Revue générale du droit, 2024.

Technologies quantiques et transformations du droit - Premières pistes de réflexion

Raphaël Maurel[1]

Citer cette publication : Raphaël Maurel, « Technologies quantiques et transformations du droit - Premières pistes de réflexion », Revue générale du droit, 2024.

[1] Maître de conférences en droit public à l'Université de Bourgogne, membre du CREDIMI (EA 7532) et membre associé au CEDIN (EA 382), directeur du programme « ALADIN – Analyse de l'élaboration d'un droit international du numérique » au sein du CREDIMI.

Le 16 août 2016, la Chine sème la stupeur mondiale : elle annonce avoir lancé, depuis le désert de Gobi, le tout premier satellite quantique[2]. Merveille technologique, ce nouvel engin est capable d'envoyer sur Terre des photons « intriqués », c'est-à-dire partageant, selon l'un des principes de la physique quantique (l'intrication), une propriété commune leur permettant d'interagir à distance – dans ce cas, à plus de 1000km. C'est le coup d'envoi des communications quantiques, annoncées comme étant impossibles à espionner car, en physique quantique, la mesure de l'un des photons (ou plus concrètement l'interception de la communication) corromprait l'ensemble et le destinataire en serait informé. Autrement dit, il est possible de commander l'autodestruction des données contenues dans des photons utilisées à des fins de communication, dès lors qu'elles sont interceptées. Trois ans plus tard, Google annonce, par une publication de ses chercheurs dans *Nature*, avoir atteint la « *suprématie quantique* », expression désignant la prouesse consistant à réaliser en 200 secondes, à l'aide d'un ordinateur quantique, ce qu'un ordinateur classique ne pourrait jamais réaliser – ou bien dans des délais se rapprochant de l'éternité[3]. Bien que la société IBM indique qu'elle est capable, grâce à ses supercalculateurs classiques, de la même prouesse en seulement quelques jours, il reste qu'il s'agit d'une révolution[4]. En utilisant la « *superposition* », autre principe de la physique quantique, il est en effet possible, théoriquement, de créer des « *Qubit* » dont le fonctionnement défie les lois...de la physique. L'informatique classique repose sur la transformation de toute donnée en bit, correspondant soit à 1, soit à 0 : leurs combinaisons, par des suites toujours plus longues, sont aujourd'hui transmises par signal lumineux – cas de la fibre optique - jusqu'au destinataire, capable de traduire le signal et de reconstituer les données. L'ordinateur quantique, qui se fonde sur la dualité onde-particule, fonctionne avec des Qubit présentant la particularité de pouvoir être à la fois des 1 et des 0. Autant dire que la puissance de l'ordinateur quantique

[2] « La Chine lance un satellite 'quantique', une première mondiale », Ouest-France.fr, 16 août 2016.
[3] Franck ARUTE and al., « Quantum supremacy using a programmable superconducting processor », Nature, n°574 (2019), pp. 505-510.
[4] Marine BENOIT, « Course à l'ordinateur quantique : Google confirme enfin avoir atteint la "suprématie", IBM réfute », Sciences et avenir, 23 octobre 2019.

est difficilement mesurable, mais nous n'en sommes pas là : malgré de nombreuses techniques en développement, les conditions infrastructurelles comme physiques sont complexes à réunir, et l'obstacle de la décohérence, c'est-à-dire du passage rapide et brutal d'un état quantique à un état classique, reste majeur[5]. Autrement dit, il n'existe pas encore de véritable ordinateur quantique stable, et il ne saurait *a priori* y avoir, à l'avenir, d'ordinateur purement quantique : leur mise au point, source d'une véritable course technologique notamment entre les États-Unis et l'Union européenne, ne fera pas disparaître les ordinateurs classiques.

En avril 2019, la France prend officiellement la mesure de ce qui s'annonce : la députée Paula Forteza est missionnée par Matignon pour réfléchir à l'émergence des technologies quantiques et anticiper, d'un point de vue politique, leur développement[6]. Son rapport « *Quantique : le virage technologique que la France ne ratera pas* », publié en novembre 2019, fait date et formule 37 recommandations[7]. Parmi elles, la création d'une cinquantaine de startups du quantique en France d'ici 2024, et, dans l'ensemble, développer des investissements massifs à tous les niveaux vers le quantique. Début 2021, le Président de la République présente la stratégie nationale sur les technologies quantiques de la France, qui entend, par un plan de près de 2 milliards d'euros sur cinq and, mettre des moyens importants au service des chercheurs et industriels en vue du développement de l'informatique quantique mais également d'autres technologies quantiques : communications, capteurs ou encore cryptographie[8]. Début 2022, la ministre des Armées Florence Parly, la

[5] Pour une explication accessible mais précise de ces questions, voir la conférence grand public de Pascale SENELLART-MARDON, directrice de recherche au CNRS, sur « Les débuts de l'ordinateur quantique », organisée par la section Paris-Sud de la Société Française de Physique le 14 janvier 2020 : https://www.youtube.com/watch?v=bVO5wdnicD4.

[6] Décret du 5 avril 2019 chargeant une députée d'une mission temporaire.

[7] Paula FORTEZA, Jean-Paul HERTEMAN, Iordanis KERENIDIS, « Quantique : le virage technologique que la France ne ratera pas », Rapport de la mission parlementaire du 15 avril 2019 au 3 octobre 2019, novembre 2019, 68 p.

[8] « Présentation de la stratégie nationale sur les technologies quantiques », 21 janvier 2021, disponible sur le site internet de l'Élysée : https://www.elysee.fr/emmanuel-macron/2021/01/21/presentation-de-la-strategie-nationale-sur-les-technologies-quantiques.

ministre de l'Enseignement Supérieur, de la Recherche et de l'Innovation Frédérique Vidal et le Secrétaire d'État chargé de la Transition numérique et des communications électroniques Cédric O annoncent, dans le cadre de « *France 2030* », le lancement d'une plateforme nationale de calcul quantique la France[9]. En octobre 2022, l'opinion publique découvre Alain Aspect[10] : le physicien français auteur d'une thèse qui permit de résoudre, dans les années 1980, un débat cinquantenaire entre Niels Bohr et Albert Einstein, est récompensé pour l'ensemble de ses travaux sur l'intrication quantique.

Enfin, en 2023, les technologies quantiques font leur apparition dans la loi de programmation militaire 2024-2030, figurant parmi les axes prioritaires du développement militaire de la décennie[11].

Nous entrons ainsi, de manière douce et continue, dans la deuxième ère quantique. La première révolution quantique est, en effet, déjà derrière nous : le transistor, inventé en 1947, puis le circuit intégré en 1959, reposent sur la mécanique quantique et permettent les sauts technologiques à l'origine des ordinateurs puis smartphones. La deuxième révolution quantique, qui est en cours depuis lors, est celle qui vise à maîtriser notamment les conséquences de l'intrication quantique et de la superposition quantique. À ce stade, peu de travaux existent, en sciences humaines, quant aux conséquences de ces technologies en développement[12]. Cela semble parfois prématuré : les ordinateurs quantiques pourraient ne fonctionner de manière stabilisée que dans trois

[9] Secrétariat général pour l'investissement, « Stratégie quantique : lancement d'une plateforme nationale de calcul quantique », 4 janvier 2022.
[10] « Alain Aspect, prix Nobel de physique 2022 », *Le journal CNRS*, 4 octobre 2022.
[11] Loi n°2023-703 du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense.
[12] Parmi les rares travaux disponibles en sciences juridiques, v. par exemple Mauritz KOP, « Establishing a Legal-Ethical Framework for Quantum Technology », *Yale Journal of Law & Technology (YJoLT)*, The Record, 2021, en ligne : https://yjolt.org/blog/establishing-legal-ethical-framework-quantum-technology ; Valentin JEUTNER, « The Quantum Imperative: Addressing the Legal Dimension of Quantum Computers », *Morals & Machines*, n°2021(1), pp. 52-59.

