Géopolitique d'une pandémie à l'ère numérique

Par **Benjamin PAJOT**
et **Henri VERDIER**
Ministère de l'Europe et des Affaires étrangères

La crise du Covid-19 est la première grande pandémie du XXIe siècle, et nous n'avons pas fini d'en analyser les conséquences. Parmi d'innombrables enseignements, elle a constitué le premier test majeur de la capacité du « numérique » à nous permettre de répondre à une crise mondiale. Cette crise a fait naître de grands espoirs, suscité de nombreuses convoitises et provoqué des confrontations géopolitiques, avant de déboucher sur ce qui sera probablement la première leçon d'humilité de la révolution numérique.

Nous avons en effet entendu bien des récits sur la « numérisation accélérée » des entreprises et des administrations, nous avons reçu bien des promesses de « nouveau monde », certains pays et certaines entreprises se sont précipités pour vanter la supériorité de leurs modèles ou de leurs solutions, et pourtant l'observateur attentif notera probablement que cette pandémie aura surtout été marquée par :

- l'inutilité du numérique arrogant, celui qui prétendait monter jusqu'au ciel : malgré les promesses initiales de l'IA, du *big data* ou de l'Internet des objets, nos sociétés ont progressivement tourné le dos à ce solutionnisme technologique, et redécouvert la nécessité, face à une crise majeure, du "*staff and stuff*" : soignants, personnels, matériels, masques, respirateurs, et capacités de production industrielle ;
- l'adoption rapide d'un numérique de grande consommation (bureautique, visioconférences, *e*-commerce), quand il pouvait se prévaloir d'usages clairs et stabilisés ;
- et surtout, invisible aux analystes de Wall Street, les progrès d'un numérique humble et quotidien (réorganisations du travail, solidarités de voisinage, réunions de famille virtuelles, nouvelles pratiques culturelles).

Du point de vue géopolitique, la pandémie offre une autre leçon frappante : cette première crise mondiale du siècle, loin de susciter solidarité et coopération, a plutôt évolué en un affrontement de modèles et en bataille de narratifs, qui ont rapidement tourné court, mais laissé chaque bloc encore plus isolé dans sa propre logique.

Le Covid-19, première pandémie massive du XXIe siècle

Le Covid-19 n'est pas la toute première pandémie du XXIe siècle. Le SRAS, qui causa 774 morts en 2003, puis le H1N1, qui, selon le *Lancet*, causa entre 150 000 et 575 000 morts en 2011, avaient déjà conduit l'Organisation mondiale de la santé (OMS) à décréter l'état de pandémie.

Mais le Covid-19, beaucoup plus virulent et dix fois plus mortel que le H1N1, a déjà causé la mort de plus de trois millions de personnes. C'est une autre affaire. Il représentait, début 2020, une menace globale, dont la gravité était évidente, et dont il aurait été bien difficile de dire si le risque ne dépassait pas tout ce qui avait été connu auparavant. Rappelons par ailleurs que, si nous écrivons ces lignes à l'heure où la planète se bat pour accéder aux vaccins, il était parfaitement probable, début 2020, que la recherche d'une solution exige une dizaine d'années.

Une telle menace aurait pu appeler une réponse universelle, en vertu d'une solidarité internationale, ou au minimum en raison d'intérêts économiques convergents, hérités de plusieurs décennies de mondialisation néolibérale. Au contraire, la crise a révélé la forte crispation des relations internationales et la fragilité du système multilatéral actuel (ce dont l'OMS a été l'incarnation par excellence), et a rapidement débouché sur un choc de modèles. Car à mesure que chaque État déployait ses efforts pour lutter contre la pandémie, plusieurs stratégies nationales bien marquées, et parfois profondément divergentes, se sont dessinées.

Nous nous limiterons dans ces lignes à la manière dont ce choc des modèles s'est illustré dans le champ technologique, marquant ainsi l'entrée dans l'ère du « technonationalisme ». Depuis plusieurs années déjà, le monde s'inquiétait de la guerre technologique dans laquelle s'étaient engagés Washington et Pékin, et dont Donald Trump fut le spectaculaire porte-parole. Cet affrontement n'est donc pas neuf, mais la pandémie en a provoqué un réel durcissement.

