité équivalant à celle de la Bibliothèque nationale de France pour sa politique d'archivage d'Internet.

Second soubassement technique de la « ville sûre » : l'analyse automatique des flux de vidéosurveillance. Alors que l'État et les collectivités françaises ont investi des centaines de millions d'euros dans l'achat de caméras depuis 2007, et ce pour des résultats dérisoires (5), l'automatisation promet monts et merveilles — et, cerise sur le gâteau, sans embauche de fonctionnaires employés au visionnage. Des projets de vidéosurveillance dite « intelligente » se mettent en place à Toulouse, Nice, Marseille, Valenciennes, Paris, ou encore dans les départements du Gard et des Yvelines.

Le maire de Nice, M. Christian Estrosi, compte parmi les responsables politiques les plus enthousiastes quant au potentiel de ces technologies. En décembre 2018, il faisait adopter par le conseil régional de la région Provence-Alpes-Côte d'Azur (PACA) une délibération autorisant l'expérimentation de portiques de reconnaissance faciale dans deux lycées afin de surveiller les entrées et sorties, en collaboration avec l'entreprise américaine Cisco. Le dernier carnaval de la ville a d'ailleurs servi de laboratoire pour l'expérimentation de dispositifs similaires.

Nice fait également partie de ces municipalités françaises qui entendent coupler la vidéosurveillance à des algorithmes de reconnaissance des émotions. Les édiles ont approché la start-up Two-i pour déployer sa solution dans les tramways de la ville. À Nancy et à Metz, Two-i travaille avec un bailleur social pour évaluer le ressenti des habitants. À Irigny, près de Lyon, la gendarmerie a préféré un concurrent, l'entreprise DC Communication, pour analyser l'« état d'esprit » du public accueilli dans ses locaux. Ces outils issus du « neuromarketing » détectent les expressions faciales associées à la joie, à la tristesse, à la peur ou encore au mépris. *« L'algorithme va ensuite tourner pour mesurer ces émotions et faire ressortir la plus présente »*, explique M. Rémy Millescamps, fondateur de DC Communication et gendarme réserviste.

Si les usages potentiels de la vidéosurveillance « intelligente » ne manquent pas, l'identification automatique d'individus ou de comportements suspects fait figure de priorité. En juin 2018, dans un discours consacré aux doctrines de maintien de l'ordre, l'ancien ministre de l'intérieur Gérard Collomb annonçait des outils d'intelligence artificielle bientôt capables de *« repérer dans la foule des individus au comportement bizarre »*. Une perspective à nouveau évoquée au Parlement français cet hiver, à l'occasion du débat sur la loi antimanifestation adoptée par le gouvernement en réponse au mouvement des « gilets jaunes ». À travers des amendements finalement rejetés, des députés Les Républicains ont tenté de légaliser le couplage des images de vidéosurveillance avec divers fichiers afin d'automatiser *« l'identification des individus dangereux au sein d'une manifestation »*. Outre le cas des militants politiques jugés dangereux ou des personnes suspectées d'activités terroristes, la multiplication des fichiers biométriques — notamment ceux liés à l'immigration, ou le fichier des titres électroniques sécurisés (TES), qui, depuis 2016, agrège les données de tous les demandeurs de carte d'identité et de passeport — rend possible une extension rapide de la reconnaissance faciale à des catégories toujours plus larges (6).

Avec le Royaume-Uni, la France fait aujourd'hui figure de leader européen dans l'utilisation de ces technologies de contrôle social. Alors que, en 2016, ses services de renseignement avaient dû acheter les outils d'analyse de données à l'entreprise américaine Palantir, l'émergence de champions nationaux en matière de big data sécuritaire apparaît désormais comme une priorité. Les projets de « ville sûre » permettent aux sociétés de services aux collectivités, à l'instar d'Engie Ineo, ou de la défense-sécurité, comme Thales, de se positionner sur ces nouveaux marchés face à la concurrence américaine ou chinoise,

avec les encouragements de l'État, qui demeure le premier actionnaire de chacun de ces deux grands groupes (23,6 % et 25,8 % des parts respectivement, et plus d'un tiers des droits de vote dans les deux cas).

Outre les collectivités commanditaires, de nombreux organismes publics participent à ces évolutions. De ce point de vue, le projet de « ville sûre » mené par Thales à Nice est emblématique. Conçu pour suivre les axes thématiques identifiés par le Comité de la filière industrielle de sécurité — qui assure l'interface entre gouvernement et secteur privé —, il bénéficie d'un label délivré par ce même organisme. Au titre du Programme d'investissements d'avenir, la Banque publique d'investissement (Bpifrance) lui a versé une aide de 11 millions d'euros sous forme de subventions et d'avances récupérables, pour un coût total du projet de 25 millions en trois ans. Enfin, plusieurs des technologies proposées ont été mises au point grâce à des projets de recherche associant des acteurs industriels et des organismes publics, comme l'Institut national de recherche en informatique et en automatique (Inria), à travers des financements de l'Agence nationale de la recherche ou de la Commission européenne.