à cinq décennies. Cependant, la Chine a déjà créé la surprise en 2016 et rien n'exclut des bonds technologiques imprévisibles dans les années à venir, d'autant que les financements américains, chinois et européens sont massifs dans ce secteur. Les États doivent donc se préparer à ces évolutions technologiques et à leur impact dans la société.

La France, qui dispose de quelques pépites comme Pasqal, *start-up* capable de rivaliser avec les géants américains dans la course aux prototypes industriels quantiques[13], a manifestement saisi l'enjeu en programmant des investissements importants dans les prochaines années. Il n'en demeure pas moins que les technologies quantiques restent un mystère pour l'opinion publique, la classe politique et la communauté universitaire en sciences humaines. Leur probable émergence prochaine – on parle d'un « Internet quantique » opérationnel en 2035[14] – appelle pourtant une mobilisation des juristes, ne serait-ce que pour anticiper l'éventuelle obsolescence de cadres existants, l'impact des technologiques quantiques sur la garantie des droits fondamentaux et les besoins de nouvelles normes.

Ces brèves réflexions, dont le caractère général est assumé, visent à proposer quelques pistes préliminaires de recherche, sans prétendre à une quelconque forme d'exhaustivité. S'agissant d'un sujet aussi vaste et complexe que l'incidence des technologies quantiques sur les transformations – prévisibles ou supposées – du droit, il est pertinent d'interroger la manière dont la réflexion juridique peut appréhender ces évolutions technologiques et de chercher à comprendre en quoi elles impliquent et impliqueront (ou non) la mobilisation de nouvelles règles de droit. À cet égard, le fait que de nouvelles technologies bousculent les cadres juridiques et invitent à les repenser n'est pas nouveau : l'apparition, puis la démocratisation d'Internet en sont des illustrations déjà

[13] Voir le site internet de la société : https://www.pasqal.com/.

[14] « La stratégie quantique française », Rapport n°377 (2021-2022) de MM. Gérard LONGUET, sénateur et Cédric VILLANI, député, fait au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologiques, déposé le 20 janvier 2022.

anciennes[15]. Face aux technologies quantiques, dont l'intégration dans la réflexion juridique française est balbutiante, trois méthodes d'analyse – au moins – sont ainsi possibles. La première consiste à observer la manière dont elles commencent à être prises en compte en droit positif (**I**). La deuxième consiste à interroger l'approche juridique que la doctrine, mais également l'État et l'Union européenne, peuvent adopter (**II**). La troisième consiste à questionner la résilience du droit existant et le besoin de nouveaux outils (**III**).

I. Une intégration binaire dans l'ordre juridique national

Les technologies quantiques ont véritablement fait leur apparition en 2023 dans la loi française, en matière militaire (**A**). Pourtant, l'Union européenne s'intéresse depuis 2016 au moins à ce thème, de sorte que la France aurait certainement pu légiférer plus en amont voire être un moteur des initiatives européennes, ce qu'elle n'a pas été. Surtout, l'Union est porteuse d'une démarche davantage axée sur la création d'infrastructures de communications quantiques à usage non militaire (**B**).

A. Le quantique, un axe prévisible de la loi de programmation militaire française

Si l'on excepte un décret relatif à l'ionisation des denrées destinées à l'alimentation en 2001 évoquant une « énergie quantique maximale produite par des appareils à rayonnements ionisant[16] et les avis de la Commission d'enrichissement de la langue française qui intègrent, depuis quelques années, des termes relevant de la physique quantique au vocabulaire officiel de la Nation[17], il n'existe aucune mention des

[15] Voir, par exemple, le colloque consacré en 2013 au sujet des interactions entre Internet et le droit international : SFDI (collectif), *Internet et le droit international. Colloque de Rouen*, Paris, Pedone, 2014, 496 p.

[16] Décret n°2001-1097 du 16 novembre 2001 relatif au traitement par ionisation des denrées destinées à l'alimentation humaine ou animale, article 3.

[17] Voir les avis suivants de la Commission d'enrichissement de la langue française, adoptés depuis 2015 : Vocabulaire des termes généraux de la chimie (liste de termes, expressions et définitions adoptés), *JORF* du 19 septembre 2015 ; Vocabulaire de la chimie et des matériaux (liste de termes, expressions et définitions adoptés), *JORF* du 1er juillet 2017 ; Vocabulaire de

technologies quantiques, dans la loi comme le domaine règlementaire[18], avant les années 2020. Au-delà des rapports de l'Office parlementaire d'évaluation des choix scientifiques et technologiques (OPECST)[19], L'enjeu quantique apparaît indirectement dans la loi de programmation de la recherche (LPPR)[20] puis, plus clairement, dans la loi du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030[21].

L'ampleur des développements militaires comme industriels des technologies quantiques est difficilement imaginable à ce jour. Il ressort cependant des travaux menés par l'OPECST[22] et les connaissances disponibles que les communications, notamment diplomatiques et

la chimie et de la mécanique quantique (liste de termes, expressions et définitions adoptés), *JORF* du 31 mars 2022 ; Vocabulaire de l'informatique quantique (liste de termes, expressions et définitions adoptés), *JORF* du 20 décembre 2022.

18 Seule une question parlementaire posée, en 2006, à la suite de la publication de résultats de recherches menées aux États-Unis, soulève la question des avancées de la recherche quantique en France. Voir la question n°104780 de Mme Nathalie Kosciusko-Morizet, *JORF* du 26 octobre 2006, p. 9988, demandant à connaître l'état des recherches en France sur la théorie de la séparation du spin (caractéristique permettant de classer mathématiquement la façon dont se transforment les objets sous l'effet des rotations de l'espace à trois dimensions ; et la réponse publiée au *JORF* du 6 février 2007, p. 1345.

19 Office parlementaire d'évaluation des choix scientifiques et technologiques. Il semble que le premier rapport exposant clairement – bien que prudemment – les enjeux des technologies quantiques, essentiellement sous l'angle des progrès en informatique, date de 2008 ; v. le Rapport sur l'évolution du secteur de la micro/nanoélectronique n° 997 déposé le 25 juin 2008 par M. Claude Saunier.

20 Voir l'extrait pertinent du rapport annexé à la loi n° 2020-1674 du 24 décembre 2020 de programmation de la recherche pour les années 2021 à 2030 et portant diverses dispositions relatives à la recherche et à l'enseignement supérieur : « La puissance de calcul des ordinateurs classiques, qui a crû de manière exponentielle depuis les années 1960, plafonne aujourd'hui. La "seconde révolution quantique" peut conduire dans les années à venir à des ordinateurs d'un type nouveau, à la puissance inégalée. […] Si elle advient, cette technologie quantique sera une rupture au moins aussi importante que ne l'a été l'ordinateur classique, permettant la résolution de problèmes d'optimisation complexes avec des applications à la recherche de nouveaux matériaux, de nouveaux médicaments, etc. Comme cette nouvelle puissance de calcul permettra de casser les codes cryptographiques qui sécurisent aujourd'hui toutes nos communications sensibles, il est nécessaire de travailler dès maintenant à la cryptographie du futur qui résistera à l'ordinateur quantique, et plus largement au développement de nouveaux algorithmes quantiques »

21 Loi précitée. Il est notable que la précédente loi de programmation militaire, la loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense, n'évoque l'informatique quantique qu'à titre très incident.