La confrontation de modèles sociaux

Le premier choc fut probablement un choc de représentations politiques. L'Europe a son histoire de pandémies, qui a nourri son imaginaire propre, avec ses confinements, ses masques à bec d'oiseau et... ses restrictions nécessaires des libertés. L'Asie a le sien, plus collectif. Chacun pressentit rapidement que les deux visions s'affronteraient.

Le débat s'ouvrit en France avec une phrase étrange du tout nouveau ministre des Solidarités et de la Santé, Olivier Véran, lors de sa première interview. Après avoir salué les efforts de santé publique de la Chine, il déclara : « Je ne suis pas sûr que ce serait possible de réaliser tout cela dans un pays dans lequel les réseaux sociaux seraient ouverts ». Curieux propos venant d'un ministre qui ne manifesta pas particulièrement, ensuite, de pulsion de censure. Et c'est ce qui le rend instructif : un médecin respecté, un ministre respectable, prenant ses fonctions, arrive avec la peur que la liberté de parole, les "*fake news*" et le « complotisme » qui caractérisent les réseaux sociaux anéantissent tous les efforts de santé publique. D'où lui viennent cette crainte et cette comparaison ?

En Chine, la gestion du Covid-19 constitua une véritable revanche pour le Parti communiste chinois (PCC), traumatisé par le double épisode du SARS de 2003 et surtout de la grippe A (H1N1), lors de laquelle l'OMS avait mis les autorités en porte-à-faux en déclarant l'état de pandémie malgré les dénégations du PCC.

Ce dernier, après avoir minimisé dans un premier temps la gravité de l'épisode actuel, s'empressa, dès qu'il s'aperçut que les pays occidentaux peinaient, contre toute attente, à maîtriser la progression de la pandémie sur leur sol, de promouvoir activement son modèle de lutte contre le virus. Ce modèle était fondé en grande partie sur la mobilisation des grandes entreprises technologiques chinoises, notamment dans les provinces reculées où l'État central n'avait pas toujours réussi à organiser la réponse. Fournissant des solutions de traçage (applications), de contrôle (QR-codes) et de livraison à distance (drones), les géants chinois contribuèrent ainsi directement à dessiner une réponse nationale ayant par la suite fait l'objet d'une intense propagande. Celle-ci fit du contrôle social numérique des populations un atout maître, et la crise permit des expérimentations susceptibles de se pérenniser au niveau local (comme à Hangzhou, où les dispositifs de traçage numérique et de suivi sanitaire sont aujourd'hui rendus permanents) comme national (par le biais du renforcement du système de crédit social).

Cette réelle efficacité de la réponse chinoise (en tous cas au regard des critères de mortalité et de maîtrise des foyers épidémiques) troubla les démocraties, pour la plupart dépassées par les événements. La première réponse vint toutefois des démocraties de la région, signe que l'Asie de l'Est ne porte pas le même regard que nos sociétés sur les nouvelles technologies. Taiwan, la Corée

du Sud et dans une moindre mesure le Japon, déployèrent chacun à leur manière une gestion « techniciste » de la pandémie, appuyée sur le numérique et sur les gains de réactivité qu'il peut offrir, tout en assurant de réelles garanties du respect des libertés individuelles, parfois éloignées des standards occidentaux mais différant réellement des méthodes chinoises. Dans des sociétés marquées par de précédentes pandémies et par d'autres acceptions des principes de solidarité nationale et de responsabilité individuelle, le numérique contribua ainsi à une gestion plus efficace de la crise.

En revanche, nos sociétés occidentales, probablement victimes d'une certaine arrogance, se retrouvèrent rapidement confrontées à leurs vieux démons : gestion bureaucratique, verticalité de la décision, lenteurs administratives, défiance envers la société civile (certains ont rappelé à cette occasion que la grande école d'épidémiologie française était l'héritière d'une médecine « coloniale », forgée pour protéger des populations mal connues et mal comprises), défiance en retour de la société civile envers les autorités publiques, rejet de certains dispositifs technologiques, etc. S'y déroula rapidement un débat feutré sur la possibilité de prendre des mesures de restriction des libertés en démocratie, sur le biopouvoir, l'infantilisation et le contrôle social. De fait, l'« hygiénisme » du XXIe siècle se cherche encore.

