Les difficiles choix de l'Europe en matière de 5G

Winston Maxwell, Alain Sibille

LES DIFFICILES CHOIX DE L'EUROPE EN MATIÈRE DE 5G

Par Winston Maxwell et Alain Sibille, Télécom Paris - Institut Polytechnique de Paris

A paraître dans l'Annuaire français de Relations internationales 2021

The European Commission has imposed ambitious 5G roll-out objectives on Member States, including 5G coverage in all major urban areas by 2025. Expensive to build, 5G networks are destined to become the "eyes and ears" of artificial intelligence, permitting the connection of up to 1 million connected devices per square kilometer, as well as highly secure, low latency, communications needed for critical applications like autonomous vehicles. But 5G raises new challenges for society. Though generally more secure than 4G, 5G networks remain vulnerable to state-sponsored actors capable of highly sophisticated cyber warfare. The controversy involving Huawei highlights the complexity of the subject. Health concerns relate to the lack of reliable data on the biological effects of exposure to new 5G frequencies such as millimeter waves. Finally, the combination of 5G and AI create the conditions for a perfect storm in privacy protection. In spite of Europe's GDPR, the connection of billions of sensors to IA platforms is likely to erode the overall privacy environment for Europeans, creating an infrastructure that can easily be misused by governments or private companies for surveillance.

La Commission européenne a imposé des objectifs ambitieux de déploiement de réseaux 5G, dont la couverture au plus tard 2025 de l'ensemble des centres urbains majeurs. Couteux à construire, les réseaux 5G deviendront les yeux et les oreilles de l'intelligence artificielle, permettant la connexion d'un million de capteurs par kilomètre carré, ainsi que des communications sécurisées avec faible temps de latence, nécessaires pour les applications critiques telles que les véhicules autonomes. La 5G soulève de nouveaux défis sociétaux. Plus sécurisée que la 4G, la 5G reste une cible pour des acteurs étatiques capables de mener des cyber-attaques sophistiquées. La controverse autour de l'équipementier Huawei illustre la complexité du sujet. Le souci en matière de santé concerne le manque de données fiables sur les effets biologiques des nouvelles fréquences utilisées pour la 5G, notamment les ondes millimétriques. Enfin, la combinaison de la 5G et de l'IA crée des conditions propices à dégrader le niveau de protection des données personnelles en Europe. Malgré le RGPD, la connexion de milliards de capteurs à des plateformes d'IA constitue une infrastructure qui peut facilement être détournée par l'État ou par les sociétés privées à des fins de surveillance.

1. L'Europe et la course à la 5G

Dans son plan ambitieux sur la société européenne du gigabit et son plan d'action sur la 5G, la Commission européenne propose une série d'objectifs ambitieux, dont la disponibilité, au plus tard en 2025, d'un service 5G dans toutes les villes majeures de l'Union européenne ainsi que le long des grands axes de transport terrestre (3, 4). Un observatoire européen de la 5G a été créé, et les conditions d'accès au spectre et les conditions d'installation de sites et de partage d'infrastructures 5G ont été clarifiées, grâce au nouveau Code européen des communications électroniques. La Commission a proposé de cofinancer à auteur de 700 millions d'euros des expérimentations dans le cadre de partenariats publics-privés.[1] La Commission a présenté la 5G comme une course internationale que l'Europe doit gagner, ou au moins ne pas perdre (4). Le sentiment d'urgence a été renforcé par la crise COVID 19, qui a souligné la dépendance de chaque citoyen et entreprise en Europe aux réseaux haut débit. En matière de 5G l'Europe

[1] 5g-ppp.eu

dispose d'atouts considérables, notamment au travers de deux équipementiers (Nokia et Ericsson), compétitifs sur un marché mondial où la lutte des brevets et normes est féroce. La Commission a souligné l'échec relatif de l'Europe dans le déploiement de la 4G, où les États Unis ont atteint très vite une couverture de 75% de la population contre 28% en Europe (5). La volonté politique de créer une industrie européenne de la 5G forte et autonome est également le résultat de l'hégémonie américaine sur les services internet et *cloud*, mal vécue par certains États membres dont la France, et que l'Europe ne souhaite pas voir se reproduire en matière de 5G, d'IA et l'internet des objets (IoT pour « *Internet of Things* »). Enfin la 5G, l'IA et l'IoT sont porteurs d'une transformation économique génératrice de croissance et d'emplois en Europe, 2,3 millions d'emplois selon la Commission (5). Tous ces facteurs poussent la Commission et les États membres à encourager les opérateurs à déployer les réseaux 5G rapidement, malgré un contexte économique difficile.