22 « La stratégie quantique française », rapport précité.

stratégiques, seront vraisemblablement révolutionnées et atteindront dans les années à venir un niveau de sécurité jamais atteint. À l'heure où les conflits contemporains démontrent la nécessité opérationnelle de communications de pointe – on pense ici à l'armée russe communiquant, sur le sol ukrainien, via des ondes radio publiques[23] –, la course vers la communication quantique est donc un enjeu stratégique crucial. Au-delà même des communications exploitant l'intrication quantique, l'émergence des ordinateurs quantiques fragilisera, voire réduira à néant les effets de la cryptographie classique, qui protège les communications et données militaires. La puissance de calcul d'un ordinateur quantique remet en effet en cause l'efficacité de la cryptographie dite classique.

La cryptographie « asymétrique », qui a été développée pour contourner les limites de la cryptographie « symétrique » (système dans lequel l'expéditeur et le destinataire d'un message doivent partager en avance une clé de déchiffrement, le danger d'interception se situant au moment du partage de la clé commune), repose encore, schématiquement, sur la difficulté de casser un code. Ce système prévoit, pour chiffrer tout message, l'existence d'une paire de clés : une clé publique pour le chiffrement et une clé privée pour le déchiffrement. La clé publique est diffusée librement, tandis que la clé privée reste secrète, aux mains du destinataire. Ce système, plus lent – d'où l'intérêt des communications quantiques – résout le problème de partage de clé. Or, le RSA (pour Rivest, Shamir, Adleman[24]) qui est l'un des algorithmes de cryptographie asymétrique les plus utilisés, s'appuie sur la difficulté de factoriser un grand nombre composé en ses facteurs premiers. Autrement dit, tant que cette tâche demeure complexe et chronophage, le message reste sécurisé ; tel ne sera plus le cas face à des ordinateurs quantiques. Comme le relève Henri Gilbert (ANSSI), « *[i]l est difficile de prédire si de tels ordinateurs existeront un jour et, dans l'affirmative, s'ils apparaîtront avant ou auprès 2035, mais la prudence*

[23] La presse s'en est fait le relais : « Guerre en Ukraine : ce que dévoilent les communications des soldats russes sur des fréquences radio non sécurisées », *Le Monde.fr*, 25 mars 2022.
[24] Ronald RIVEST, Adi SHAMIR et Leonard ADLEMAN, « *A method for obtaining digital signatures and public-key cryptosystems* », *Communications of the ACM*, vol. 21, n° 2, 1978, p. 120–126.

commande de commencer à se prémunir dès maintenant contre les attaques de tels ordinateurs, afin notamment de prévenir les attaques rétroactives du type 'enregistrer maintenant sur des systèmes actuels, cryptanalyser n années plus tard'. Pour des données hautement sensibles à protéger durablement, nous sommes dès aujourd'hui exposés à cette menace. L'ANSSI recommande, comme la plupart des agences mondiales de sécurité, de commencer à prévenir cette menace quantique dès que possible »[25].

Il convient donc de développer de nouvelles méthodes afin de sécuriser les communications futures. Deux sont principalement explorées à l'heure actuelle. La cryptographie quantique, d'abord, vise principalement la création et la distribution sécurisées de clés cryptographiques. Les particules quantiques – *a priori* des photons – seront utilisées pour générer une clé secrète partagée entre deux parties, de sorte que toute tentative d'interception se heurtera au principe d'incertitude de la mécanique quantique (principe d'incertitude de Heisenberg) qui garantit que cette tentative sera détectée. Contrairement à la communication quantique qui vise à sécuriser le message lui-même, l'objectif principal de la cryptographie quantique est de garantir la sécurité de la clé, qui peut ensuite être utilisée dans un algorithme de chiffrement classique pour sécuriser la transmission de plusieurs messages. La cryptographie post-quantique, ensuite, a pour objectif de concevoir des chiffrements résistant à des attaques quantiques. Contrairement à la cryptographie quantique, elle n'utilise pas de phénomènes quantiques dans son fonctionnement, mais repose sur des algorithmes mathématiques qui restent difficiles, voire impossibles à résoudre même avec un ordinateur quantique. Il s'agit donc de miser sur les limites des technologiques quantiques, avant même leur émergence concrète – ce qui permet d'ailleurs une expérimentation anticipée[26].

[25] « La stratégie quantique française », rapport précité

[26] V. par exemple les essais réalisés en France : « Informatique quantique - La Banque de France expérimente la cryptographie post-quantique », *Revue de Droit bancaire et financier*, n° 6, Novembre-Décembre 2022, alerte 159.

Ces recherches nécessitent des investissements massifs, en vue d'usages militaires incontournables – à défaut d'être parfaitement évidents à ce stade. C'est la raison pour laquelle la loi sur la programmation militaire 2024-2030 intègre pleinement le sujet. Le rapport annexé à la loi précise ainsi que « *[p]our maintenir la supériorité opérationnelle de nos armées, une transformation doit être entreprise pour anticiper les sauts technologiques et les usages associés, notamment dans le domaine de l'espace, des fonds marins, de la cybersécurité, des drones, des différents domaines de la recherche fondamentale et appliquée issue de la physique quantique ou de l'intelligence artificielle* », et que « *la recherche quantique dans ses divers aspects et le domaine des calculateurs à haute performance doivent faire l'objet d'un investissement et d'une vigilance particulière de l'État afin de développer et de protéger des filières souveraines* »[27]. Les technologies quantiques occupent deux des dix « *axes prioritaire* » d'innovation miliaire : les capteurs à l'ère des technologies quantiques d'une part, le calcul quantique au service de capacités souveraines comme le renseignement ou la dissuasion d'autre part. Enfin, un rapport gouvernemental sur les utilisations possibles de la technologie quantique dans les armées françaises sera remis au Parlement en 2025, de sorte que le sujet devrait animer, au-delà de la communauté scientifique, les débats stratégiques militaires durant plusieurs années.

L'irruption des technologies quantiques dans l'ordre juridique français se fait donc par l'entrée militaire, ce qui n'a rien de surprenant. Il s'agit d'une approche par l'usage – ici militaire – couplée à une approche par le risque en termes de sécurité. Elle est cependant, et dans l'ensemble, tardive et limitée.