Sur le terrain aussi, la « ville sûre » engage une privatisation sans précédent des politiques de sécurité. L'expertise technique est tout entière confiée aux acteurs privés, tandis que les paramètres qui président à leurs algorithmes resteront selon toute vraisemblance soumis au secret des affaires. Sur le plan juridique, il n'existe à ce jour aucune analyse sérieuse de la conformité de ces dispositifs avec le droit au respect de la vie privée ou avec la liberté d'expression et de conscience, pourtant directement mis en cause. Pour l'heure, seuls les juristes des entreprises concernées veillent, sans zèle excessif, au respect de la législation en vigueur, révisée en 2018 mais déjà dépassée. Les effets politiques de tels déploiements s'annoncent significatifs : surenchère dans le traitement policier de certains quartiers, aggravation des discriminations que subissent déjà certaines catégories de personnes, répression des mouvements sociaux. Ils ne sont, bien entendu, jamais évoqués par les promoteurs.

Quant à la Commission nationale de l'informatique et des libertés (CNIL), elle s'en tient à un laisser-faire indolent. Abritée derrière son manque de moyens et derrière le fait que le règlement européen sur la protection des données personnelles lui a ôté son pouvoir d'autorisation a priori, elle appelle à un *« débat démocratique »* afin que *« soient définis les encadrements appropriés »* (7). Et reconnaît par là l'absence de tout cadre juridique spécifique, ce qui, en vertu de la jurisprudence de la Cour européenne des droits de l'homme, suffit pourtant à démontrer l'illégalité pure et simple de ces projets. Le gouvernement, qui a annoncé une révision de la loi relative au renseignement pour 2020, pourrait quant à lui profiter de ce texte pour blanchir sur le plan législatif les expérimentations en cours, et préparer la généralisation de ces dispositifs de surveillance policière. À moins que des mobilisations citoyennes ne parviennent à les tenir en échec.

Félix Tréguer

Chercheur et membre de La Quadrature du Net.

(1) Lire Shoshana Zuboff, « Un capitalisme de surveillance », *Le Monde diplomatique,* janvier 2019.

(2) *Cf.* Evgeny Morozov, *Pour tout résoudre, cliquez ici. L'aberration du solutionnisme technologique,* FYP Éditions, Limoges, 2014.

(3) « Convention d'expérimentation, de mise à disposition et de démonstration. Projet d'expérimentation "Safe City" » (PDF), 2018.

(4) « Création d'un outil big data de la tranquillité publique et prestations d'accompagnement (2 lots). Cahier des clauses techniques particulières (CCTP) » (PDF), délégation générale adjointe du numérique et des systèmes d'information de la ville de Marseille.

(5) *Cf.* Laurent Mucchielli, *Vous êtes filmés ! Enquête sur le bluff de la vidéosurveillance,* Armand Colin, Malakoff, 2018.

(6) Lire François Pellegrini et André Vitalis, « L'ère du fichage généralisé », *Le Monde diplomatique*, avril 2018.

(7) « La CNIL appelle à la tenue d'un débat démocratique sur les nouveaux usages des caméras vidéo », CNIL, Paris, 19 septembre 2018.

Écouter cet article 14:17 • Lu par Lola Felouzis

2) 17/10/2019 : Le Canard Enchaîné : 5G : un sacré progrès pour le flicage et les pirates

Bonjour,

Article ci-dessous du 6 octobre 2019

Pour la diffusion sur des sites, citez bien le Canard Enchaîné

Denis, pour le collectif Stop Linky 5G Loire

5G : un sacré progrès pour le flicage et les pirates

Grâce à la nouvelle norme téléphonique, c'est la fête aux objets connectés.

Au prix d'une surveillance accrue.

Match de foot ou concert en réalité augmentée, maison intelligente et opérations médicales à distance, industrie numérisée... les opérateurs de téléphonie le proclament : loin d'être un simple saut technologique, la 5G s'apparentera à une véritable révolution. La nouvelle norme de réseaux mobiles (la cinquième génération), qui entrera en service au printemps prochain, va offrir un débit dix fois supérieur à celui de la 4G et un temps de latence (lié à la vitesse de circulation des données en réseau) quasi nul. Plus rapide que l'éclair !