2. La 5G: une technologie prometteuse

    a. La bataille des "G" : une histoire semée de controverses et de rivalités

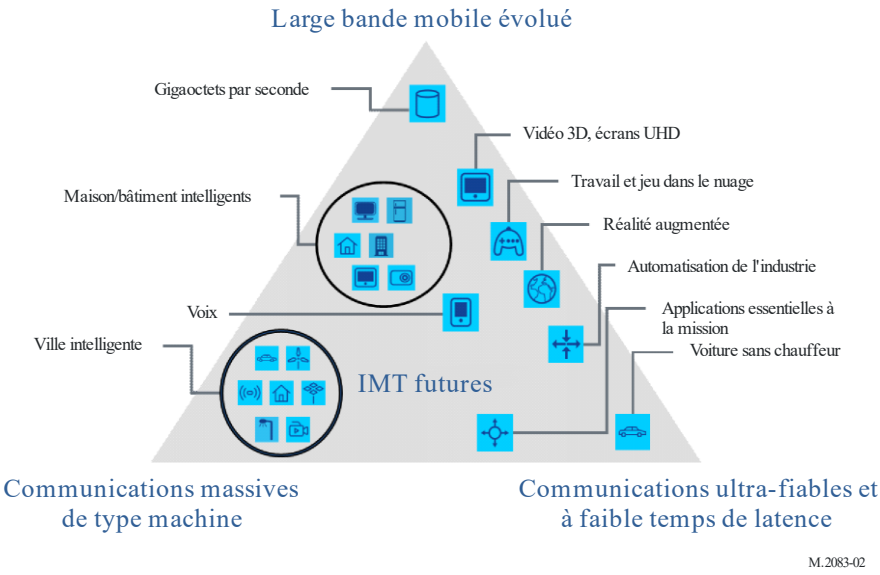
L'histoire des générations de téléphonie mobile démarre dans les années 80, en France selon la norme Radiocom 2000. Il s'agissait d'une technologie cellulaire mais principalement analogique, très coûteuse et donc réservée à des usages professionnels exigeants. La 2G (« GSM ») a marqué l'avènement de l'accès au grand public avec une technologie pleinement numérique dont le développement commercial a largement dépassé les espoirs des concepteurs. L'équivalent américain (IS-95) repose sur une technique différente (CDMA), incompatible avec le GSM. La 3G a vu un combat assez long dans le cadre de la normalisation, les divers champions sur la scène mondiale cherchant à imposer leur propre standard afin de capter le marché au travers de l'avantage concurrentiel apporté par la propriété des brevets critiques. A l'arrivée, cela a abouti à autant de normes que de grandes régions, puisque le standard américain (CDMA 2000) cohabite avec l'européen (UMTS) et même le chinois (TDSCDMA). Enfin la 4G (LTE) a permis la réconciliation, ayant été normalisée par l'ETSI (organisme européen de standardisation) selon les spécifications de l'Union Internationale des Télécommunications (UIT).

    b. L'apport technologique de la 5G par rapport à la 4G

Chaque nouvelle génération de téléphonie mobile met en avant un ensemble de techniques novatrices par rapport aux générations précédentes, propres à faciliter le développement de nouveaux services ou amplifier les services existants. Certaines d'entre elles, envisagées au départ, ne verront finalement pas le jour ou en tous cas à court terme, d'autres sont bien prévues et constitueront même le cœur de la novation technologique de la 5G. C'est le cas du « MIMO massif », consistant à placer au niveau des stations de base des panneaux comportant un grand nombre d'antennes élémentaires (ex. 128). La focalisation fine des ondes permises par cette technique permet de connecter simultanément beaucoup plus d'utilisateurs et donc d'augmenter fortement la capacité globale du réseau. D'autres idées sont beaucoup plus classiques, reposant sur l'augmentation du « spectre » alloué par la réglementation, soit dans les bandes inférieurs à 6 GHz, soit dans les bandes dites millimétriques, ex. aux alentours de 28 GHz ou au-delà. Toutefois il est probable que ces dernières, très contraintes par les caractéristiques physiques de la propagation (fortement directive, facilement bloquée par les obstacles), ne seront employées que de manière limitée (ex. pour relier sans fil des antennes déportées à des équipements centralisés).

