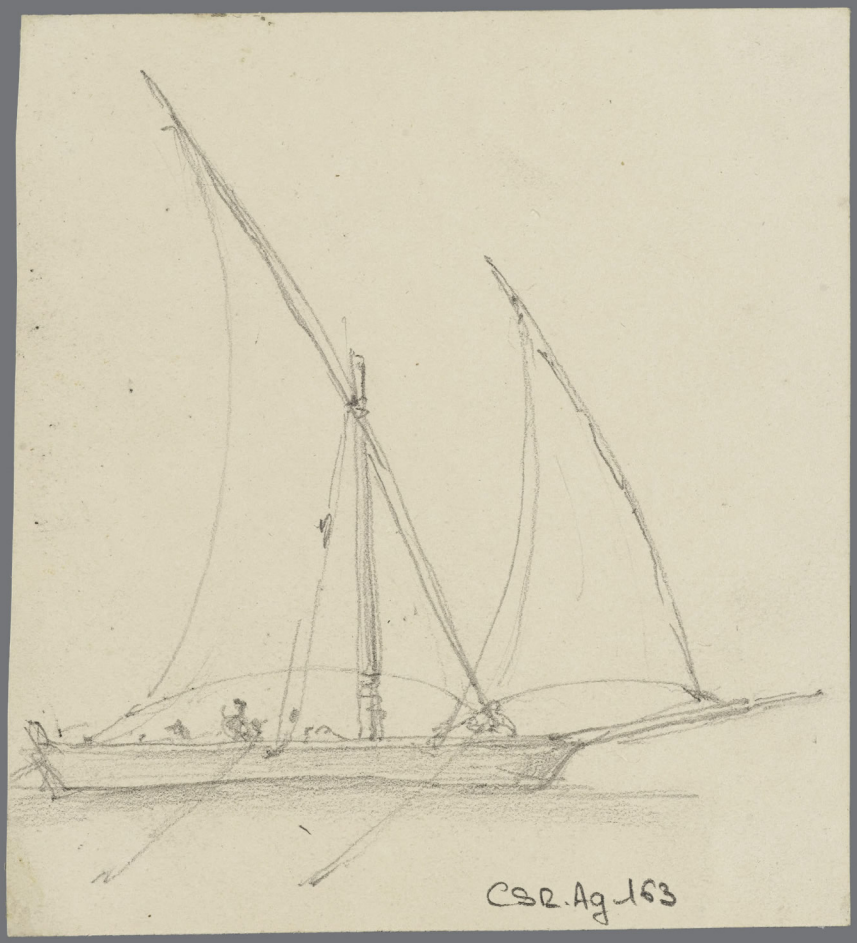
Enjeux numériques



La souveraineté numérique : dix ans de débats, et après ?

UNE SÉRIE DES
ANNALES DES MINES
FONDÉES EN 1794

N°23 - SEPTEMBRE 2023

Publiées avec le soutien de l'Institut Mines-Télécom

UNE SÉRIE DES

ANNALES
DES MINES

FONDÉES EN 1794

ENJEUX NUMÉRIQUES

ISSN 2781-1263 (en ligne)
ISSN 2607-9984 (imprimé)
Série trimestrielle - N°23 - Septembre 2023

Rédaction

Conseil général de l'Économie
Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique
120, rue de Bercy
Télédoc 797
75572 Paris Cedex 12
Tél. : 01 53 18 52 68
http://www.annales.org

Grégoire Postel-Vinay
Rédacteur en chef

Gérard Comby
Secrétaire général

Alexia Kappelmann
Secrétaire générale

Daniel Boula
Secrétaire général adjoint

Magali Gimon
Assistante de rédaction et Maquettiste

Myriam Michaux
Webmestre et Maquettiste

Publication

Photo de couverture
René Marjolin, dessinateur, *Étude de bateau*, dessin, 19e siècle. Paris, Musée de la Vie romantique (©Paris Musées / Musée de la Vie Romantique)

Iconographie
Alexia Kappelmann

Mise en page
Magali Gimon

Impression
Dupliprint Mayenne

La souveraineté numérique : dix ans de débats, et après ?

Ce numéro a été coordonné par
Julien NOCETTI

Introduction
Souveraineté numérique : dix ans de débats, et après ?

Par Julien NOCETTI
Chercheur, GEODE (Géopolitique de la datasphère, Université Paris 8) et IFRI

Faut-il se réjouir qu'en 2023 la souveraineté numérique suscite des débats aussi polymorphes et extraits des seuls cercles d'expertise auxquels elle a été confinée pendant des années ? Il est peu de dire que l'enjeu dont il est question dans ce numéro a pris une dimension nouvelle, bien au-delà de sa quasi-exclusive coloration technologique et industrielle d'origine, pour embrasser une série d'enjeux de nature démocratique, socio-économique, sécuritaire et de défense, financière, de formation, etc.

Une actualité omniprésente

En 2023 donc, une part substantielle de l'actualité numérique et technologique renvoie à des considérations souveraines. En juillet, la polémique née de la nomination, par la Commission européenne, d'une experte américaine au poste de cheffe économiste à l'influente direction générale de la concurrence, chargée d'enquêter sur les pratiques anti-concurrentielles des entreprises – dont les Gafam – révèle tout autant le manque de sens politique de la Commission sur un enjeu majeur de la relation transatlantique et le risque bien réel d'instrumentalisation politique par des formations eurosceptiques.