B. Une approche européenne tournée vers des usages civils et commerciaux

Dès 2016, un « *Manifeste Quantique* » proposé par une équipe européenne composée du commissaire Aymard de Touzalin, du ministre néerlandais des affaires économiques et de quatre universitaires a été proposé en vue

[27] Loi précitée.

d'une stratégie commune de l'Union face à le seconde révolution quantique[28]. Sur cette base, l'Union européenne a lancé en 2018 le *Quantum Technologies Flagship*, une initiative de recherche dotée d'un budget d'un milliard d'euros, puis, dans le cadre de l'entreprise commune européenne pour le calcul à haute performance (EC EuroHPC), des travaux en vue de parvenir à la mise au moins d'ordinateurs quantiques ont été lancés. Le 13 juin 2019, une déclaration visant au développement d'une infrastructure de communication quantique couvrant l'ensemble de l'UE (EuroQCI) est signée par sept États membres[29]. La France n'a rejoint l'initiative que fin 2019. Celle-ci prévoit la couverture, par l'Union, de cinq domaines : la communication quantique, l'informatique quantique, la simulation quantique, la métrologie et la détection quantiques, ainsi que la science fondamentale des technologies quantiques. Cette déclaration, qui constitue le cadre des débats européens, ne prévoit pas qu'un usage militaire – elle ne l'envisage d'ailleurs pas, l'Union ne disposant pas de compétence en la matière. En effet, la déclaration prévoit que les États membres :

« *1. prévoient de travailler ensemble pour établir un cadre de coopération – EuroQCI – afin d'étudier, dans les 12 prochains mois, la possibilité de développer et de déployer dans l'Union, au cours des 10 prochaines années, une infrastructure de communication quantique (QCI) certifiée et sécurisée de bout en bout, composée de solutions spatiales et terrestres, permettant de transmettre et de stocker des informations et des données de manière ultra-sécurisée et capable de relier des moyens de communication publics essentiels dans l'ensemble de l'Union.*

[…]

3. conviennent que l'infrastructure de communication à sécurité quantique cible devrait se concentrer sur les besoins croissants du secteur public en matière de sécurité, tout en explorant les moyens et les conditions permettant d'ouvrir la disponibilité de cette infrastructure aux utilisateurs de l'industrie, tout en garantissant la meilleure utilisation

[28] V. la page « Quantum Manifesto for Quantum Technologies », en ligne : https://ec.europa.eu/futurium/en/content/quantum-manifesto-quantum-technologies.html.
[29] Commission, « The future is quantum: EU countries plan ultra-secure communication network », 13 juin 2019, en ligne : https://digital-strategy.ec.europa.eu/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network.

possible de l'infrastructure pour un usage public et pour la promotion d'une industrie européenne innovante et compétitive »[30].

Il est donc bien question d'une exploitation industrielle et civile des communications quantiques – *a minima* – d'ici 2030, que les États de l'Union devront anticiper au niveau national. Sur le plan européen, ces objectifs ambitieux sont déjà traduits par plusieurs textes renforçant et développant les infrastructures existantes, qu'il s'agisse de l'industrie spatiale européenne[31] ou de celle des semi-conducteurs[32]. L'émergence prochaine de certaines technologies quantiques est, plus largement, palpable à la lecture des textes européens adoptés depuis 2019. Il n'est à cet égard pas neutre que le cadre commun de l'Union concernant le filtrage des investissements étrangers de 2019 intègre, parmi les investissements directs étrangers susceptibles de porter atteinte à la sécurité ou à l'ordre public des États, « *les technologies critiques [...], y compris les technologies concernant l'intelligence artificielle, la robotique, les semi-conducteurs, la cybersécurité, l'aérospatiale, la défense, le stockage de l'énergie, les technologies quantiques et nucléaires, ainsi que les nanotechnologies et les biotechnologies* »[33].

Autrement dit, l'Union européenne dispose d'une avance certaine en matière d'anticipation des transformations sociales liées aux technologies quantiques. À vrai dire, l'emprise de l'Union sur le développement quantique européen est particulièrement significative, en témoigne l'article 6 du Règlement 2023/588 qui prévoit notamment que « *[l]'Union est propriétaire de tous les biens corporels et incorporels qui font partie de l'infrastructure gouvernementale élaborée dans le cadre du programme, [...] à l'exception de*

[30] Digital Assembly, *Declaration of cooperation for exploring how to make available across the EU an integrated Quantum-secure Communication Infrastructure*, Bucharest, 13-14 June 2019 (traduction personnelle).
[31] Règlement (UE) 2023/588 du Parlement européen et du Conseil du 15 mars 2023 établissant le programme de l'Union pour une connectivité sécurisée pour la période 2023-2027.
[32] Règlement (UE) 2023/1781 du Parlement européen et du Conseil du 13 septembre 2023 établissant un cadre de mesures pour renforcer l'écosystème européen des semi-conducteurs et modifiant le règlement (UE) 2021/694 (« règlement sur les puces »).
[33] Règlement (UE) 2019/452 du Parlement européen et du Conseil du 19 mars 2019 établissant un cadre pour le filtrage des investissements directs étrangers dans l'Union, article 4.

l'infrastructure terrestre EuroQCI, qui est la propriété des États membres »[34]. L'objectif assumé de l'Union est de développer une politique européenne du quantique et, à ce stade, d'être un moteur économique et industriel dans la course technologique en cours.

Toutefois, l'approche nationale comme européenne reste infrastructurelle, et non matérielle. L'idée selon laquelle les technologies quantiques pourraient affecter l'exercice des droits fondamentaux n'est, ainsi, jamais mentionnée – à l'exception de l'article 17 de la Charte des droits fondamentaux de l'Union, posé comme limite au principe de la propriété par l'Union de tous le siens liés à l'infrastructure de communication à venir[35]. Or, c'est à notre sens sur cette base que les juristes doivent, aujourd'hui, penser le futur encadrement des technologies quantique. L'intégration des enjeux quantiques dans les lois de programmation militaire et de la recherche, en France, ne résout par ailleurs pas la question de savoir comment, concrètement, ceux-ci seront appréhendés du point de vue juridique – et il en est de même au niveau européen.

II. La nécessaire construction d'approches doctrinales des technologies quantiques

On le sait, le « droit du numérique » soulève de redoutables enjeux juridiques, jusque dans sa définition. Les approches théoriques demeurent encore éparses, le choix des termes volatile. Dans la galaxie doctrinale du droit du numérique, on parle de « droit des activités numériques » en général pour désigner l'encadrement des activités reposant sur des technologies numériques[36], de « droit de l'Internet » en particulier pour désigner les règles, parmi celles applicables aux activités numériques, destinées à l'encadrement d'Internet[37] – qu'il s'agisse de son

[34] *Ibid*., article 6.
[35] *Ibid*., paragraphe 22 du préambule.
[36] Luc GRYNBAUM, Caroline LE GOFFIC, Ludovic PAILLER, *Droit des activités numériques*, 2ème éd., Paris, Dalloz, 1144 p.
[37] Concernant uniquement le commerce et la vente électroniques : Jean-Michel BRUGUIERE, Pierre DEPREZ, Frédéric DUMONT, Vincent FAUCHOUX, *Le droit de l'Internet*, 3ème éd.,

infrastructure[38] ou des activités qui y sont menées, ou encore, de manière sectorielle, de « droit de la cybersécurité »[39], de « droit de la blockchain »[40] ou – impliquant un champ plus vaste que celui des seules activités numériques – de « droit des données personnelles »[41]. Sans entrer dans de complexes débats qui dépassent le champ de cette réflexion préliminaire, on peut admettre qu'il existe encore des discussions conceptuelles quant à la construction d'une discipline juridique[42] propre à l'encadrement des activités numériques, dont il est d'ailleurs permis de se demander si elle ne devrait pas inclure également le sujet de l'encadrement juridique de l'impact de ces technologies sur la société – l'expression appropriée étant alors peut-être, comme à l'étranger, « droit de la digitalisation ».

Toujours est-il que l'encadrement des technologies et activités quantiques rejoindra inévitablement ce vaste ensemble sémantique et qu'il conviendra d'adopter d'une part une expression appropriée – « droit du quantique », « droit des activités quantiques » ? – et surtout, d'autre part, une approche juridique adéquate. La diversité des titres disciplinaires ou sous-disciplinaires mentionnés plus haut traduit en effet une relative indétermination collective dans la démarche scientifique optimale pour saisir les phénomènes juridiques découlant de l'usage ou de l'existence de technologies numériques – indétermination collective et non individuelle, chaque auteur proposant une approche personnelle et justifiée de son objet d'étude. Il n'y a pas de raison que ce flou théorique, que favorise sans

Paris, LexisNexis, 2017, 432 p. Pour une approche plus large, v. Céline CASTETS-RENARD, *Droit de l'internet : droit français et européen*, 2ème éd., Paris, Montchrestien, 2012, 492 p.