« *Tous les usages de la 5G ne sont pas encore connus* », admet Stéphane Richard, le grand patron d'Orange (France Info, 8/10). « *C'est aux start-up, créateurs, chercheurs et innovateurs de les créer.* » Un horizon prometteur ... mais aussi un brin inquiétant, si l'on songe aux possibles malveillances, intrusions dans la vie privée et autres piratages que devrait bientôt favoriser ce beau progrès technologique.

Petite revue de détail.

Zoomer sur Mbappé

Avec son smartphone 5G haut de gamme, le fan de l'OM ou du PSG pourra suivre un match de foot comme s'il s'agissait d'un jeu vidéo. Il disposera d'une image à 360 degrés (et non plus à 120) de très grande qualité -fournie par des drones 5G- et verra les joueurs évoluer sur le terrain avec différents points de vue. Il aura, en outre, la possibilité de zoomer sur le joueur de son choix et de rejouer la scène à son gré.

A priori ludique, cette vision multifacette et télescopique pourrait, estiment les experts, constituer un magnifique instrument d'espionnage dans l'entreprise ou dans la vie privée...

Ma maison ensorcelée

Au rayon des nouveaux usages : la maison dite « intelligente ». Le concept de domotique n'est pas neuf, mais la 5G risque de décupler l'efficacité des objets connectés pilotant le réglage du chauffage, l'éclairage du four, la gestion du frigo en ligne, voire le verrouillage des portes et des volets. Une véritable forteresse électronique !

Paradoxe : si tout est connecté, tout devient vulnérable ... Comment se protéger d'un pirate informatique prenant le contrôle des alarmes et de la vidéosurveillance ? Et s'il transformait le grille-pain en robot maléfique ?

Roulez, petits chariots !

Au supermarché, doté de son super smartphone, le consommateur n'aura plus à sortir sa carte bancaire. Son chariot sera scanné automatiquement sans passage en caisse, et son compte dûment débité. En prime, un robot à paniers le suivra jusqu'à la maison. Le prototype existe, mais le cadre légal fait encore défaut, qui devra réguler la circulation dans la rue de ce genre de petit bolide. Ce n'est pas comme si les municipalités étaient déjà débordées par les trottinettes et les vélos électriques ...

Opéré comme à la télé

La télémédecine est dans les starting-blocks : opérations ou consultations à distance, prise de tension ou de pression artérielle loin d'un centre de soins... Et, en cas de pépin, qui sera responsable ? Difficile de traîner un robot sur le banc des accusés !

Réseaux très en train

Pour les industriels, la 5G ressemble au Graal. Les plus technophiles en sont sûrs : les avions se poseront plus vite sur le tarmac, la circulation des trains sera optimisée, et les retards de circulation résorbés. Aujourd'hui, le système qui détecte le passage d'un train nécessite des kilomètres de câbles électriques. Demain, les rames seront connectées. C'est pain bénit. Et c'est aussi une chouette opportunité pour un agresseur décidé à paralyser totalement les transports.

Pas d'apéro dans l'auto

Les amoureux de science-fiction seront sans doute déçus : le véhicule autonome roulant pendant qu'on prend l'apéritif à bord avec ses copains, ce n'est pas pour demain ! Avec la 5G, les conducteurs auront tout de même accès à de nouveaux services, telles la présignalisation d'un accident, la détection d'un piéton traversant inopinément ou celle d'une place de parking libre. Et les amendes ? Elles seront virtuelles ? Que nenni ! Un logiciel espion transmettra directement vos coordonnées bancaires au centre des impôts.

Vive le progrès !

Odile Benyahia-Kouider

Une compétition à moindre débit

Les opérateurs de télécoms retiennent leur souffle : dans quelques jours, le gouvernement va rendre publiques les conditions de mise aux enchères des fréquences 5G. En Italie, l'opération a rapporté 6,5 milliards d'euros à l'Etat, soit trois fois plus qu'espéré. Idem en Allemagne : 6,55 milliards d'euros.

La France, elle, a opté pour des... enchères partielles ! Les trois quarts des fréquences mises à disposition seront en effet vendues directement aux quatre opérateurs à un prix fixe déterminé par le gouvernement et qui sera connu avant la fin du mois. C'est dans un second temps, début 2020, que les véritables enchères débuteront sur le dernier (petit) quart restant. Le but de la manœuvre ? Limiter la facture des malheureux opérateurs croulant sous les obligations d'investir.

« *On ne peut pas nous demander d'achever la couverture 4G, de déployer la fibre et, en plus, de débourser des sommes folles pour la SG* », se lamente un ponte de Bouygues Télécom. Xavier Niel, le fondateur d'Iliad, a lui aussi fustigé « *des enchères mortelles* » risquant d'entraîner l'éviction de Free du processus d'attribution (« La Tribune », 3/9). On en finirait presque par oublier que ces boîtes, malgré une concurrence acharnée, continuent de dégager de fastueuses marges à deux chiffres...