En outre, le projecteur politique placé sur TikTok, des deux côtés de l'Atlantique, montre bien que la régulation des plateformes du numérique se situe au cœur des rapports de puissance, tant entre alliés qu'entre adversaires géopolitiques. Il est frappant de remarquer les analogies du discours américain sur TikTok avec les inquiétudes exprimées de longue date par l'Union européenne (UE) en matière de « souveraineté numérique ». À travers son expansion numérique, la Chine tendrait-elle un miroir déformant aux États-Unis ? Comme lors de l'entrée en application du RGPD (Règlement général de protection des données) européen, en mai 2018, l'effet d'entraînement normatif de l'UE est et restera scruté de près avec l'affaire TikTok, à travers la mobilisation des outils juridiques de celle-ci, à commencer par le Digital Services Act (DSA) entrant en vigueur.

« Dix ans de débats », suggère le titre du présent numéro. À l'évidence, la souveraineté numérique telle que discutée en 2012-2013 est différente de celle actuellement débattue. Le concept n'est lui-même pas apparu partout au même moment. En Europe, et en France en particulier, est évoqué le lien entre la souveraineté des États et l'ère de foisonnement numérique qui s'ouvre entre le milieu et la fin des années 2000, sous l'influence (certes encore modeste) de débats internationaux qui, de Genève à Tunis, commençaient à replacer les États en haut de la pyramide des acteurs de la gouvernance de l'internet. Le concept, sans surprise, monte en puissance au moment des révélations de l'ancien contractuel de la National Security Agency (NSA) américaine Edward Snowden, en juin 2013, avant que l'emprise croissante des grandes plateformes californiennes ne vienne révéler crûment les propres failles de l'Europe en matière de souveraineté.

L'extension du champ de la souveraineté numérique

Une décennie plus tôt, les débats sur la souveraineté numérique demeuraient souvent centrés autour de la réponse apportée à la question « qui contrôle internet ? ». Ils sont, depuis, élargis par l'extension considérable du champ numérique porté par le développement et la dissémination des technologies dites émergentes (ou critiques) : intelligences artificielles, réseaux 5G, quantique. Élargir la focale se révèle donc une nécessité absolue, en y ajoutant par ailleurs l'enjeu de la maîtrise des algorithmes sensibles et, autre fait d'actualité notable, l'approvisionnement en composants critiques.

En réalité, l'extension du domaine de la souveraineté numérique fait s'imbriquer sans aucune ambiguïté désormais la question industrielle et la question géopolitique. C'est tout particulièrement le cas dans le domaine des semi-conducteurs, dans lequel la Chine poursuit ses efforts d'autonomisation et de rattrapage technologique dans les semi-conducteurs avancés, mais ceux-ci constituent le maillon faible de la stratégie de développement chinoise centrée sur l'innovation. Les aspirations de Pékin dans ce domaine ne se sont jamais traduites par un quelconque *leadership*, ce depuis le « Plan 531 » de 1986 ou le fonds doté de 50 milliards de dollars pour les circuits intégrés en 2014. Les fabricants chinois manquent d'une base industrielle et d'un savoir-faire suffisamment solides dans ce secteur, surtout pour les composants les plus sophistiqués, ce qui conduit à faire des puces le premier poste d'importation du pays, devant les hydrocarbures[1]. Le facteur géopolitique vient limiter la capacité de la Chine à rattraper son retard sur le court terme, qui mise sur ses avancées en matière d'intelligence artificielle (IA) pour combler son retard. Il n'en demeure pas moins que les montants publiés – un soutien étatique chinois à la filière qui se chiffrerait à plus de 290 milliards de dollars en 2021-2022[2] – donnent un double sentiment de vertige et d'une bataille rangée pour la maîtrise de la production et des chaînes d'approvisionnement. En Europe, les luttes d'influence entre États (Allemagne, France, etc.) pour attirer des investissements taïwanais et américains afin de relocaliser (très partiellement) un tissu de production sur le continent illustrent bien la prise en compte d'une dimension géopolitique tout autant que les errements du *fabless* à tout crin.

Il faut dire que la souveraineté numérique n'est pas comprise de manière uniforme – c'est une litote. Des États comme la Chine et la Russie, mais pas seulement, ont pensé de longue date la souveraineté numérique sous le prisme de la souveraineté de l'information (c'est-à-dire du contenu produit sur le *Web* et des messages échangés). Cette différence ne doit pas être traitée de manière hors-sol : avec la multiplication des risques portés par la diffusion des discours de haine et des campagnes de manipulations informationnelles, l'aspect « cognitif » de la souveraineté numérique ne peut dorénavant être écarté d'un revers de main, à plus forte raison lorsque certaines pratiques des États démocratiques s'alignent – toutes proportions gardées – avec les pratiques de régimes autoritaires. La souveraineté numérique est donc, par extension, un enjeu lié à la défense de valeurs spécifiques.

[1] CAPRI A. (2021), "China's microchip ambitions: Semiconductors advance the next phase of technonationalism", Report, Hinrich Foundation, juin 2021, disponible sur www.hinrichfoundation.com.