38 Les approches infrastructurelles sont rares. À paraître en incluant cette approche, v. Raphaël MAUREL, *Droit de l'Internet*, Paris, Bréal, coll. Lexifac, 2024.

39 V., depuis 2023, le *Code de la cybersécurité* publié chez Dalloz sous la direction de Michel SÉJEAN.

40 Alice BARBET-MASSIN, Faustine FLEURET, Alexandre LOURIMI, William O'RORKE, Claire PION, *Droit des crypto-actifs et de la blockchain*, Paris, LexisNexis, 2020, 432 p.

41 V., récemment, Antoine RENUCCI, Jean-François RENUCCI, *Droit et protection des données à caractère personnel*, Paris, LGDJ, Manuels, 2022, 258 p. ; à paraître, Thibault DOUVILLE, *Droit des données à caractère personnel*, Paris, LGDJ, Précis Domat, 2023, 684 p.

42 Sur ce point, voir les travaux éclairants réunis par Frédéric AUDREN, Ségolène BARBOU DES PLACES (dir.), *Qu'est-ce qu'une discipline juridique ? Fondations et recompositions des disciplines dans les facultés de droit*, Paris, LGDJ, coll. Contextes, 2018, 390 p.

doute le caractère post-régulatoire du droit du numérique[43], s'estompe lorsqu'émergeront des normes visant à encadrer les technologies quantiques. Aussi peut-on tenter d'identifier quelques approches possibles de ces nouvelles règles ou ensembles normatifs, qui emprunteront nécessairement à d'autres sous-ensembles tout en s'inscrivant, d'un point de vue théorique, au sein du « droit du numérique ». Deux pistes paraissent, de prime abord, intéressantes parmi d'autres[44] : les approches infrastructurelle (**A**) et par les risques (**B**).

A. L'intérêt d'une approche infrastructurelle

Une première démarche possible, sur la base de la démarche européenne mais qui manque encore trop souvent – à notre sens – en matière de doctrine droit du numérique, consiste à développer une approche infrastructurelle. Les manuels contemporains de droit du numérique et la doctrine se sont en effet efforcés de construire et présenter de manière ordonnée une approche matérielle des règles applicables aux technologies numériques, en laissant parfois de côté la question de l'encadrement des infrastructures permettant l'accès à ces outils (câbles, satellites, centres de données…). Ces sujets, il est vrai techniques, relèvent parfois davantage de la normalisation technique que d'autre chose ; pour autant, les enjeux géopolitiques de ces infrastructures sont tels[45] que les juristes ne peuvent pas s'en désinstéresser – à plus forte raison lorsque des textes internationaux les protègent[46].

---

43 La technologie évolue toujours plus vite que le droit qui l'encadre.

44 D'autres travaux envisagent ou adoptent des approches sectorielles, par exemple sous l'angle de la propriété intellectuelle ; v. par exemple Mauritz KOP, « Regulating Transformative Technology in The Quantum Age: Intellectual Property, Standardization & Sustainable Innovation », *Transatlantic Antitrust and IPR Developments*, Issue 2/2020, 2020.

45 Voir pour un exemple d'ouvrage récent sur ce thème Ophélie COELHO, *Géopolitique du numérique. L'impérialisme à pas de géants,* Éditions de l'Atelier, 2023, 272 p.

46 Tel est notamment le cas des câbles sous-marins, dont la protection remonte quasiment à leur création avec la Convention de Paris de 1884 relative à la protection des câbles sous-marins ; voir également les articles 21 et 60 de la Convention des Nations Unies sur le droit de la mer du 10 décembre 1982 et, plus largement sur ce régime juridique, Camille MOREL, *Les câbles sous-marins*, CNRS Éditions, 2023, 192 p.

Or, les technologies quantiques ne sont pas indépendantes de matériaux, structures et infrastructures qui sont déjà, pour une partie d'entre elles, soumises à des législations et cadres internationaux existants. Ainsi, le droit de l'Internet renvoie immédiatement, selon cette approche, au régime international des câbles sous-marins[47] et dans une moindre mesure au droit des télécommunications par satellites. En matière de technologies quantiques, des satellites quantiques pourraient être préférés aux câbles à fibre optiques – en témoigne l'expérience chinoise de 2016 et les orientations du règlement européen sur la connectivité sécurisée pour la période 2023-2027[48]. L'infrastructure des réseaux quantiques demeure cependant à construire, selon des normes spécifiques : ces systèmes devraient s'avérer extrêmement sensibles aux interférences et devront être particulièrement protégés. Dans un autre registre, alors que les technologies numériques classiques utilisent majoritairement des matériaux semi-conducteurs – objets d'une « guerre commerciale » entre la Chine et les États-Unis[49] – les technologies quantiques devraient également reposer sur des supraconducteurs, dont le marché est aujourd'hui dominé par les États-Unis, le Japon et dans une moindre mesure l'Allemagne. Une approche infrastructurelle du droit du quantique pourrait dès lors débuter par une analyse des cadres physiques de l'utilisation des technologies quantiques et une étude du droit applicable aux probables guerres commerciales et technologiques que se livreront les États sur ces sujets, sous l'angle du droit international économique mais également des droits fondamentaux et environnementaux. Dans l'ensemble, les observateurs s'accordent certes pour considérer que la prochaine révolution quantique réduira significativement l'impact environnemental de nos technologies. Celles-ci requièrent pour l'instant « *un équipement hardware spécifique, construit en utilisant des minerais rares (cobalt,*

[47] V. la note précédente.
[48] Règlement (UE) 2023/588 précité.
[49] V. par exemple Zhou QI, « US Technological Decoupling from China: Strategic Motives and Policy Measures », *China International Studies*, vol. 98, 2023, pp. 101-126. Il est à noter que le décret présidentiel pris par Joe Biden en août 2023 limite fortement les investissements américains en Chine dans le domaine des technologiques quantiques (« États-Unis : adoption d'un décret présidentiel interdisant certains investissements américains dans des technologies sensibles en Chine », *Revue Internationale de la Compliance et de l'Éthique des Affaires*, n°5, 18 octobre 2023, actualité 214, p. 5).

lithium, néodyme, indium, …) provenant parfois de zones de conflits (on parle de 'minerais de sang') et dont le fonctionnement induit une consommation d'énergie considérable, même si elle se réduira avec les avancées de la technologie quantique »[50]. S'agissant des semi-conducteurs, l'extraction du silicium (essentiellement en Chine), du germanium ou du gallium soulève en effet des questions de protection de l'environnement et de statut des travailleurs. Sur ce point, l'une des missions du Conseil européen des semi-conducteurs créé par le Règlement sur les puces, qui prévoit une réduction de l'impact environnemental de ces industries, sera d'étudier et de préparer « *le recensement des secteurs et technologies spécifiques, susceptibles d'avoir une forte incidence sociale ou environnementale ou revêtant une importance en matière de sécurité, et qui doivent, par conséquent, faire l'objet d'une certification attestant que leurs produits sont verts, fiables et sûrs* »[51]. Les supraconducteurs, également nécessaires à certaines technologies quantiques, impliquent de leur côté l'utilisation de composés à base de niobium, de titane ou encore de fer. L'extraction actuelle et future de certains de ces minerais, comme le niobium en Afrique, soulève pourtant déjà des problématiques géopolitiques, éthiques et environnementales qu'il sera difficile d'ignorer[52], et pourrait aboutir à la création d'autorités nationales, régionales et mondiales de régulations du secteur minier.