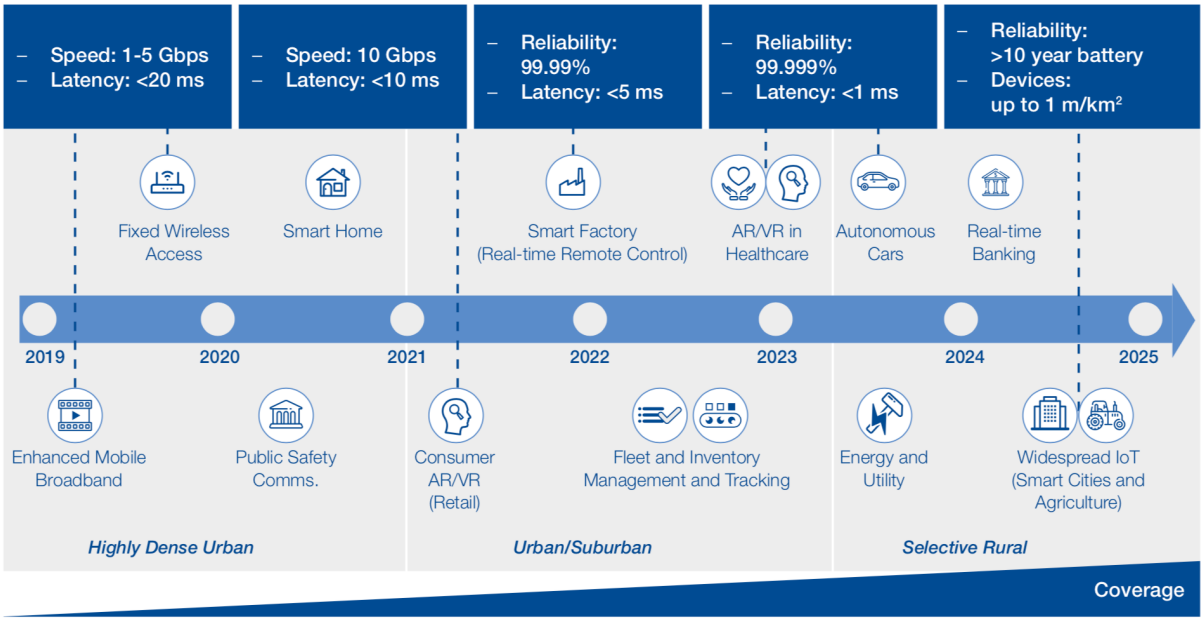
    c. Les nouveaux usages

La véritable novation de la 5G porte sur les usages, qui vont bien au-delà de la téléphonie traditionnelle ou même de l'accès haut débit tel que popularisé par la 4G. Elle ouvre en effet l'accès radio cellulaire, donc contrôlé et réglementé, à des dispositifs industriels, professionnels et du domaine privé leur permettant d'échanger des informations ainsi qu'avec des systèmes de traitement des données. La 5G se présente donc comme une technologie « phare » pour l'IoT en fixe ou en mobilité, par exemple pour la voiture connectée. Les services 5G permettront la connexion jusqu'à 1 million d'objets par kilomètre carré, soit mille fois plus qu'en 4G, avec un temps de latence d'une milliseconde, soit 50 fois inférieur à celui de la 4G (50 ms). La standardisation au niveau mondial et l'accès généralisé permettront de baisser fortement les coûts de l'IoT et d'en faciliter la dissémination rapide pour des besoins extrêmement diversifiés. On peut donc attendre que la 5G aura un effet « booster » espéré depuis de nombreuses années pour l'IoT. Un aspect très important à ce titre sera la possibilité étendue de développer des services très modulables au travers du « *slicing* » (tranche de réseau), i.e. la programmation de services définis très finement en termes de qualité de service (latence, débit, priorité, taux d'erreur…), ouvrant la possibilité pour des fournisseurs de services d'entrer sur le marché, se positionnant entre les opérateurs et les usagers de ces services.



Source : (28)

Toutes les possibilités de la 5G ne seront pas disponibles dès le premier jour. Dans un premier temps les réseaux 5G s'appuieront en partie sur l'infrastructures 4G, servant principalement à augmenter la capacité de celles-ci pour l'accès haut débit – une sorte de « 4G + » (8). Les innovations les plus fortes viendront dans un second temps, lors de l'émergence de réseaux 5G autonomes (*standalone*) capables de soutenir les communications massives ainsi que les communications ultra-fiables et à faible temps de latence. Le World Economic Forum prévoit une introduction progressive de ces nouvelles capacités sur une période de cinq années (31):



AR = augmented reality; VR = virtual reality; IoT = internet of things.
Source: PwC Strategy& and World Economic Forum, "5G for the Fourth Industrial Revolution", 2019.

Source : (31)

d. La 5G: partenaire indispensable de l'IA

En permettant de connecter des milliards de capteurs à faible coût, la 5G deviendra les « yeux et les oreilles » de l'IA, permettant de récolter des données qui seront ensuite interprétées par les modèles d'apprentissage machine. Aujourd'hui l'IA s'appuie essentiellement sur le traitement de données massives générées par des navigateurs internet et *smartphones*. La Commission constate que l'Europe a manqué le tournant de l'IA pour ces types de données consommateurs (achats en ligne…), laissant la place aux géants américains (9), mais elle pense aussi que l'Europe peut devenir leader pour les applications *B2B* de l'IA (industrie 4.0, santé, transports, environnement, énergie, agriculture, administrations publiques, villes intelligentes…). La facilitation permise par le *slicing* et l'attribution de règles de sécurité et de qualité spécifiques et la forte densité de connections y contribueront, de même que l'autonomie des dispositifs (10 ans ou plus). En réduisant le temps de latence, la 5G facilitera également des applications critiques de l'IA telles que la communication en temps réel entre véhicules pour éviter des collisions. Enfin, l'architecture des réseaux 5G permettra le déplacement vers les extrémités du réseau de certaines fonctions de calcul (*edge computing*) ce qui facilitera les applications gourmands en calculs, du type *machine learning*. Compte tenu de tous ces aspects, la technologie 5G va devenir un partenaire essentiel pour l'IA, surtout dans des domaines industriels et professionnels que la Commission européenne espère prioriser en Europe.