La bataille des applications de traçage

En quelques semaines, la confrontation des imaginaires stratégiques convergea sur la question des applications de traçage, supposées aider à retrouver les cas contacts.

Ce débat fut largement importé d'Asie. Dans la stratégie « zéro virus », généralement adoptée dans la zone, le repérage immédiat, au cas près, des patients et de leurs cas contacts est essentiel. Mais dans les stratégies d'endiguement adoptées par tous les pays d'Europe, qui font que tout un chacun croise, tôt ou tard, la route d'un malade, la nécessité de ces applications est beaucoup moins évidente.

En Asie en revanche, même si les moyens techniques étaient parfois plus rudimentaires que les solutions imaginées par les Européens (les Coréens par exemple ont surtout utilisé la géolocalisation des téléphones, des tableurs Excel et parfois des bracelets électroniques), ces solutions firent florès. Singapour, en particulier, qui a fait de la modernité un marqueur fort, a consacré de réels efforts à promouvoir le code source ouvert de son application, certes non sans polémique ultérieure lorsqu'il fut proposé d'autoriser la police à utiliser les résultats de cette application.

Sous pression communicationnelle, l'Europe se sentit tenue de déployer ses propres dispositifs, bien décidée à montrer que le respect de la vie privée n'était pas une entrave à l'innovation ni à l'efficacité sociale. Elle s'engagea donc dans la voie des applications de traçage de contacts rendus anonymes. Le succès fut incertain : d'une part, il est quasiment impossible d'assurer l'inviolabilité totale d'un dispositif qui, *in fine*, doit être capable d'adresser un message aux cas contacts ; d'autre part, dans la précipitation, et sous le feu des polémiques, les équipes projet, dans la plupart des pays d'Europe, ont fini par sacrifier l'efficacité sanitaire. Mais surtout, cet épisode montra la difficulté, pour l'action publique, de piloter un projet en se concentrant en permanence sur son impact. À force de tenter de concilier les inquiétudes des uns et des autres, mais aussi de gérer les propositions de contribution des différents services et des entreprises nationales, le projet français, par exemple, perdit peu à peu une grande part de la pertinence sanitaire à laquelle il aurait pu prétendre.

Cette bataille des applications de traçage fut aussi une défaite pour la souveraineté numérique européenne. En effet, la question de savoir si une application pourrait exiger l'activation du Bluetooth sur téléphone, en activant directement le système d'exploitation, devint rapidement

centrale. On en comprend l'intérêt, mais on comprend également l'inquiétude des entreprises technologiques à accepter d'autoriser un État à activer des fonctionnalités à distance. Avec un tel précédent, de nombreux États, moins soucieux des libertés fondamentales que le nôtre, pourraient envisager des applications très inquiétantes. Apple et Google profitèrent de ce débat pour proposer une technologie qui était dans leur feuille de route (présentant une fonctionnalité très utile à la publicité géolocalisée, mais dont le développement était ralenti par des interrogations concernant aussi bien la protection de la vie privée que les règles contre les ententes). Au passage, bien entendu, ils conservaient le monopole d'accès au système d'exploitation. Dans cette controverse, la France, qui voulait un droit d'accès souverain au système d'exploitation, fut progressivement lâchée par l'ensemble des pays européens, et se retrouva donc avec une application non interopérable avec celle de ses partenaires. Visiblement, la question de la souveraineté numérique européenne manque encore à la fois d'un cadre conceptuel solide quand on en vient aux décisions techniques, et d'un cadre d'élaboration au sein des 27. Espérons au moins que tous les enseignements possibles seront tirés de cet épisode, notamment dans le cadre de l'élaboration du futur passeport sanitaire.

Cette bataille des applications de "*contact tracing*", au demeurant, n'est que la partie la plus visible d'une offensive généralisée des acteurs techno-sécuritaires, qui ont tenté de saisir l'occasion de cette crise pour s'implanter sur de nouveaux marchés.