[2] LIN J. (2023), "China invested US$ 290.8 billion in semiconductor projects between 2021-2022", *DigiTimes Asia*, 27 juin 2023.

La double lecture d'une « souveraineté numérique européenne »

En Europe – puisqu'il s'agit grandement, dans ces colonnes, de replacer les débats dans cette perspective géographique et politique –, la décennie écoulée a essentiellement vu le concept de souveraineté numérique accolé à l'idée de servitude. À grands renforts de termes évoquant celle-ci (« colonie », « vassalisée », « sous tutelle », « garde-manger de trois empires »), une lecture répandue considère que l'Europe est (quasiment) sortie de l'histoire numérique en raison d'un dépeçage en règle de sa capacité d'autonomie politique et économique. Pessimiste, cette appréciation n'en conserve pas moins un fond de vérité tant les pays européens ont contribué à l'expansion des grandes plateformes privées extra-européennes et ont délocalisé leurs outils de production sans anticiper qu'ils subiraient un double effet ciseau – l'hégémonie américaine et l'affirmation chinoise. Elle reste aussi largement stato-centrée, alors que l'enjeu de la souveraineté numérique concerne également l'auto-détermination des individus. Enfin, telle que conceptualisée dans la décennie 2010, la souveraineté numérique tend à masquer les logiques d'interdépendances qui sont les marqueurs de notre époque.

La seconde lecture procède à l'inverse d'une croyance dans la capacité d'action de l'Europe dans le numérique, laquelle fonderait une politique en mouvement. Le numérique est l'un des très rares domaines dans lequel l'UE parle de souveraineté, qu'elle dépolitise le plus souvent en le resituant dans le cadre du marché et du droit. La valeur des entreprises de technologie européennes a été multipliée par quatre ces sept dernières années. L'Europe compte le plus grand nombre de scientifiques de haut niveau dans l'IA et plus de développeurs de logiciels que les États-Unis[3]. La formation du capital humain est un atout autant qu'une faiblesse en Europe qui devra éviter la fuite de ses meilleurs experts pour pouvoir espérer peser contre le duopole sino-américain. C'est en étant capable de choisir ses interdépendances que l'Europe parviendra à surmonter sa précarité technologique.

Conclusion

Enfin, la souveraineté numérique est devenue indissociable de l'effet systémique et de domination produit par les Gafam. Si l'érosion des prérogatives souveraines des États par l'action de ces acteurs est aujourd'hui bien documentée[4], il faut éviter de céder à l'effet de halo plaçant ces oligopoles technologiques au centre de tous les enjeux de souveraineté (numérique) – qu'ils contribuent d'ailleurs à déspatialiser –, avec le risque d'occulter des pans entiers de réflexion et d'action politique et industrielle. Là n'est pas le moindre des enjeux.

L'ensemble de ces constats et enjeux innervent la présente édition, dont l'objectif est d'actualiser un débat devenu plus dense et réfléchi, mais en même temps plus polarisé, avec le souci de proposer des pistes et leviers d'action.

[3] Discours d'Ursula von der Leyen, Web Summit, 2 décembre 2020, disponible sur https://ec.europa.eu/

[4] À titre d'exemple : TOLEDANO J. (2021), *Gafa : Reprenons le pouvoir !,* Paris, Odile Jacob.

Souveraineté numérique, une occasion manquée

Par Tariq KRIM
Entrepreneur et pionnier de l'Internet

Le débat sur la souveraineté numérique, un sujet qui divise les acteurs du numérique et institutionnels, coïncide avec l'arrivée de l'Internet commercial au début des années 1990. La combinaison de la désindustrialisation de nos industries télécoms, de la « dénumérisation » de l'informatique d'État et d'un modèle de croissance fondé sur l'utilisation des services des grandes plateformes américaines nous a mis dans une situation de grande dépendance. La France doit désormais avec la guerre en Ukraine s'assurer qu'elle dispose encore d'une forme de résilience numérique en s'appuyant sur son écosystème local.

Le débat sur la souveraineté numérique, un sujet qui divise les acteurs du numérique et institutionnels, coïncide avec l'arrivée de l'Internet commercial au début des années 1990.

Avant l'adoption de cette technologie essentiellement américaine (bien qu'une partie de son architecture décentralisée originale, le datagramme, ait été imaginée par Louis Pouzin) la France était le pays de référence dans la conception et le savoir-faire de produits numériques à grande échelle : le Minitel, Numéris ou encore la carte Vitale.

Elle était capable de déployer intégralement des réseaux filaires, satellitaires, mobiles ou des câbles sous-marins en s'appuyant quasi exclusivement sur ses acteurs industriels nationaux, qui étaient d'ailleurs considérés à l'époque parmi les meilleurs au monde. Mais cette excellence s'inscrivait dans le cadre d'un environnement technique fermé dont les cycles d'innovation étaient définis à l'avance par les industriels, les instances de normalisation et les opérateurs de télécom. C'est ce savoir-faire qui sera démantelé dans les trente années qui suivirent.