e. La 5G soulève des controverses

La 5G ne fait pas que des heureux. Sur le plan économique, le déploiement de la 5G sera beaucoup plus coûteux que la 4G, nécessitant la construction d'un réseau plus dense d'antennes et d'infrastructures de collecte (*backhaul*), certaines en fibre optique. Pour tirer parti de toutes les possibilités de la 5G, il faut construire jusqu'à 800 sites d'accès (*small cells*) par km², s'appuyant sur un réseau dense de fibre optique. Pour simplifier le déploiement et réduire les coûts, le nouveau Code européen des Communications électroniques encourage le partage d'infrastructures, le co-investissement, et l'émergence d'opérateurs d'infrastructures sur le marché de gros (*wholesale only*). Toutefois un unique réseau partagé amène à une forme de monopole, allant à l'encontre de la politique de la Commission européenne en matière de

concurrence depuis plus de vingt ans. Certains économistes aussi posent la question de la viabilité des investissements à un moment où ceux de la 4G ne sont pas encore amortis et où la demande des usagers et leur propension à dépenser plus pour de nouveaux services est incertaine (26). D'autres acteurs dénoncent la présentation de la 5G comme une course essentielle pour l'Europe, qui serait entretenue par les équipementiers pour relancer les investissements (26, 27). Enfin, *last but not least*, la 5G soulève des préoccupations majeures en matière de vulnérabilité accrue aux cyberattaques, d'éventuels effets sur la santé, et de surveillance généralisée, que nous examinons ci-dessous.

3. 5G et cybersécurité

    a. Des objets aux services : une sécurité de bout en bout

Les objets connectés, potentiellement en très grand nombre et largement disséminés, constituent la porte d'entrée vers les réseaux et peuvent constituer un point névralgique en matière de sécurité., leur démultiplication augmentant la « surface d'attaque » disponible pour des acteurs malveillants (8). S'agissant (pour l'IoT) de dispositifs très simples et peu coûteux, disposant de faibles ressources énergétiques, les capacités de calcul et les protections matérielles ne peuvent être qu'extrêmement limitées. Il s'y ajoute, et c'est un point essentiel, que c'est souvent l'humain, par négligence ou par méconnaissance, qui est le maillon faible. La démarche de « *privacy by design* » fait partie des approches aujourd'hui privilégiées, notamment dans le contexte de plus en plus important de la protection des données personnelles. L'objectif est d'assurer une sécurité « de bout en bout », pour un service donné. La question de « modèles de confiance » n'est d'ailleurs pas indépendante des modèles économiques, dans la mesure où il y a un coût pour la sécurité et où il faut en trouver le juste niveau. La sécurité d'un réseau reliant des capteurs dans une voiture sera différente de celle reliant des capteurs de poubelles municipales. Tout ceci fait l'objet, dans le contexte 5G, de travaux qui se poursuivent, nécessitant la standardisation des processus et des architectures, puis l'adoption de réglementations coordonnées internationalement. Les services concernés seront très nombreux, chacun instancié par une « tranche de réseau » i.e. par l'explicitation des ressources techniques nécessitées par ce service et la plupart restent à définir précisément. Même si chaque service sera instancié par une tranche de réseau (ce qui contribue à augmenter la sécurité), certains auront vocation à fonctionner entre eux, le niveau de sécurité de l'ensemble étant dicté en grande partie par celui du maillon le plus faible. La 5G permettra l'intégration de couches logicielles plus développées, ce qui facilitera le cryptage des données de bout en bout, un autre atout pour la sécurité.

    b. Le cœur de réseau et les menaces étatiques

Compte tenu de ces éléments, la 5G sera globalement plus sûre que la 4G lorsqu'il s'agit de cyber-menaces classiques. La menace restera élevée, cependant, à l'égard d'acteurs étatiques capables de mener des stratégies de cyberguerre sophistiquées. Or, du fait de son installation en profondeur dans notre société technologique, la 5G nous rendra plus vulnérable en cas d'attaque réussie sur les équipements des opérateurs (« cœur de réseau »). En effet, il est possible de cacher dans les circuits électroniques ou les logiciels embarqués des morceaux de processeur ou de code informatique susceptibles d'être activés de façon malveillante, puisque par définition ces équipements sont reliés à l'extérieur. Bien que la sécurité des systèmes électroniques fasse l'objet depuis plusieurs décennies de recherches et de développements d'outils de détection, une garantie absolue est impossible si de tels « chevaux de Troie » ont été introduits avec un haut niveau de connaissance et des moyens importants, tels qu'un État en est capable. Les acteurs malveillants financés par un état étranger constituent le risque principal identifié (23), ce qui nourrit un débat vif sur l'utilisation d'équipements chinois dans le cœur de

réseau. Il s'y ajoute que la « softwarisation » des réseaux fait que leurs fonctionnalités et leur opération repose largement sur du logiciel (on parle de programmation des réseaux, de virtualisation). Ceci ouvre à des possibilités multiples d'introduction de codes malveillants, susceptibles ultimement de casser un réseau entier ou de l'exploiter à des fins dramatiques.

c. L'enjeu de souveraineté et de sécurité nationale

Comme indiqué plus haut, la 5G permettra la connexion de millions d'objets profondément impliqués dans la vie économique et sociale du pays. Deux risques se superposent : d'une part un risque de dépendance par rapport à des composants et technologies étrangers, d'autre part un risque de vulnérabilité par rapport à une cyber-attaque par un acteur étranger. La crise Covid-19 nous a éclairé sur les risques des ruptures d'approvisionnement, ainsi que sur la dépendance accrue de l'économie aux réseaux haut débit. Pour gérer le risque de rupture d'approvisionnement, la Commission européenne recommande aux États membres de ne jamais dépendre d'un seul fournisseur et d'évaluer le risque lié aux ruptures d'approvisionnement pour chaque élément de réseau 5G (8). En ce qui concerne les cyber-attaques, l'analyse de risque conduit par le groupe européen de coopération en matière de cyber-sécurité NIS confirme que les acteurs étatiques seront les principaux adversaires capables de pénétrer au cœur du réseau, et recommande d'écarter des fournisseurs à haut risque, au moins pour les parties sensibles du réseau (21, 23).

