

Chapitre 12

Les technologies quantiques

Raphaël MAUREL

Jusqu'au début du XX^e siècle, la physique n'était que « classique », c'est-à-dire fondée sur une approche adaptée aux objets à taille humaine permettant d'expliquer les phénomènes directement observables. Les interactions atomiques ne pouvant être expliquées, entre autres par cette théorie, la physique quantique apparaît avec Max Planck ou encore Albert Einstein. Elle a permis de décrire de manière inédite des phénomènes relatifs aux particules, aux atomes et aux champs électromagnétiques, et entraîné dès les années 1940 des avancées technologiques aussi majeures que le transistor ou la maîtrise de l'énergie nucléaire. Si la dualité onde-particule, c'est-à-dire le principe de la possibilité d'états physiques multiples pour une unique particule, est aujourd'hui connue, l'intrication quantique n'a encore pas livré tous ses secrets et la deuxième révolution quantique n'est pas achevée.

Maître de conférences en droit public à l'université de Bourgogne, Raphaël Maurel est spécialiste de droit international et secrétaire général de l'Observatoire de l'éthique publique, dont il dirige le département « Éthique des affaires ». Il se spécialise en droit du numérique dans le cadre du projet « Aladin-Analyse de la formation d'un droit international du numérique » qu'il porte au sein du Credimi de Dijon.

Matthieu CARON : La « physique quantique » est une expression qui fait peur. Quel rapport faire avec la transition numérique ?

Raphaël MAUREL : Il est vrai qu'avant 2022, en France, on entendait peu parler de physique quantique. Deux choses ont peut-être changé. D'une part, la publication de la stratégie quantique française au Parlement en mars 2022, à propos de laquelle des députés issus du monde scientifique, comme Cédric Villani, se sont particulièrement impliqués. D'autre part, la réception du prix Nobel de physique 2022 par Alain Aspect, célèbre physicien optique français connu pour avoir notamment résolu l'historique débat entre Niels Bohr et Albert Einstein, ou encore démontré, par l'expérience, la dualité onde-particule sur un photon unique.

C'est en tout cas un paradoxe : l'expression effraie alors que les deux tiers de « la » science actuelle nécessitent le recours à la physique quantique pour comprendre ce qui nous entoure. L'enjeu est surtout économique : plus de la moitié des richesses produites chaque année dans le monde est liée à des technologies quantiques. Nos ordinateurs, nos smartphones, les câbles isolants, les systèmes GPS, les

nanotechnologies... tout cela utilise les principes de la physique quantique. On comprend alors que la transition numérique est par essence quantique ! Cela se ressent particulièrement dans certains secteurs ou domaines de compétition mondiale, comme la miniaturisation des composants. De nouvelles technologies sont aussi en cours de développement et vont bouleverser nos modes de fonctionnement.

MC : Faut-il s'attendre à une « révolution quantique » ? Que font les États pour s'y préparer ?

RM : La première révolution quantique est déjà derrière nous. C'est celle du transistor, du circuit intégré, et donc du smartphone, de l'ordinateur. La deuxième révolution quantique est celle qui est en cours, mais elle est douce, à l'échelle de la physique. Elle a débuté en théorie dans les années 1930 et en pratique dans les années 1960. Peut-être devrait-on parler de « transition quantique », mais ce serait nier les effets que vont provoquer certaines technologies lorsqu'elles seront au point.

Le point de départ de la révolution en cours est l'intrication quantique, c'est-à-dire le fait – quantique ! – que deux particules « intriquées » se comportent de manière similaire, voire identique... alors même qu'elles sont éloignées de plusieurs mètres, kilomètres ou milliers de kilomètres. Imaginez que je remplisse mon verre d'eau et que, comme par magie, le vôtre se remplisse en même temps alors que je ne le touche pas. Dans la réalité physique, cela ne fonctionne pas comme cela, bien sûr, et il faut comprendre que l'on parle de particules uniques, infiniment petites, comme des électrons qui ont un « lien » spécial – un peu comme des jumeaux. On maîtrise encore mal l'intrication quantique, mais on mesure les capacités qu'elle peut offrir : modifier l'état d'une particule B en influant uniquement sur la particule A ouvre des perspectives vertigineuses. La plupart des recherches actuelles s'orientent vers la cryptographie quantique et l'ordinateur quantique.