La « pagaille informationnelle »

Alors que le monde se confinait progressivement, l'afflux d'informations contradictoires, anxiogènes ou fausses fit rapidement craindre aux autorités l'impossibilité de faire adopter les gestes sanitaires et de garantir l'acceptabilité de leurs mesures. Le secrétaire général des Nations unies y alla de son concept, estimant que nous faisions face à une « infodémie » dommageable pour la réponse publique à apporter. Il visait principalement, pour sa part, les rumeurs et les inepties sanitaires, sachant combien la rumeur peut se révéler le pire danger en cas d'épidémie.

Non sans une dose d'opportunisme, les principaux réseaux sociaux firent montre d'activisme et prirent de multiples dispositions pour lutter contre les fausses informations, et pour manifester ostensiblement leur engagement. Mais dans un contexte de coïncidence avec l'élection présidentielle américaine (et le poids qu'y jouèrent à la fois les "*fake news*", les groupes complotistes et le Covid-19), cette question initialement sanitaire s'agrégea insensiblement à toutes les autres questions liées aux contenus problématiques. Comme on le vit par la suite, les entreprises de la Silicon Valley, au cours de l'année, firent sauter bien des verrous qui semblaient intangibles au pays du "*First amendment*".

Il se joua également dans le champ informationnel une bataille de diplomatie publique d'une rare virulence, exacerbée par la rivalité sino-américaine. Elle porta d'abord sur l'origine du virus, et se déplaça ensuite vers le choc des modèles. On peut noter à ce titre l'inflexion profonde de la posture chinoise, à l'appui des « loups combattants », ces diplomates chargés de répandre la propagande du PCC et de « défendre » l'image de la Chine avec une agressivité inégalée sur les réseaux sociaux. Pour autant, il ne faut pas se tromper de lecture : les « loups combattants » servirent avant tout des objectifs de politique intérieure et s'adressèrent surtout à Pékin, à l'opinion intérieure et aux diasporas. Ils traduisirent aussi la fébrilité d'une Chine mise sous pression par l'opinion publique internationale.

Dans cette cacophonie générale, la dénonciation de véritables manipulations de l'information, c'est-à-dire d'opérations secrètes menées par des acteurs étatiques, fit florès. Si de nombreux signaux faibles ont montré que certains États jouèrent des ambiguïtés inhérentes à ces opérations, il n'y eut pas de signe patent d'une opération étatique d'ampleur liée au Covid-19. Mais il n'en fut pas de même en matière d'espionnage, voire d'opérations « cyber ».

L'explosion des risques cyber

Car la bascule générale vers le numérique et le télétravail entraînèrent un accroissement sans précédent de la surface d'exposition aux risques cyber, sans même parler de l'abandon de bien des procédures de sécurité ou du recours à des solutions non orthodoxes. À l'explosion de la cybercriminalité (multiplication par quatre du nombre d'actes criminels en France entre 2019 et 2020 selon l'ANSSI – l'Agence nationale de la sécurité des systèmes d'information), qui toucha sans distinction aussi bien des infrastructures publiques (mairies, hôpitaux, universités…) que privées, s'ajouta une explosion de l'espionnage par des moyens cyber, dont on ne mesure probablement pas encore toute l'ampleur. Les récentes manifestations de ce phénomène aux États-Unis (comme l'affaire SolarWinds) invitent à le prendre très au sérieux, et font redouter de lourdes conséquences à venir sur les moyen et long termes.

La généralisation de la prise de conscience de ces risques donna naissance à un discours sur la nécessité de protéger à l'échelle internationale les infrastructures sanitaires, relayé par la société civile et même par certains groupes de *hackers* (« *hackers* éthiques »).

Pour la première fois, dans les négociations de textes onusiens (le texte sur la cybersécurité adopté en mars 2021 représentant l'un des premiers documents de consensus de l'histoire, négocié en ligne par 140 pays), le sentiment qu'il fallait « vraiment » s'assurer que personne n'irait trop loin était palpable.

En revanche, la confusion entre cybercriminalité (qui se combat par l'action coordonnée de la police et la justice) et l'action des États (supposée régie par le droit international), entre sabotage, espionnage, vol de propriété intellectuelle ou simple fraude, fut à son comble, engendrant une réelle nervosité, et donc de réels risques de surréaction et d'escalade.