Les États-Unis, le Royaume-Uni, l'Australie, et le Japon, entre autres, ont de leur côté décidé de bannir entièrement l'utilisation d'équipements Huawei dans les réseaux 5G, ce fournisseur étant considérée comme trop proche du gouvernement chinois, gouvernement par ailleurs accusé d'avoir lancé des cyberattaques contre plusieurs pays occidentaux. La réalité de ce risque est difficile à évaluer. D'une part, la décision américaine de bannissement s'insère dans un jeu d'échecs plus large sur le commerce international, les risques sécuritaires pouvant servir à faire la pression sur la Chine dans d'autres domaines. Certaines études ont révélé des défaillances dans les règles de sécurité appliquées par Huawei (17), voire l'existence potentielle de portes dérobées dans 55% des produits testés (15). Tout en admettant la nécessité d'améliorer ses processus de sécurité, Huawei conteste évidemment l'existence de portes dérobées. Ceci n'a pas empêché la FCC (régulateur américain des télécommunications) de considérer que Huawei posait un risque excessif pour les réseaux 5G américains (12), de même que le gouvernement britannique, qualifiant l'entreprise de "haut risque" en raison de sa proximité instituée avec les services de sécurité chinois (30). Enfin le parlement européen a émis des recommandations visant particulièrement les fournisseurs chinois d'équipements 5G, soulignant les risques pour l'autonomie stratégique de l'UE (25). La Commission européenne (7) a laissé à chaque État membre la liberté d'effectuer leur propre évaluation du risque, mais la boîte à outils élaborée par le groupe de coopération NIS souligne la nécessité de prendre en considération le risque d'interférence d'États tiers, prenant en considération leurs systèmes politique et juridique (22).

La situation reste complexe car Huawei dispose d'une forte avance sur ses concurrents, qui a amené les nouveaux entrants 5G de plusieurs pays européens à choisir Huawei afin d'accélérer leur déploiement, créant une dynamique concurrentielle saine favorisée par le cadre réglementaire européen. Pour cette raison, la position française et d'autres pays européens était jusqu'à présent assez modérée mais elle est en train d'évoluer, notamment sur le conseil de l'ANSSI (Agence nationale de la sécurité des systèmes d'information). Le déploiement de certains équipements est désormais soumis à un régime d'autorisation préalable, « fondé sur des motifs de défense et sécurité nationale ».

Malgré la pression exercée par les États-Unis, l'Europe tente de maintenir une position plus nuancée, évitant de faire un procès d'intention à l'encontre de l'équipementier chinois, d'où l'élaboration d'une boîte à outils contenant une méthodologie commune d'analyse de risque. En application du Traité sur le fonctionnement de l'Union européenne, les questions de sécurité relèvent de la compétence exclusive de chaque État membre, ce qui empêche la Commission d'imposer une règle unique. Chaque État membre doit développer sa propre doctrine fondée sur une analyse des risques, mais la Commission et l'ENISA essaient d'harmoniser les réponses le plus possible.

4. 5G et santé

a. Les incertitudes des mécanismes physiologiques

Le large déploiement des réseaux mobiles à partir du milieu des années 90 a créé dans une partie de l'opinion, notamment au sein d'associations activistes ou dans des groupes de personnes comme les « hypersensibles », l'idée que les ondes électromagnétiques liées à l'exploitation de ces réseaux pouvaient créer des risques en matière de santé publique. Depuis cette époque, de nombreux travaux de par le monde ont visé à confirmer ou infirmer ces craintes, et à quantifier l'exposition aux ondes électromagnétiques. Il s'est ensuivi l'établissement de normes limitant la puissance émise ou le champ électromagnétique, supposant garantir la sécurité sanitaire des personnes. Les seuils en Europe sont définis par une recommandation de 1999, qui reste valable aujourd'hui.[2] La difficulté fondamentale du problème vient du fait qu'aucun mécanisme physiologique établi ne soutient cette notion de risque, contrairement par exemple aux rayonnements ionisants dont on connaît les mécanismes destructeurs. Les champs auxquels est exposée la population générale ne peuvent créer que des effets athermiques, dont l'impact physiologique est très mal connu. Un argument des opérateurs et constructeurs est d'ailleurs que les plafonds de champs autorisés par les normes réglementaires ne sont jamais atteints et, le plus souvent, de très loin. Or ces plafonds (ex. 61 V/m entre 2 et 300 GHz) ont été choisis pour déjà assurer une bonne marge par rapport à des effets thermiques.