La cryptographie quantique, c'est-à-dire le chiffrement des données pour les transmettre d'un point A à un point B, est un enjeu diplomatique majeur. Un État doit pouvoir communiquer avec ses ambassadeurs, ses émissaires, voire ses troupes à l'étranger sans pouvoir être écouté ; et à l'inverse, les États font quotidiennement du « renseignement » pour tenter d'intercepter les messages des autres – ennemis comme alliés. L'utilisation de l'intrication quantique pourrait virtuellement permettre de distribuer simultanément une même clé de chiffrement (secrète) d'un code entre A et B, quelle que soit leur distance. Il deviendrait dès lors impossible d'intercepter la clé de chiffrement.

L'ordinateur quantique, qui ne verra sans doute pas le jour avant plusieurs décennies, repose sur la superposition quantique et la capacité de calcul démultipliée que permet la physique quantique. Les processeurs quantiques ne fonctionneront demain plus

uniquement avec des « bits », unité simple à base de 0 ou de 1, mais avec des « qubits ». Il existe plusieurs projets différents ; par exemple, l'ordinateur quantique optique projeté par la start-up française Quandela fonctionnerait avec un générateur de « qubits » sous forme de photons, qui arriveraient à la vitesse de la lumière dans une puce comprenant des circuits amenant les photons à interagir avant que des détecteurs ne procèdent à des mesures. Cela permettrait de résoudre simultanément un nombre de calculs difficilement quantifiable.

Les États sont bien sûr lancés dans la course à l'ordinateur quantique ; ils se préparent également à résister à des attaques lancées par des ordinateurs quantiques. Par exemple, la cryptographie postquantique a pour objectif de concevoir des chiffrements résistants à des attaques quantiques. Les États accompagnent ces recherches ; la France est par exemple le 6^e investisseur mondial dans le domaine des technologies quantiques. Ils tentent aussi, voire surtout, de se prémunir de celles développées par les autres : c'est une course.

MC : Quelles propositions faire pour penser, au niveau de l'État, cette deuxième révolution ?

RM : Il ne faut pas perdre de vue que les technologies quantiques reposent sur les connaissances de l'humanité. On pourrait multiplier les exemples d'application positive de l'ordinateur quantique et des futurs capteurs quantiques : avancées majeures en médecine, meilleure gestion de l'énergie, rationalisation de l'agriculture – avec des capteurs permettant de mesurer des variations infimes du champ gravitationnel –, etc. Les États qui le peuvent sont proactifs par les investissements dans le quantique et la compétition est intense : il s'agit de ne pas manquer le virage. Mais on peut relever, en France, que ce sont pour beaucoup des entreprises privées qui bénéficient de financements suffisants. La perte massive d'attractivité de l'Université et le manque de financements publics – malgré une stratégie quantique ambitieuse – font que les plus grands chercheurs sont également engagés dans les start-up quantiques pour espérer faire avancer concrètement leurs recherches. Nombre d'entre eux le dénoncent. Il y a là un enjeu démocratique important, je crois : les technologies quantiques devraient pouvoir être pensées au sein de l'Université et relever de l'intérêt général plutôt que d'être privatisées avant même leur émergence. Il faut aussi être en capacité de former les « cerveaux » de demain, détenteurs de ces savoirs indispensables à l'humanité ! Pour cela, une seule solution : il faut financer la recherche publique et augmenter les budgets récurrents des laboratoires, qu'ils fassent de la recherche « appliquée » (je ne suis pas sûr que cela signifie quelque chose : il n'y a pas de recherche « inappliquée ») ou « fondamentale »...

MC : Peut-on penser les technologies quantiques et la sobriété numérique ensemble ?

RM : C'est indispensable, car c'est un impératif social. Je fais partie des « objectivistes sociologique », c'est-à-dire des juristes qui pensent, dans la lignée de George Scelle, Léon Duguit et Émile Durkheim, que le droit n'est que le produit des contraintes sociales exprimées par un groupe social donné. Le groupe social « monde occidental » demande davantage d'attention portée aux enjeux du réchauffement climatique et on en voit les premiers effets : les lois, règlements et décisions publiques comme privées se multiplient pour essayer d'éteindre ou en tout cas d'atténuer l'incendie. Toute nouvelle technologie, pour être développée, doit être financée, et, culturellement comme juridiquement, il ne sera sans doute plus imaginable, d'ici quelques années, de financer des technologies sans penser à leur impact environnemental. À vrai dire, les scientifiques n'ont pas vraiment besoin de la pression de la loi pour penser aux enjeux environnementaux de ce qu'ils font : ils sont les mieux placés pour mesurer leur importance. Mais je pense que tant la communauté scientifique que les législateurs ne pourront que faire de plus en plus ce lien.