En 2023, avec un risque réel d'une fragmentation et d'une militarisation de l'Internet, conséquence de la guerre en Ukraine et de la nouvelle guerre froide entre les États-Unis et la Chine, la France aurait eu bien besoin de ses capacités souveraines d'antan, notamment au niveau de ses infrastructures. Hélas, nous ne sommes plus capables d'affronter ces nouveaux défis pour cause d'une dépendance trop importante vis-à-vis des briques technologiques développées par la Silicon Valley, Taiwan, la Corée ou encore la Chine.

Cette dépendance oblige d'ailleurs l'ensemble des pays européens, à défaut de mettre en œuvre une véritable politique de souveraineté[1], à s'assurer qu'ils ont à leur disposition un

[1] Nonobstant des inflexions récentes : le 29 septembre 2017, un sommet des chefs d'États européens était, pour la première fois, intégralement consacré au numérique et affirmait une volonté commune de faire de l'Europe une puissance numérique. Il fut suivi dans un premier temps par des avancées sur les droits d'auteurs, les services de médias audiovisuels et par les réunions de Tallin et Helsinki sur l'IA et l'éthique et stratégie IA. La présidence française de l'UE en a fait un de ses chevaux de bataille, https://www.economie.gouv.fr/pfue-reunion-informelle-des-ministres-charges-des-telecommunications# et l'UE s'est lancée dans une activité réglementaire notable (Digital Governance Act, Data Act, Digital Market Act, Digital Service Act, régulation de l'IA…). Toutefois, la guerre en Ukraine a marqué de nouveau une inflexion sous l'égide de l'Otan, plus en faveur d'une suprématie américaine (espace, cybersécurité…).

plan B de résilience numérique en cas de basculement du conflit en guerre numérique de haute intensité[2].

Comment en sommes-nous arrivés là ? Cet article revient sur la séquence d'événements qui se sont enchaînés et qui ont conduit à la situation actuelle.

Introduction

Les historiens étudieront peut-être un jour les raisons qui ont conduit, après plusieurs décennies d'excellence en matière d'informatique et de réseau, à la perte de compétitivité des industries d'électronique grand public et de télécoms françaises, et à une intégration logicielle avec les grandes plateformes américaines.

Cette stratégie à contretemps des enjeux géopolitiques peut s'expliquer par deux raisons apparentes.

La première est liée au fait qu'une partie de l'élite économique française convertie dès les années 1990 à l'utopie d'un Internet ouvert à tous et fascinée par les succès de la Silicon Valley n'aura de cesse de critiquer le modèle national (notamment le Minitel) et de réclamer une intégration immédiate au réseau mondial sans s'assurer que nos industries télécoms pourraient y prospérer. Un parallèle peut être également fait aujourd'hui avec les injonctions pour une importation massive de voitures électriques d'origine extra-européenne sans analyser les conséquences pour les acteurs européens de l'automobile.

La seconde est d'avoir voulu, avec la *French Tech*, être le meilleur élève du modèle d'ultra-croissance des licornes sans avoir pris le temps de comprendre que nos dépendances aux acteurs du *cloud*, du référencement, de la publicité des grandes plateformes américaines rendaient cette course extrêmement coûteuse et difficilement atteignable.

Mais c'est une tout autre raison, plus culturelle, qu'il faut envisager. Avec la migration vers le tout logiciel, notre savoir-faire industriel et notre perception de la technologie auraient dû être entièrement repensés. La création logicielle est un art et les talents capables de construire des produits d'exception sont extrêmement rares. Aux États-Unis, ils sont choyés et soutenus au point d'accepter que leurs entreprises ne soient pas rentables pendant plusieurs années. Le terme de licorne est d'ailleurs introduit en 2013 par Aileen Lee[3] pour définir l'extrême rareté de ces entreprises capables de monopoliser un secteur. En Europe, on aura surtout retenu l'idée d'une valorisation à hauteur d'un milliard de dollars devenue à tort le seul mètre-étalon des stratégies numériques des États.

Ce critère de rareté a du mal à s'imposer en France. De nombreux talents, effrayés par l'obsession des investisseurs et des institutions pour une rentabilité à court terme, leur mécompréhension du rôle central du produit et l'absence de prise de risque, sont partis s'exiler aux États-Unis dès les années 2010 où ils ont été accueillis en héros pour y construire les meilleures entreprises technologiques d'origine française[4].

Comme nous allons le voir dans cet article, notre incapacité à maintenir notre souveraineté numérique est une histoire en cinq actes qui mélange naïveté, erreur de jugement et manque de courage. À l'aube d'un nouveau conflit numérique mondial, il est important d'en comprendre les ressorts pour ne plus reproduire les mêmes erreurs.

[2] https://www.cybernetica.fr/souverainete-numerique-est-morte-vive-la-resilience/

[3] Lire https://techcrunch.com/2013/11/02/welcome-to-the-unicorn-club/

[4] Algolia, Dataiku, Snowflake, Hugging Face notamment.