b. La rationalité de la physique

Il convient déjà de distinguer, pour un individu donné, ce qui provient des émetteurs du réseau, qui lui est imposé et sur quoi il n'a aucun contrôle, de ce qui provient des dispositifs (ex. *smartphone*) utilisés par lui-même ou son entourage. Le premier (exposition descendante) est beaucoup plus faible que le second (exposition montante) car les personnes ne sont jamais très proches des émetteurs et la puissance décroît avec le carré de la distance, voire avec le cube de la distance ou pire en cas d'obstructions entre l'émetteur et le récepteur (typiquement en zone urbaine dense). Ainsi, la proximité entre l'antenne du réseau et l'utilisateur est un facteur favorable, conduisant à réduire la puissance émise nécessaire, qui est de toute façon contrôlée à la valeur juste nécessaire. Par conséquent, la densification du réseau prévue pour la 5G (cellules plus petites) conduit non seulement à en augmenter la capacité mais aussi à « régulariser » le rayonnement émis, moins variable d'un point à un autre.

c. Les spécificités de la 5G par rapport aux générations précédentes

La finesse du faisceau permise par les antennes de type « MIMO massif » permet de ne rayonner qu'en direction de l'utilisateur visé, ce qui est bénéfique à la fois en termes énergétiques et en termes d'exposition puisqu'une personne dans une direction différente ne recevra qu'un faible

[2] Recommandation 1999/519/CE du Conseil du 12 juillet 1999 relative à la limitation de l'exposition du public aux champs électromagnétiques (de 0 Hz à 300 GHz)

rayonnement. Toutefois cet argument ne tient pas dans les zones à forte densité d'utilisateurs, un des grands intérêts de ces antennes étant de pouvoir communiquer simultanément vers ceux qui sont dans diverses directions. Dans les zones denses (centres urbains, centres commerciaux, zones événementielles…), la 5G permettra une gestion beaucoup plus efficace de l'énergie consommée par les équipements du réseau, par exemple grâce à des modes de « somnolence » lorsque peu d'utilisateurs sont actifs. Au global, la consommation de données mobiles grandissantes est un facteur d'augmentation générale des champs électromagnétiques ambiants, souvent efficacement compensé par un bien meilleur contrôle des émissions par rapport aux besoins.

Les fréquences principalement utilisées par la 5G se situent autour de 3.5 GHz, c'est-à-dire modérément au-dessus de la 4G (2.6 GHz), ainsi que dans la bande 28 GHz, dite bande « millimétrique », actuellement utilisée pour les scanners corporels dans les aéroports. Ces fréquences millimétriques se comportent quantitativement assez différemment des bandes basses et moyennes, car la profondeur de pénétration se réduit fortement avec la montée en fréquence. Ainsi à 28 GHz elle n'est que de quelques millimètres dans le corps humain, alors qu'aux fréquences basses comme le GSM (0.9 ou 1.8 GHz) les ondes peuvent pénétrer profondément et atteindre les organes. Si effets sanitaires il devait y avoir, ils seraient donc très différents selon la fréquence. Un rapport du Parlement européen souligne l'absence de recul sur les effets biologiques des ondes électromagnétiques, et l'incapacité pour les chercheurs de reproduire, et donc d'étudier, l'environnement électromagnétique complexe qui existera dans une zone couverte par des antennes 5G (27). Certaines études ont conclu à l'existence d'effets biologiques (19, 27), mais ces études restent controversées, les effets biologiques éventuels restant mal compris. L'agence française ANSES a constaté l'absence de données relatives aux effets biologiques et sanitaires potentiels dans les bandes de fréquences 3,5GHz et 28GHz prévues pour la 5G (2).

180 scientifiques et médecins ont demandé à la Commission européenne un moratoire sur le déploiement des réseaux 5G jusqu'à ce que les effets sanitaires sur la population et sur l'environnement puissent être mieux étudiés (20). La Commission a répondu à l'appel de ces scientifiques en soulignant le caractère rigoureux des études effectuées par les instances européennes (études qui confirment le caractère adéquat des seuils actuels d'exposition), et en indiquant qu'un moratoire serait disproportionné compte tenu des bénéfices sociétaux de la 5G, y compris pour la santé (6). La Chine impose des seuils d'exposition *inférieurs* à ceux recommandés en Europe, ce qui conduit à des problèmes de couverture à l'intérieur des immeubles pour les réseaux 4G (29). L'une des priorités de la Chine pour le déploiement 5G serait donc de combler ce problème de couverture à l'intérieur des immeubles par l'augmentation du nombre de *small cells* (26).

5. La 5G et la protection de la vie privée

Permettant la connexion d'un million de capteurs par km², la 5G incarne une société ou chaque aspect de la vie sera transformé en un flux de données qui seront stockées et analysées afin de conduire, via l'IA, à des décisions individuelles et collectives plus sages. Cela crée évidemment des opportunités pour améliorer le bien-être de tous : gestion d'épidémies, réduction de la pollution, réduction d'inégalités sociales. Mais le revers de la médaille est que la 5G met en place une infrastructure où la collecte de données massives devient la norme. Une telle infrastructure pourrait contribuer à la surveillance généralisée des personnes, que ce soit par des sociétés privées ou par l'État, avec un risque de détournement à des fins contestables pour des raisons politiques ou sécuritaires (1). Le Règlement général sur la Protection des Données personnelles (RGPD) établit les principes d'un traitement de données respectueux des droits et libertés

individuelles, en interdisant la collecte excessive de données, en imposant le traitement pour des finalités spécifiques, en encadrant le profilage, et en décourageant l'interconnexion des bases de données. Néanmoins, comme la construction d'autoroutes et de voitures puissantes contribue aux excès de vitesse, la construction d'une infrastructure de capteurs 5G contribuera inévitablement à des excès en matière de traitement de données personnelles, rendant l'application des principes du RGPD plus difficile. De plus, le risque de détournement ne peut être écarté : un réseau 5G intégré dans un projet *smart city* pourrait potentiellement être utilisé pour surveiller des manifestants ou des opposants politiques (13, 14, 16).