L'accélération de la fragmentation d'Internet

Cette montée des périls et des tensions, et ces réflexes protectionnistes, voire technonationalistes, eurent naturellement pour conséquence une augmentation des menaces sur l'unicité d'Internet. On ne parle pas seulement ici des diverses formes de censures nationales, qui se sont développées dans quasiment tous les pays, à la grande inquiétude de la société civile. Le « repli sur soi » numérique a également permis l'accélération de certains agendas menaçant cette unicité d'Internet : progrès des propositions de Huawei à l'UIT (Union internationale des télécommunications) de concevoir un nouveau protocole TCP/IP plus stable… parce que plus centralisé et accessoirement plus facile à contrôler ; applications bannies des *stores* en fonction de la nationalité des entreprises les ayant conçues ; accélération du projet de RU.net (essentiellement : un DNS – *domain name system* – russe permettant d'isoler la plupart des internautes russes dans une bulle filtrée par les autorités) ; agressivité de la Chine et de la Russie contre le caractère multi parties-prenantes de la gouvernance de l'ICANN (*Internet corporation for assigned names and numbers*).

La crainte que le technonationalisme n'en vienne à menacer l'intégrité même de l'Internet que nous connaissons, et notamment son caractère unifié, neutre et ouvert, n'est plus une chimère. La réaction des États démocratiques, et singulièrement de l'Europe, devient indispensable.

Innovations et coopérations

Dans ce contexte de forte conflictualité, on doit quand même noter quelques belles initiatives numériques locales, ainsi que de premières ébauches de coopération internationale.

Au rang de ces succès numériques, on doit probablement compter… le développement des vaccins. La mise au point de plusieurs vaccins en moins d'un an provient certes de l'argent considérable investi par les États dans ces projets et de l'ardeur de la compétition pour un marché potentiel de 7 milliards d'humains. Mais elle aurait été tout bonnement impossible sans la profonde transformation du monde de la recherche, notamment sous l'angle du partage et du traitement des données.

De même, nul ne semble s'étonner *a posteriori* de la capacité qu'eut l'assurance maladie à mettre en place en quelques mois une application permettant de suivre tous les cas positifs.

En Inde, le programme « Digital India » (l'« État plateforme » à l'indienne), qui facilita en particulier la création d'une identité numérique pour quasiment chaque Indien, conjugué aux dispositions de la loi sur la sécurité alimentaire de 2013, permit d'assurer l'aide alimentaire de 650 millions de personnes malgré le confinement.

Çà et là, on vit fleurir des coopérations originales, souvent portées par les cercles de *makers* et la société civile (comme le JustOneGiantLab parisien qui développa, entre autres, des réactifs en *open source* et bon marché pour produire des tests dans le monde entier). L'OIF (Organisation internationale de la francophonie), appuyée par la Belgique et la France, créa ainsi un réseau d'entraide avec les innovateurs africains qui rassembla rapidement 5 000 innovateurs, responsables de *fab-lab*, entrepreneurs, chercheurs, et leur permit de soutenir des initiatives de production locale de masques, de respirateurs, ou des actions de sensibilisation.

En France, l'AP-HP (Assistance publique-Hôpitaux de Paris), après avoir développé l'application « Covidom », qui servit à suivre à domicile un million de patients, accompagna le développement par la Tunisie d'une version en langue arabe.

Ces exemples, prometteurs et riches d'enseignements, ne suffisent pourtant pas à infirmer le diagnostic d'une absence globale de coopération entre États, ou entre États et sociétés civiles. En particulier, et contrairement à d'autres questions (comme la gestion des vaccins), l'Europe numérique s'est révélée cruellement inexistante. Elle doit capitaliser sur cet échec et se (re)mettre rapidement en ordre de bataille, face à la multiplication des enjeux et l'accélération causée par la pandémie.

De nouveaux défis pour l'Europe

Alors que la nouvelle Commission européenne se veut profondément « géopolitique », les défis à relever pour l'UE sont encore plus nombreux aujourd'hui qu'à la veille de la pandémie. Celle-ci se doit tout à la fois d'assurer la résilience et la sécurité de ses infrastructures numériques (câbles sous-marins, 5G, *cloud*, etc.), de protéger ses citoyens face à la multiplicité des menaces ("*harmful content*", manipulations de l'information, risques cyber…), et de réduire ses dépendances technologiques de sorte à préserver son autonomie en matière de choix stratégiques.