Le terreau fertile de l'avant Internet

Avant de détailler les raisons qui ont amené la France à perdre une grande partie de sa souveraineté numérique, il est important de rappeler que la France a été capable de construire des industries informatiques, télécoms et technologiques de premier plan. Dans la foulée du plan Calcul, lancé en 1966[5], la France devient l'un des *leaders* du numérique dans le monde. Pour les besoins de conception de la bombe atomique, mais pas uniquement. Contrairement à ce qui est souvent annoncé, la France s'intéresse très tôt également au domaine de la bureautique. Il y a certes des partenariats avec de grandes entreprises américaines, notamment la société Honeywell, mais la France conserve un *leadership* d'idées et de technologies. C'est François Gernelle qui révolutionne le marché de l'informatique en créant le premier micro-ordinateur, bien avant ses concurrents américains sur les microprocesseurs Intel. Avec la télématique, les équipes de recherche du CNET puis du CCETT mettront en œuvre le plus grand réseau mondial basé sur les technologies de commutation par paquets X25 : Transpac et son terminal Minitel. À ce réseau souverain s'ajoutent l'implémentation réussie du réseau Numéris, le déploiement d'un réseau mobile GSM de qualité mondiale et le succès du déploiement de l'ADSL et des stratégies de *triple play*.

C'est avec l'arrivée de l'Internet que la machine s'enraye.

Le mythe d'un réseau mondial ouvert

Si l'Internet prend les industriels américains et européens par surprise, il n'est pourtant pas voué au départ à devenir un tel succès. D'origine militaire, mais popularisé dans les universités du monde entier, ce réseau relie essentiellement des stations Unix qui ne sont pas des équipements grand public. Au même moment, l'administration Clinton souhaite lancer un projet parallèle d'autoroutes de l'information qui propose de déployer des services fermés interactifs opérés par les géants de l'édition, de l'informatique et des télécoms. Cette vision, qui s'inspire du modèle français du Minitel[6], sera prise de court par la popularité des premiers fournisseurs d'accès internet et la possibilité pour des ordinateurs personnels d'accéder au *web* grâce au logiciel Netscape. Dès 1994, Microsoft, dans son fameux mémo, reconnaît qu'il faut d'urgence embrasser cette technologie. En France, la décision sera prise en 1999 par le Premier ministre Lionel Jospin lors de son discours d'Hourtin.

Dès ses débuts, l'Internet orchestre une mythologie d'un réseau ouvert, décentralisé et à l'abri de toute hiérarchie. Mais le contrôle technique et la gouvernance du réseau restent essentiellement américains. Surfinancées par l'argent des investisseurs de la Silicon Valley, les *start-up* créées dans la foulée vont rapidement dominer le monde du *web*.

Elles obligent l'Europe à se replier sur le GSM et la télévision interactive où leur contrôle industriel et normatif est encore significatif.

La déconstruction de notre avantage numérique

Alors que l'Internet semble devenir le nouveau vecteur de croissance de l'économie mondiale, l'Europe et la France en particulier vont fortement se désengager.

[5] https://www.gouvernement.fr/partage/8705-juillet-1966-lancement-du-plan-calcul-informatique-par-le-general-de-gaulle-et-le-gouvernement

[6] https://www.liberation.fr/futurs/1995/02/27/david-lytel-un-americain-a-l-ecole-du-minitel_121979/

Il y a tout d'abord la désindustrialisation des secteurs des télécoms et de l'électronique grand public qui verront coup sur coup la disparition ou le dépeçage de sociétés comme Thomson, Alcatel. Elle met en exergue l'ignorance du politique. Ces sociétés sont vues comme de simples acteurs industriels alors qu'elles disposent des brevets essentiels pour la distribution de contenus numériques (MP3, MPEG).

Il y a ensuite la privatisation et l'ouverture à la concurrence des réseaux téléphoniques nationaux qui seront également un coup dur pour les laboratoires de recherche de France Télécom qui se retrouveront en compétition frontale avec la Silicon Valley.

Il faut également noter le rôle prépondérant de l'ordinateur comme nouveau *hub* multimédia qui oblige les acteurs européens à se repositionner comme simples fabricants de périphériques informatiques. Une recomposition du secteur qui renforcera naturellement les acteurs américains (par exemple sur les baladeurs, télévisions et périphériques multimédias).

Il y a enfin la « dénumérisation » de l'État et des grandes entreprises qui décident à cette époque de transférer les compétences en développement logiciel vers les cabinets de conseils et ESN[7]. La conséquence sera le remplacement des informaticiens capables de développer des solutions sur mesure par l'achat de produits « sur étagère ».

Il faut noter qu'au moment où nos ingénieurs sont mis en concurrence avec les informaticiens indiens[8], les *start-up* américaines embauchent les meilleurs ingénieurs français pour constituer leurs équipes de recherches. Beaucoup d'entre eux seront essentiels pour permettre aux Gafam de développer le *smartphone*, la voiture autonome, l'intelligence artificielle ou même le *cloud*[9].

Cette perte n'est pas qu'industrielle, elle est également normative. Bien qu'inventés en Europe, Linux et le *web* voient leurs fondations respectives W3C et Linux Foundation se déplacer aux États-Unis. Ce sont désormais les géants du mobile américains qui contrôlent la destinée du *web*.

Ils feront tout pour empêcher le *web* d'avancer suffisamment rapidement pour concurrencer les applications mobiles[10].

L'ère des monopoles mondiaux

Avec l'introduction de l'iPhone, l'avance technologique de l'Europe dans le domaine réservé du mobile disparaît. Et avec elle, les principales marques de téléphone mobile européennes.