Une approche par les infrastructures permettrait notamment d'intégrer pleinement ces questions, essentiellement d'ordre géopolitique et environnemental, aux débats sur l'encadrement des usages des technologies quantiques, alors qu'elles sont globalement peu présentes dans ceux relatifs au droit du numérique.

---

[50] William FEUGÈRE, « Compliance et métavers – une éthique réelle dans un monde virtuel », *Revue pratique de la prospective et de l'innovation*, n° 2, Novembre 2022, dossier 16, p. 30.
[51] Règlement (UE) 2023/1781 précité, article 28, 1. d).
[52] La presse africaine s'en fait l'écho ; par exemple Nicaise KIBEL'BEL OKA, « RDC. Niobium, minerai stratégique au cœur d'une géopolitique de l'insécurité au Nord-Kivu », *Echos d'Afrique*, 11 décembre 2022 ; « Malawi : la construction de la première mine de niobium d'Afrique commencera d'ici septembre 2024 », *Agence Cofin.com*, 14 juin 2023.

B. L'indispensable approche par les risques

Une seconde démarche possible est l'approche du droit par les risques. Dans un ouvrage récent, Arnaud Latil montre comment le droit du numérique a été construit en tant que droit des risques, et, bien que le droit des technologies quantiques ne figure pas encore parmi son spectre d'analyse, sa conclusion résonne avec les propos qui précèdent : « *Le droit des risques est un droit trajectif. Avec lui l'État régulateur montre aux justifiables les voies à suivre afin de prévenir les risques et d'en surmonter les conséquences négatives. […] Le droit des risques est aussi un droit pragmatique. Il marque en effet un tournant méthodologique pour la production et l'application du droit. L'appréciation critique des objectifs de prévention des risques et de résilience face aux dommages implique de mesurer l'effectivité des normes et de sortir d'une logique abstraite d'appréciation des règles de droit. Une recherche pragmatique s'impose. L'ensemble des phénomènes normatifs doivent pouvoir être mesurés afin de déterminer le degré de résistance aux risques. Le rapprochement du droit et des autres sciences est alors indispensable pour apprécier son effectivité* »[53].

En matière de technologies quantiques, tout reste à construire et on ne peut que traces les grandes lignes de ce qu'une telle approche pourrait impliquer. Une approche du quantique par les risques, débutant par une taxonomie des usages du quantique en vue d'une cartographie des risques induits par les technologies quantiques, intègrerait d'abord une logique infrastructurelle mais la dépasserait en posant la question des risques démocratiques et sociaux. Telle est d'ailleurs l'approche retenue par les premières réflexions anglophones sur l'encadrement des technologies quantiques. Mauritz Kop identifie ainsi une demi-douzaine de secteurs – mais pas de cas d'usages concrets – clés (ordinateur quantique, communication quantique, capteurs quantiques, simulation quantique, science fondamentale, intelligence artificielle) et envisage dix catégories de risques sociaux pressant : le risque d'augmentation des inégalités et de monopolisation des technologies par la propriété intellectuelle dans un premier temps, le risque pour la stabilité du système économique et

[53] Arnaud LATIL, *Le droit du numérique. Une approche par les risques*, Paris, Dalloz, 2023, p. 241.

financier, le risque pour la confidentialité et la sécurité des données, le risque d'une désinformation massive, le risque de piratage, le risque d'activités criminelles, le risque environnementale, les risques associés à l'autoritarisme et à la surveillance d'État, le risque de recomposition géopolitique et de course aux armes quantiques, et, avec un pessimisme alarmant, les risques liés à des scénarios d'extinction humaine[54]. Et l'auteur de conclure : « *A lack of policy, inaction and absence of international consensus will amplify these risks* ». Faisant appel à d'autres ensembles normatifs et d'autres sciences que le droit, comme la philosophie, l'éthique, les sciences de gestion ou encore les sciences du vivant, une telle approche des risques quantiques présenterait l'avantage d'encourager d'emblée des réflexions systémiques, dépassant les approches techniques et sectorielles (domaine militaire, cybersécurité, télécommunications, …) de ces outils.

Ces deux approches, infrastructurelle et par les risques, ne sont ni exclusives l'une de l'autre, ni les seules possibles. Elles pourraient cependant constituer une première base de réflexion pour penser le futur « droit du quantique ». Au-delà des approches doctrinales, il est cependant nécessaire d'analyser concrètement en quoi les technologies quantiques – ou certaines d'entre elles – soulèvent ou soulèveront des interrogations juridiques.

III. L'indispensable réflexion quant au droit applicable aux phénomènes quantiques

La question des cadres doctrinaux qu'il conviendra de développer ne permet pas de faire face aux urgences soulignées par les experts du sujet[55]. Or, face à de nouveaux phénomènes sociaux, le juriste identifie généralement deux lignes de conduite distinctes mais complémentaires. Il

[54] Mauritz KOP, « Establishing a Legal-Ethical Framework for Quantum Technology », *op. cit.*
[55] V. pour une tentative de synthèse Mauritz KOP, Mateo ABOY, Eline DE JONG, Urs GASSER, Timo MINSSEN, I. Glenn COHEN, Mark BRONGERSMA, Teresa QUINTEL, Luciano FLORIDI, Ray LAFLAMME, « Towards Responsible Quantum Technology », *Harvard Berkman Klein Center for Internet & Society Research Publication Series*, #2023-1, Harvard University 2023, 22 p.

s'agit souvent de chercher à étendre, par plusieurs techniques juridiques comme l'interprétation dynamique, le droit existant pour embrasser les nouvelles situations (**A**). Une autre approche consiste à identifier les lacunes du droit existant pour le compléter par de nouveaux instruments spécifiquement dédiés à l'encadrement du nouvel élément (**B**).

A. Penser la pertinence des cadres existants

L'une des premières questions qu'il convient de soulever est celle de la capacité de nos modèles juridiques actuels à intégrer les problématiques et risques induits par le développement du quantique. Or, la communauté internationale, confrontée à de nouvelles technologies, a produit de nombreuses règles – *soft* ou *hard* – pour les encadrer ces dernières années, et continue à le faire. Aussi paraît-il de prime abord pertinent de raisonner par analogie avec la régulation de l'intelligence artificielle (IA), en plein développement. Comme l'indique Mauritz Kop, *« A legal framework for quantum technology should build on existing rules and requirements for AI. We should connect AI to quantum »*[56], d'autant que les ordinateurs quantiques et d'autres outils quantiques seront en grande partie hybridés avec des systèmes d'IA. C'est d'ailleurs la raison pour laquelle les dix principes de base que l'auteur propose en vue de l'élaboration d'un quantique sûr et protecteur des principes démocratiques sont essentiellement inspirés des travaux en matière d'IA[57].