Pour cela, l'Europe peut s'appuyer sur sa puissance normative, incarnée par une série de textes fondamentaux et prises de position (RGPD, DSA, DMA, DGA [1], annulation du "Privacy Shield", "5G cyber toolbox", futures lignes directrices en matière d'IA) amenés à régir le marché commun numérique et à influencer la régulation au niveau mondial.

Elle peut compter sur sa puissance industrielle en cours de restructuration (plans semi-conducteurs, quantique, satellites, 6G), de refinancement (20 % du Plan de relance seront dédiés

(1) RGPD : règlement général sur la protection des données ; DSA : "Digital Services Act" ; DMA : "Digital Markets Act" ; DGA : "Data Governance Act".

au secteur numérique) et de réadaptation face aux nouveaux défis stratégiques de ce siècle (ce dont témoigne son Plan d'action sur les synergies entre les industries civile, spatiale et de défense).

Elle peut enfin s'appuyer sur une ambition, celle de devenir une puissance de coopération, capable de proposer de véritables partenariats en matière de développement et de souveraineté numériques des États partenaires (notamment en Afrique et dans l'Indopacifique), aux antipodes de ce que propose la Chine *via* ses routes de la soie numériques.

Mais elle devra pour cela se constituer en acteur réel, développeur et exportateur de solutions, familier des communs numériques, habitué, d'abord en son sein puis avec ses grands partenaires, aux coopérations effectives. La crise du Covid-19 a prouvé qu'elle en était loin.

Conclusion

Révélatrice des tensions préexistantes sur la scène internationale, la pandémie a joué le rôle de catalyseur dans la polarisation technologique croissante entre Extrême-Orient et Occident, qui ne se réduit pas au seul affrontement sino-américain. Le fameux « pivot vers l'Asie » s'en trouve conforté, et nos démocraties occidentales, hantées par le spectre de leurs échecs, ont de fait reçu une leçon d'humilité. Elles devront trouver le bon équilibre entre s'inspirer davantage de modèles à l'efficacité éprouvée (Taiwan constituant un cas d'école) et préserver leur propre logiciel, valeurs et appréhension de ce qui est acceptable ou non en temps de crise.

Il leur faudra pour cela interroger toujours un peu plus leur rapport aux technologies numériques. Car le numérique ne doit pas être rendu responsable de notre incapacité à gérer cette crise efficacement : celle-ci tient avant tout à notre immaturité collective.

Au regard de la pandémie actuelle, force est de constater que la planète n'a pas beaucoup progressé depuis le Moyen Âge. L'aphorisme médiéval « pars vite, et reviens tard », avec tout ce qu'il comprend d'individualisme, reste d'une triste actualité. La crise a entraîné des dynamiques somme toute classiques de repli sur soi, restrictions des libertés, peur de l'autre et démagogie, dont le numérique a constitué une caisse de résonance et un amplificateur logique.

On peut se demander aussi s'il n'a pas également joué un rôle positif moins visible : vitesse de la réaction internationale, compréhension rapide des enjeux par les citoyens (la diffusion rapide de la cérémonie des applaudissements aux soignants). Mais ces résultats ne doivent pas cacher que le potentiel du numérique n'a pas réellement été mobilisé : nous n'avons pas su tirer parti de la disponibilité d'une infrastructure ouverte partagée par toute l'humanité, des possibilités de synchronisation et de partage de données, des possibilités de diffuser de la capacité d'action dans les zones les plus déshéritées… et n'avons pas su capitaliser sur les possibilités pourtant réelles de mobiliser et d'équiper la société civile.

Le Covid-19 n'est sans doute que la première pandémie du XXI^{e} siècle : l'état dans lequel nous avons plongé la planète et l'organisation de nos échanges mondialisés laissent penser que nous en connaîtrons de pires. La prise de conscience de cette insuffisance de la réponse internationale et des dangers d'instabilité et de confrontation que nous avons connus, et l'organisation en vue de proposer de meilleures réponses à l'avenir, en ayant recours au numérique là et quand cela s'avère nécessaire, sont désormais notre responsabilité collective.