2007 est une année importante car elle est le point de départ de la convergence du mobile, du *cloud* et des réseaux sociaux qui permettront à la Silicon Valley de dominer totalement les interfaces utilisateurs, la gestion des données dans le *cloud* ainsi que les graphes sociaux de milliards d'utilisateurs.

La privatisation des interfaces mobiles au détriment du *web* ouvert ouvre la possibilité de transformer radicalement l'économie Internet en modèle locatif. Seul un petit nombre d'élus, les licornes[11], vont sur-accélérer leur croissance grâce à leur maîtrise de cet envi-

[7] Entreprise de services du numérique.

[8] https://www.lesechos.fr/2009/02/capgemini-deplace-son-centre-de-gravite-vers-linde-448961

[9] https://www.cybernetica.fr/mission-gouvernementale-liste-dune-centaine-de-developpeurs-marquants/

[10] https://doctorow.medium.com/web-apps-could-de-monopolize-mobile-devices-57e8a2d4bfb2

[11] Uber, Airbnb, Dropbox, Asana, Box, Snap.

ronnement pour devenir en quelques années des acteurs mondiaux aux côtés de Google, Apple, Facebook, Amazon et Microsoft (Gafam).

Cette capacité d'hyper-croissance (référencement, promotion sur les réseaux sociaux, disponibilité sur les magasins d'applications, passage à l'échelle en mode *cloud*) sera commercialisée ensuite au reste du monde. Elle promet à toute société qui dépense suffisamment d'argent sur ces services d'atteindre une croissance ultrarapide.

Elle va séduire beaucoup d'acteurs européens qui croient en leurs chances sur le marché mondial.

L'espérance d'un renouveau français motorisé par les Gafam et les idéaux de la Silicon Valley

La *start-up* nation et sa marque commerciale la *French Tech* démarre en 2013 à l'occasion d'un rapport de préfiguration remis à Fleur Pellerin[12]. Mais c'est avec l'arrivée d'Emmanuel Macron qu'elle prend véritablement son envol. Elle s'appuie, comme dans la plupart des autres pays d'Europe, sur la doctrine d'hyper-croissance des licornes, c'est-à-dire le déploiement rapide d'applications mobiles capables de répondre aux besoins des utilisateurs, mais aussi sur l'ubérisation de certains secteurs d'activités économiques ou réglementaires. Ce modèle très populaire dans les écoles de commerce va rapidement devenir le modèle le plus soutenu en France. En quelques années l'objectif de création de quelques dizaines de licornes dont la valorisation dépasse le milliard d'euros est atteint[13].

En octobre 2022, on compte dans le monde 1 191 licornes pour une capitalisation globale de 3 853 milliards de dollars, dont 85,5 % en valeur dans six pays :

États-Unis	644	2 074 G$	(53,80 %)
Chine	172	669 G$	(17,40 %)
Royaume Uni	46	208 G$	(5,40 %)
Inde	70	203 G$	(5,30 %)
Allemagne	29	81 G$	(2,10 %)
France	24	58 G$	(1,52 %)

Une injonction similaire se met en œuvre en parallèle dans les grandes entreprises où l'on utilise la terminologie de transformation numérique. De nombreuses entreprises du CAC 40 vont mettre en place des partenariats stratégiques avec les Gafam et déporter des fonctions prioritaires de l'entreprise dans leurs *clouds*. L'objectif affiché est d'atteindre la même agilité et capacité d'innovation que les grands de la Silicon Valley.

Ce modèle est assez simple à mettre en œuvre, mais il est coûteux, car toute la chaîne de valeur de la transition numérique autrefois possédée par l'entreprise est disponible sous forme d'abonnements payants dans le *cloud*. À ce jeu, peu d'entreprises françaises du

[12] https://www.cybernetica.fr/les-developpeurs-un-atout-pour-la-france/

[13] https://www.bfmtv.com/economie/cedric-o-l-objectif-des-25-licornes-pourrait-etre-atteint_VN-202201050483.html

cloud arrivent à tirer leur épingle du jeu et l'immense majorité des services retenus pour motoriser le CAC 40 sont américains[14].

Jusqu'à présent épargnés, pour des raisons de sécurité nationale et de souveraineté, l'État et l'administration sont pressés d'opérer les mêmes transformations. Avec la doctrine de l'État Plateforme, qui s'inspire du modèle américain *Government as a platform*, utilise les mêmes ressorts d'hyper-croissance des licornes. Avec la doctrine *cloud* au centre, une partie des services publics doit être transférée vers le *cloud*. Grâce à la norme SecNumCloud et un montage juridique complexe, il sera permis d'ici 2024 à l'administration d'opérer sur des versions sous licences françaises des *clouds* américains.

Quel avenir pour la souveraineté numérique française ?

La crise du Covid, la guerre en Ukraine et la nouvelle guerre froide technologique entre les États-Unis et la Chine pourraient remettre en question la pertinence de cette stratégie d'intégration pensée pour les situations de paix.

Tout d'abord le coût de l'énergie et le prix des puces font exploser les coûts du numérique. Le modèle du *cloud* s'avère plus coûteux que prévu. L'inflation impacte également la rentabilité des stratégies d'hyper-croissance au point qu'aux États-Unis, où le prix de l'énergie est plus compétitif, certains investisseurs remettent déjà en question le modèle du *cloud*[15].