Il n'est cependant pas certain que les approches de la régulation de l'IA, qui s'avèrent dans l'ensemble régionalement fragmentées et tardives, puissent être aussi simplement dupliquées. Les enjeux juridiques soulevés par les technologies quantiques sont en effet aussi nombreux que la date de leur mise en fonctionnement incertaine. Il est néanmoins pertinent de chercher d'abord à appliquer les cadres juridiques existants. En ce sens,

[56] Mauritz KOP, « Establishing a Legal-Ethical Framework for Quantum Technology », *op. cit.*
[57] Comparer les dix principes, sous forme de déclaration d'intention qu'entreprises et États sont invités à adopter, avec la *Déclaration sur l'intelligence artificielle, la robotique et les systèmes « autonomes »* proposée par le Groupe Européen d'Éthique des Sciences et des Nouvelles Technologies (Commission européenne), Bruxelles, 9 mars 2018.

Valentin Jeutner, concentrant son analyse sur les ordinateurs quantiques, distingue de manière chronologiques deux enjeux juridiques majeurs. Le premier, aussi politique que juridique, est celui de la standardisation dans son développement – faisant ici un parallèle avec la standardisation, y compris linguistique, qui présida au développement des ordinateurs classiques[58]. Des normalisations techniques et standardisations, au niveau national (militaire) et international s'imposeront à l'évidence, comme pour toute nouvelle technologie. Il faudra en effet garantir l'interopérabilité des systèmes quantiques, sans quoi ils ne pourront communiquer entre eux. Or, le processus de normalisation technique est intrinsèquement politique : la Chine, les États-Unis et l'Union européenne se livreront certainement à des batailles diplomatiques souterraines pour parvenir à imposer leur conception auprès des normalisateurs mondiaux. Le *National Institute of Standards and Technology* (NIST), institut américain de normalisation, a d'ailleurs d'ores-et-déjà marqué le domaine de son emprise et entrepris de définir les futures normes mondiales en matière quantique[59]. Tout porte également à croire que l'ISO (Organisation internationale de standardisation) jouera un rôle majeur dans la normalisation des infrastructures quantiques, à l'instar de son positionnement incontournable en matière d'infrastructures informatiques classiques. Il n'est cependant pas inconcevable que, sur le modèle de l'*Internet Engineering Task Force* (IETF) créée pour développer des standards dédiés au fonctionnement d'Internet, de nouveaux consortiums de standardisation émergent pour traiter des questions spécifiquement liées à l'interopérabilité des technologies quantiques. Les États auront alors à se positionner pour déterminer le fonctionnement de tels organismes : seront-ils publics, privés ou mixtes ? Quel sera le modèle, démocratique ou non, retenu pour leur fonctionnement et la formation des standards ? Ces questions, relatives à la réglementation technique des outils quantiques, doivent être anticipées dès maintenant.

[58] Valentin JEUTNER, « The Quantum Imperative: Addressing the Legal Dimension of Quantum Computers », *op. cit.*, p. 55.
[59] « La stratégie quantique française », rapport précité.

Le second enjeu juridique posé par les ordinateurs quantiques, selon Valentin Jeutner, est le plus pressant : la capacité de ces ordinateurs à surmonter les protocoles de cryptage conventionnels. Bien que la cryptographie post-quantique s'emploie à limiter les difficultés, il demeure que les futurs algorithmes quantiques pourraient être utilisés pour déchiffrer des informations a posteriori. Autrement dit, il est possible de collecter aujourd'hui des données cryptées de manière classique et de les décrypter ultérieurement, lorsque des ordinateurs quantiques suffisamment puissants seront disponibles[60]. Là encore, les solutions sont aussi politiques que juridiques : « *[a]gainst this background, it is crucial to develop strategies to avoid that the development and operation of quantum computers leads to a situation where, on the one hand, there are actors who have unlimited access to previously protected data and can communicate in encrypted form and, on the other hand, actors who have no access to quantum technology and are more or less at the mercy of the former* »[61]. L'auteur préconise de garantir, par le droit, un accès égal aux technologies quantiques, lequel pourrait être traduit de manière anticipée – car il sera trop tard ensuite – par un « droit au quantique ». Juridiquement, « *examples of such regulatory measures could include limiting the material or temporal scope of patents or to make technology transfers obligatory in certain areas* »[62].

On le voit, et comme le concède l'auteur en conclusion, plusieurs des grands principes voire des normes nécessaires, selon lui, à l'anticipation du quantique existent déjà dans nos systèmes juridiques : principe d'égalité, de non-discrimination, de transparence, de bonne gouvernance en particulier[63]. Il est intéressant de noter que, d'emblée, le lien entre standardisation technique et droits fondamentaux, est assumé. Une telle approche nous paraît particulièrement pertinente, la « détechnicisation » des enjeux technologiques, seule à même de permettre aux citoyennes et citoyens de s'en saisir, étant un impératif démocratique. Par ailleurs, nous

60 Valentin JEUTNER, « The Quantum Imperative: Addressing the Legal Dimension of Quantum Computers », *op. cit.*, p. 55.
61 *Ibid.*, p. 56.
62 *Idem.*
63 *Ibid.*, p. 58.

avons souligné plus haut l'importance de penser les risques du quantique en termes de droits de la personne humaine, et de ne pas les cantonner à des questions purement militaires et économiques. Cependant, l'application spécifique de ces grands principes au domaine des technologies quantiques – ici, des seuls ordinateurs quantiques – pourrait nécessiter l'adoption de nouvelles règles, au niveau international, régional ou national.

B. Anticiper le besoin de nouveaux instruments

Comme l'indique très justement Brunessen Bertrand, « *[l]e droit n'est pas toujours en mesure d'anticiper toutes les évolutions technologiques – et toutes celles que laissent imaginer aujourd'hui les* 'deep tech' *l'illustrent bien : calcul à haute performance, technologies quantiques, blockchain représentent un véritable défi pour l'application des standards normatifs de protection des droits. C'est tout l'enjeu de la neutralité technologique du droit et des droits fondamentaux. Cela exige malgré tout une réflexion constante sur la régulation juridique de ces technologies [...]. Le risque, en la matière, est aussi celui de la consécration de principes théoriques trop abstraits pour être opérants. Des questions telles que la portabilité et l'interopérabilité montrent que des normes techniques sont nécessaires à l'effectivité du droit et des droits dans les activités numériques* »[64]. Ce sont ces normes dont il convient de prévoir, dans la mesure du possible, l'adoption, en tentant d'identifier autant que faire ce peu le niveau d'action pertinent.

Au niveau européen et étatique, se poseront principalement des questions de respect des droits fondamentaux, de lutte contre la cybercriminalité, ou encore de protection des données personnelles. L'amélioration des capacités de chiffrement aura nécessairement un impact sur les techniques de surveillance déployées par les États et donc sur le droit à la vie privée. Si les technologies quantiques venaient à être commercialisées et généralisées dans la société civile, comme l'ordinateur, l'accès à Internet puis le téléphone cellulaire l'ont été, de nombreuses questions devraient

[64] Brunessen BERTRAND, « Le modèle européen de partage de données », *Europe*, n° 2, Février 2021, étude 1, p. 2.

être résolues. L'Union européenne souhaitera-t-elle harmoniser les règlementations relatives à ces nouvelles technologiques, afin de garantir un marché unique fonctionnel ? Telle semble bien être la voie choisie par les règlements précités[65], bien que la problématique du respect des droits fondamentaux soit, si l'on excepte la volonté de créer un accès égal à ces technologies et le respect général du droit à la propriété, encore absente des textes européens. Une déclaration générale sur les droits et libertés garantis par les États membres de l'Union à l'ère quantique, traçant une feuille de route parallèle à celle élaborée en vue de la connectivité sécurisée dans l'Union, serait certainement une initiative pertinente.