La tension entre l'utilité sociale d'un réseau dense de capteurs du type *smart city* et la protection de la vie privée se manifeste aujourd'hui dans la mise en place d'infrastructures de vidéo-surveillance dans les villes. Les autorités de protection des données personnelles veillent à ce que les caméras se limitent à des emplacements où leur utilisation apporte une vraie valeur ajoutée pour la sécurité de la ville, par exemple devant un distributeur automatique de billets ou dans un hall de gare. Les autorités de police, quant à elles, préféreraient un maillage plus fin de la ville, pour rendre le contournement du dispositif plus difficile pour les criminels et augmenter l'impression de sécurité pour les citoyens. Ces deux principes — d'une part limiter l'installation des caméras au strict nécessaire afin de préserver la vie privée, d'autre part assurer une couverture dense pour protéger la sécurité publique — nécessitent une mise en balance au cas par cas, dans le respect du principe de proportionnalité. Les autorités de protection des données à caractère personnel tiennent compte notamment de la possibilité d'un éventuel détournement d'un dispositif, l'effet « cliquet » lié à la mise en place d'un nouveau dispositif technologique, et la banalisation progressive d'une société de surveillance. Ces risques sont mis en face de l'effet utile du dispositif pour la lutte contre la criminalité. Actuellement la mise en balance s'effectue application par application. En favorisant la connexion (et l'interconnexion) de millions d'objets IoT la 5G rendra plus difficile l'application les principes du RGPD et notamment celui de « privacy by design » qui exige d'évaluer la nécessité et l'utilité de chaque application par rapport aux risques pour la vie privée. Les capteurs et les applications associées seront installés et gérés par une multitude d'acteurs différents, sans autorisation ni concertation préalable. Même si chaque acteur de la chaîne veille au respect du RGPD pour sa partie, l'effet cumulé de ce réseau dense de capteurs interconnectés sera de créer une infrastructure propice à la surveillance généralisée, sans qu'un seul acteur ne soit responsable de cette évolution.

La tension évidente entre la 5G et les droits fondamentaux se retrouve dans les déclarations politiques de la Commission européenne, qui déclare à la fois vouloir créer des espaces communs de partage de données, alimentés en partie par l'Internet des objets et les réseaux 5G, et défendre le modèle européen en matière de protection des données à caractère personnel. Les deux objectifs semblent contradictoires. La Commission essaie néanmoins de créer une « voie européenne » capable de concilier les deux principes : « *Afin de réaliser le potentiel de l'Europe, nous devons trouver notre propre voie européenne, en équilibrant le flux et la large utilisation des données, tout en préservant des normes élevées en matière de protection de la vie privée, de sécurité, de sûreté et d'éthique* » (9).

5G, IA et développement des villes intelligentes seront donc des progrès à double tranchant : ils apporteront de nouveaux services, dont certains seront très utiles pour la collectivité, mais ils auront aussi besoin d'une infrastructure potentiellement détournable et plus facilement contrôlable par un pouvoir local que l'internet actuel. La réponse souhaitable n'est pas d'interdire la 5G, mais de mettre des garde-fous, par exemple via des instances de contrôle dont la mission serait de mesurer les risques posés par l'omniprésence de capteurs et d'infrastructures 5G par

rapport aux droits et libertés individuels. Dans un pays comme la France, une telle mission pourrait impliquer conjointement l'ARCEP et la CNIL.

6. La course pour la 5G met en évidence des objectifs contradictoires

La Commission européenne comme les acteurs privés (équipementiers, opérateurs) semblent globalement très moteurs dans la course pour le déploiement de la 5G. Toutefois, ce déploiement pose de nouvelles questions et met en lumière des objectifs contradictoires qui devront être mis en balance. Les coûts d'investissement et de fonctionnement poussent vers une coopération accrue entre opérateurs, voire vers le partage d'infrastructures, pouvant entrer en conflit avec la politique concurrentielle de la Commission. Les fortes restrictions imposées aux équipementiers chinois peuvent s'avérer justifiées pour garantir la sécurité, mais cette interdiction handicapera certains opérateurs, réduisant la concurrence en Europe. L'UE souhaite coopérer avec la Chine en matière de normes 5G (18), mais elle ne saurait ignorer le contexte géopolitique caractérisé par une guerre commerciale entre les États-Unis et la Chine, ainsi que le risque lié à l'espionnage et à la possibilité de cyberguerre provenant de puissance non-européennes, dont la Chine. En matière de santé, il manque surtout d'études sur les effets des fréquences millimétriques, mais imposer à ce titre un moratoire sur le déploiement de la 5G serait disproportionné et priverait les citoyens européens de nouveaux services par ailleurs bénéfiques. Enfin, l'Europe ambitionne de catalyser l'industrie et le monde professionnel par l'exploitation de données issues en grande partie des réseaux 5G, tout en préservant le modèle européen de protection des données à caractère personnel. Pour certains, ces objectifs sont difficilement conciliables, la création d'une société hyper connectée conduisant nécessairement à l'affaiblissement progressif de ce modèle. Il est possible que, sans encadrement strict, les dispositifs IoT de toutes sortes et les applications interconnectées mènent à une société où l'individu subirait bon gré mal gré une surveillance de tous les instants.