Ensuite, la hausse des taux d'intérêt s'accompagne d'une crise importante des liquidités qui pourrait mettre en difficulté le financement de la *French Tech*, certaines *start-up* ayant déjà annoncé d'importants licenciements[16]. Il est vrai qu'avec des taux d'intérêts encore plus élevés aux États-Unis, ce phénomène a frappé au moins autant les concurrents d'outre-Atlantique, mais une part de ceux-ci disposent de moyens plus importants.

Enfin les enseignements de la guerre en Ukraine qui a déplacé, avant le conflit, le cœur de son État numérique chez Amazon et Microsoft et nous obligent désormais à envisager le *cloud* comme un outil de négociation géopolitique.

Si nous souhaitons minimiser l'impact des grandes plateformes dans notre politique étrangère, alors il faut réintroduire des capacités de souveraineté numérique et construire une infrastructure d'émancipation indépendante des Gafam. Sinon, à l'instar de nombreux pays européens, nous négocions un pacte de sécurité technologique avec les Gafam mais dont le coût économique et politique reste encore à déterminer.

Indépendamment du choix qui sera retenu, la France va devoir aussi investir dans sa résilience, c'est-à-dire la capacité à opérer un service minimal en cas d'extension à l'Europe d'un conflit numérique similaire à celui actuellement à l'œuvre en Ukraine (sabotage de câbles sous-marins, cyberattaque, brouillage des communications).

[14] https://www.zdnet.fr/actualites/zd-tech-le-cloud-francais-ecrase-par-trois-geants-americains-39942686.htm

[15] https://www.infoworld.com/article/3684369/2023-could-be-the-year-of-public-cloud-repatriation.html

[16] https://www.latribune.fr/technos-medias/innovation-et-start-up/french-tech-vague-de-licenciements-dans-les-startups-sous-la-pression-des-investisseurs-962902.html

Numérique et marché : souveraineté de fait, souveraineté par le droit

Par Annie BLANDIN
Professeur à l'IMT Atlantique

Un discours critique se déploie sur les orientations prises par la France et l'Union européenne dans le domaine de la souveraineté numérique. Il se focalise en partie sur la place du droit. Celui-ci cantonnerait l'Union dans un rôle subalterne quand d'autres (les États-Unis au premier chef) maîtrisent les fondations du numérique. Pour éclairer cette question, l'article présente la souveraineté numérique de fait et la souveraineté par le droit. La situation de fait amène les grandes plateformes à se propulser dans le champ de la souveraineté. Pour rattraper un certain retard, l'Union européenne mise sur la régulation concurrentielle tout en œuvrant à poser les jalons d'une éthique par la souveraineté.

Introduction

La question de la souveraineté est désormais bien installée dans le paysage numérique au point de susciter parfois une sorte de *sovereignty washing* ou d'injonction à la souveraineté. En passant de l'intention à l'action, un nouveau vocabulaire se fait jour et l'on parle désormais souvent d'autonomie stratégique. Cette évolution témoigne également de l'insertion de la notion de souveraineté numérique dans un contexte plus large, celui d'une forme de renouveau de la souveraineté. Celui-ci se manifeste dans de nombreux domaines et se traduit notamment par des actions de relocalisation de production, celle de certains médicaments par exemple. En fait de souveraineté, il est question en réalité de politique industrielle, de compétition, d'enjeux géopolitiques.

On a beaucoup fait pour la souveraineté numérique ou sous couvert de sa promotion, et tout à la fois assez peu, si l'on en croit les résultats contrastés et souvent faibles. Il n'est donc pas étonnant que se déploie un discours critique sur les orientations prises par la France et l'Union européenne. Celui-ci emprunte cependant une forme inattendue. Car c'est la place du droit lui-même qui fait désormais débat : trop de droit, pas assez, pas forcément le bon droit, un droit à l'efficacité limitée ?

Pour éclairer ce débat, nous proposons ici de présenter la souveraineté sous deux aspects, la souveraineté de fait et la souveraineté par le droit et la régulation. Bien sûr, il peut paraître paradoxal de parler de souveraineté de fait s'agissant d'une construction juridique. Cependant, il est indéniable que le numérique contribue à redéfinir les contours de la souveraineté. En effet, « un État ne saurait être souverain numériquement comme il est souverain politiquement » écrit le professeur Quiviger[1]. Lorsque le numérique paraît, on parle de souveraineté en réseau avec la multiplication des pôles de normativité, de stratégie de souveraineté, de souveraineté efficace. Qu'elle soit de fait ou fondée sur le

[1] https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseil-constitutionnel/une-approche-philosophique-du-concept-emergent-de-souverainete-numerique

droit, la souveraineté présente en tout cas deux facettes, l'une qui la projette sur le numérique, l'autre dans le champ du numérique.

La souveraineté de fait

Le marché est indéniablement l'étalon qui permet de mesurer un certain état de la souveraineté dont il est l'expression.

Le marché, expression de la souveraineté sur le numérique

Il est désormais impossible de parler de souveraineté numérique sans évoquer les formes de concurrence entre souveraineté étatique voire européenne et pouvoir des entreprises. On sait à quel point le marché du numérique est dominé par de grandes plateformes américaines. Il s'agit là d'un état de fait.