En droit international, des questions spécifiques ne manqueront pas non plus d'émerger. L'expérience des transformations du droit international du fait d'Internet – ne serait-ce que concernant les débats sur la question de savoir si le droit de la guerre s'applique au cyberespace[66] – devrait servir de leçon et permettre d'anticiper certains sujets. Le régime international de la cybersécurité, qui reste d'une densité limitée, devra sans doute être refondé et approfondi. L'intrication quantique ouvre également la voie à de futures activités étrangères sur les sols des États, soulevant des problématiques de souveraineté territoriale, de lutte contre les ingérences étrangères et de cybercriminalité. La convention de Budapest[67] du Conseil de l'Europe sur la cybercriminalité – mais ouverte à l'adhésion au-delà de l'organisation – pourrait utilement être complétée par un troisième protocole relatif à la cybercriminalité dans l'ère quantique. Pourtant, la question des technologies quantiques n'est pas au programme de travail

[65] Voir en particulier le Règlement (UE) 2023/588 du Parlement européen et du Conseil du 15 mars 2023 établissant le programme de l'Union pour une connectivité sécurisée pour la période 2023-2027 (précité).
[66] La question ne fait plus guère débat : oui. Le Manuel de Tallinn, publié en 2013 par l'OTAN, expose clairement la manière dont le droit international s'applique aux menaces numériques en matière de conflits armés ; une version 2.0, en 2017, explore la question des incidents cyber n'atteignant pas les seuils de recours à la force ou de conflit armé tandis qu'une version 3.0 est attendue pour 2026. Ce texte reste non contraignant (ce n'est pas un traité international) et marqué, pour ses détracteurs, par un atlantisme certain. La France réaffirme régulièrement que le droit international s'applique au cyberespace.
[67] Convention de Budapest sur la cybercriminalité (STE n° 185), 23 novembre 2011.

2022-2023 du Comité de la Convention[68], ni d'ailleurs à l'ordre du jour des négociations du futur instrument international sur cybercriminalité. Le rapport du Secrétaire général des Nations unies de 2019, qui a servi de base à la création par l'Assemblée générale du Comité *ad hoc* chargé d'élaborer une convention internationale globale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles[69], n'évoque à aucun moment les risques quantiques. Censé achever ses travaux en 2024, le comité a produit un projet de convention qui ne tient, *a priori*, qu'imparfaitement compte de la révolution quantique à venir – on pense par exemple au projet d'article 22 paragraphe 1er relatif à l'établissement de la compétence territoriale des États[70]. Le sujet du quantique n'a, visiblement, pas été abordé durant les débats, malgré une proposition d'une ONG multipartite à destination du Comité *ad hoc* le requérant expressément[71].

Le régime international des télécommunications devra certainement être adapté pour intégrer la question des autorisations d'envois de données par satellites quantiques, et clarifier la manière dont les États pourront exercer des pouvoirs de contrôle. On pense par exemple à l'utilisation de communications quantiques à des fins illicites, et à la difficulté d'appliquer l'article 7 du Règlement des télécommunications en vertu duquel les États « *devraient s'efforcer de prendre les mesures nécessaires pour empêcher la propagation de communications électroniques non sollicitées envoyées en masse et en réduire autant que*

68 COE, T-CY Workplan for the period January 2022 – December 2023, adopted by the 25th T-CY Plenary (15 November 2021).
69 Résolution 74/247 adoptée par l'Assemblée générale le 27 décembre 2019, A/RES/247.
70 Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, Sixième session, New York, 21 août-1er septembre 2023, Projet de texte de la convention, 29 mai 2023, A/AC.291/22.
71 Proposition by the Center for Cyber Risk Research and Policy at the Cyber Institute to the Ad Hoc Committee, August 2022. Évoquant le fait que « *[e]merging Technologies such as Artificial Intelligence, Quantum Computing, and Blockchain have become increasingly exponential enabling innovations for potential criminal actors exploiting Information and Communication Technologies* », le Centre conclut ainsi son courrier : « *we implore this Ad Hoc Committee explore and deliberately include aspects of emerging technologies into our discussions* ».

possible l'incidence sur les services internationaux de télécommunication »[72]. Plus largement, de nouveaux standards de sécurité s'imposeront rapidement au sein de l'UIT. La sécurisation des nouveaux réseaux – 5G, internet des objets, 6G demain – et leur résilience aux futures attaques quantiques passe, en effet, également par la standardisation internationale au sein de l'UIT. Or, comme l'indiquait en 2019 un responsable d'entreprise privée spécialisé dans le quantique, « *[s]tandardization is relatively new to the quantum technology community, both in industry and academia. We did not fully anticipate the need for standards to support large-scale deployment of technologies [...]. Having now recognized this need, we have fast built an ecosystem of quantum specialists within ITU and we are learning ITU's procedures as we work together to draft a first set of ITU standards on quantum-safe security* »[73].

Surtout, l'émergence potentielle d'armes s'appuyant sur les technologies quantiques devrait dès maintenant faire l'objet de discussions mondiales. À défaut d'un traité interdisant le développement de certaines armes quantiques auquel il faudra certainement réfléchir à l'avenir, une déclaration mondiale sur l'utilisation pacifique des technologies quantiques, à l'heure où la course aux armements quantiques est limitée à la cybersécurité[74], serait en particulier un premier pas pertinent. Certes, l'utilité d'une énième déclaration mondiale peut être discutée, d'autant qu'elle peut paraître quelque peu anticipée. Pourtant, il faut garder en mémoire que le Traité sur l'espace de 1967, posant l'exigence d'une utilisation pacifique de l'espace extra-atmosphérique, a été adopté alors même que l'humain n'avait jamais mis les pieds sur la Lune. C'est sans doute un outil visionnaire de cet ordre, posant un cadre incroyablement futuriste et qui a certainement évité de nombreux conflits[75], dont la

[72] UIT, Règlement des télécommunications internationales (RTI), Actes finaux de la Conférence mondiale sur les télécommunications internationales (CMTI-12), Dubaï, 2012, article 7.1.
[73] « Quantum specialists are racing to join the ITU membership: ID Quantique explains why », *ITU News*, May 21, 2019, en ligne : https://news.itu.int/why-quantum-specialists-join-itu/.
[74] Neil THACKER, « Cybersécurité : la course aux armements quantiques a commencé », *Silicon.fr*, 31 janvier 2023.
[75] On se permet de renvoyer, sur ce point, à Raphaël MAUREL, « Les garanties du maintien de l'utilisation pacifique de l'espace extra-atmosphérique : l'exemple de l'inspection

communauté internationale a besoin pour éviter d'être encore une fois pris de court par des technologies dont il est encore possible, à l'heure actuelle, d'observer les avancées.

Les avancées technologiques fondées sur la physique quantique, bien que d'apparence complexes, méritent que l'on s'y intéresse dès aujourd'hui. Quelques propositions, autour de principes affirmant la nécessité que le développement et l'usage des technologies quantiques respectent les droits de la personne humaine, émergent certes peu à peu dans la littérature académique[76]. L'existence même de cette seconde révolution quantique, dont les effets ne seront pas mesurables avant des années, reste néanmoins mal connue par l'opinion publique comme de la communauté juridique...qui doivent pourtant s'en saisir aussi vite que possible.

internationale spatiale », *in* SFDI (collectif ; dir. Clémentine BORIES, Lucien RAPP), *L'espace extra-atmosphérique et le droit international. Colloque de Toulouse*, Paris, Pedone, 2021, pp. 359-376.

[76] V. l'exemple précité de Mauritz KOP, « Establishing a Legal-Ethical Framework for Quantum Technology », *op. cit.*