Remerciements

Les auteurs remercient Houda Labiod, professeure à Télécom Paris, pour ses apports concernant les aspects techniques de la sécurité des réseaux 5G.

Références

1) Ross Anderson, ‘China is What Orwell Feared’, *The Atlantic*, 29 juillet 2020.

2) ANSES, ‘Exposition de la population aux champs électromagnétiques liée au déploiement de la technologie de communication 5G et effets sanitaires associés’, Rapport préliminaire, octobre 2019.

3) Commission européenne, ‘Connectivité pour un marché unique numérique compétitif – vers une société européenne du gigabit’, Communication COM(2016) 587 final, 14 septembre 2016.

4) - - , ‘Un plan d’action pour la 5G en Europe’, Communication COM(2016) 588 final, 14 septembre 2016.

5) - -, ‘5G Global Developments’, Staff Working Document SWD(2016) 306 final, 14 septembre 2016.

6) - -, Lettres aux professeurs Nyberg et Hardelle, 13 octobre 2017 et 29 novembre 2017.

7) - -, ‘Cybersécurité des réseaux 5G’, Recommandation (UE) 2019/534, 26 mars 2019.

8) - -, ‘La sécurité du déploiement de la 5G dans l’UE – Mise en œuvre de la boîte à outils de l’UE’, Communication COM(2020) 50 final, 29 janvier 2020.

9) - -, ‘Une stratégie européenne pour les données’, Communication COM(2020) 66 final, 19 février 2020.

10) - -, ‘Intelligence artificielle – Une approche européenne axée sur l’excellence et la confiance’, Livre Blanc COM(2020) 65 final, 19 février 2020.

11) European Network and Information Security Agency (ENISA), ‘Threat Landscape for 5G Networks’, novembre 2019.

12) Federal Communications Commission (FCC), ‘Order on Protecting Against National Security Threats on the Communications Supply Chain Through FCC Programs – Huawei Designation’, 30 juin 2020.

13) Steven Feldstein, ‘The Global Expansion of AI Surveillance’, *Carnegie Endowment for International Peace, Working Paper*, septembre 2019.

14) - -, ‘The Road to Digital Unfreedom: How Artificial Intelligence is Reshaping Repression’, *Journal of Democracy* vol. 30 n° 1, janvier 2020.

15) Finite State, ‘Supply Chain Assessment, Huawei Technologies Co., Ltd.’, 2020.

16) Sue Halpern, ‘The Terrifying Potential of the 5G Network’, *The New Yorker*, 26 avril 2019.

17) Huawei Cyber Security Evaluation Centre (HCSEC), ‘Oversight Board Annual Report 2019’, mars 2019.

18) Joint Declaration by the EU and China on Strategic Cooperation in the Area of Fifth Generation of Mobile Communication Networks, 28 septembre 2015.

19) Christopher Ketcham, ‘Is 5G Going to Kill Us All?’ *The New Republic*, 8 mai 2020.

20) Joel M. Moskowitz, ‘We Have No Reason to Believe 5G is Safe’, *Scientific American Blog*, 17 octobre 2019.

21) NIS Cooperation Group, ‘EU coordinated risk assessment of the cybersecurity of 5G networks’, 9 octobre 2019.

22) - -, ‘Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures’, 01/2020, 2020.

23) - -, ‘Progress in Implementing the EU Toolbox on 5G Cybersecurity’, juillet 2020.

24) Parlement européen, ‘Briefing: vers une société européenne du gigabit – Objectifs en matière de connectivité et de 5G’, service de recherche, juin 2017.

25) - -, ‘Les menaces pour la sécurité liées à la présence technologique croissante de la Chine dans l’Union et les actions possibles à l’échelle de l’UE pour les réduire’, Résolution 2019/2575(RSP), 12 mars 2019.

26) - -, ‘5G Deployment, State of Play in Europe, USA and Asia’, policy department, avril 2019.

27) - -, ‘Effects of 5G wireless communication on human health’, service de recherche, mars 2020.

28) Union Internationale des Télécommunications (UIT), ‘Vision pour les IMT – Cadre et objectifs généraux du développement future des IMT à l’horizon 2020 et au-delà’, Recommandation-R M.2083-0, septembre 2015.

29) UK National Institute for Public Health and the Environment, ‘Comparison of international policies on electromagnetic fields’, 2018.

30) UK Department for Digital, Culture, Media & Sport, ‘UK Telecoms Supply Chain Review Report’, juillet 2019.

31) World Economic Forum, ‘White paper: the Impact of 5G: Creating New Value across Industries and Society’, juin 2020.