Toutefois, cette configuration du marché n'est pas le résultat d'une génération spontanée.

Sur le plan économique, l'effet réseau joue à plein et amplifie le phénomène du *winner-take-all* où le *leader* tend à acquérir une position dominante durable. C'est tout un écosystème qui est soumis de surcroît à ces plateformes. Par ailleurs, la domination américaine trouve ses racines dans la maîtrise des fondations du numérique, qui elle-même se nourrit d'une politique économique et juridique favorable à l'innovation et à l'investissement. Par fondations, nous entendons en particulier les infrastructures de réseau, le logiciel et les données.

L'asymétrie entre la situation américaine et européenne est manifeste, sans compter la Chine qui occupe désormais une place essentielle dans le monde numérique. Elle repose pour partie sur une attitude proactive là où une certaine priorité serait donnée à l'action juridique souvent défensive en Europe. On ferait pourtant un raccourci en laissant croire que la situation des États-Unis est étrangère à sa politique juridique.

Le marché, propulseur du numérique dans le champ de la souveraineté

C'est en tout cas cette configuration concurrentielle du marché qui conduit les grandes plateformes américaines à revendiquer certains attributs de la souveraineté tant il est vrai que le régalien n'est jamais très éloigné du marché. Les prétentions souveraines affichées par les grandes plateformes en témoignent, à l'instar de Google qui veut organiser les informations à l'échelle mondiale dans le but de les rendre accessibles et utiles à tous ou encore de Facebook qui veut connecter le monde entier[2].

On peut dire qu'elles détiennent les attributs de la souveraineté : un territoire transnational qui est celui de leur marché et du lieu d'édiction de normes, une population dont le système cognitif est contrôlé et l'attention captée, une langue car l'anglais prédomine, des monnaies virtuelles, une fiscalité optimisée. Mais la principale originalité vient de la maîtrise de la production/utilisation de données et de l'accès à l'information (moteurs de recherche, assistants vocaux très prescriptifs).

Le tableau serait incomplet si l'on ne mentionnait pas le fait que certaines entreprises de l'Union européenne veulent aussi se positionner en promoteurs de la souveraineté numérique par la maîtrise des briques de l'Internet, sans que le droit ne les y encourage nécessairement. On en trouve par exemple dans le domaine du logiciel (libre à plus forte raison) ou encore dans celui du *cloud*. Ces entreprises (on pourrait y ajouter les pouvoirs

[2] BLANDIN-OBERNESSER A. (2016), *Droits et souveraineté numérique en Europe*, Bruylant.

publics dans le cadre du réarmement de la filière numérique de l'État) attendent plus de volontarisme politique en la matière.

Le marché lieu de normes

Pour les grandes plateformes commerciales en tout cas, le marché devient un véritable lieu de production de normes. De normes techniques en premier lieu. Le mouvement dit de « plateformisation » en est une illustration[3]. Le modèle technique de la plateforme est en effet générique et reproductible. Vient se greffer sur cette infrastructure, un modèle d'affaires qui est consubstantiel à l'économie du numérique. Ce sont aussi des normes sociales qui sont créées, notamment sur la base de l'usage du mobile et des réseaux sociaux. Ces normes résultent d'une interaction entre un usage prescrit par les entreprises (par exemple, enfermement dans une bulle informationnelle, manipulation informationnelle) et de pratiques libératrices et créatrices des utilisateurs[4]. Plus encore, ces entreprises jouent un rôle déterminant dans la fixation de la norme, comme modèle anthropologique et civilisationnel fondé désormais sur l'accompagnement algorithmique personnel de la vie[5].

Ce sont enfin des normes juridiques qui sont créées. On peut ainsi qualifier les conditions générales d'utilisation ou encore la modération voire la régulation des contenus. Celle-ci offre un exemple éclairant des chevauchements entre souveraineté étatique et « privée ». Est-ce un hasard si Facebook a officialisé son projet de Conseil de surveillance avant le début de l'examen par l'Assemblée nationale de la proposition de loi visant à lutter contre la haine sur Internet en 2019 ? Pompeusement appelé « Cour suprême » par Mark Zuckerberg, ce Conseil est chargé de statuer sur les litiges liés à la modération des contenus par ses plateformes.

La modération des contenus par les réseaux sociaux est fondée sur des standards et procédures certes privés, mais dans un cadre juridique comprenant des obligations de faire, en l'occurrence de retrait des contenus illégaux[6]. On observe un double mouvement de mise en concurrence des normes privées avec les normes publiques et d'appropriation de normes publiques par le privé. Si à première vue, le Conseil de surveillance apparaît comme l'expression d'une aspiration souveraine, l'examen de ses premières décisions montre que celui-ci a (aussi) recours aux standards internationaux de protection des données[7].

La souveraineté par le droit

Ainsi propulsées dans le champ de la souveraineté, les entreprises rencontrent l'État et les fonctions régulatrices. Selon les termes du président de la République, « Les États-Unis ont les Gafa (Google, Amazon, Facebook et Apple), la Chine a les BATX (Baidu, Alibaba, Tencent et Xiaomi). Et l'Europe ? Nous avons le RGPD. Il est temps de ne pas dépendre uniquement des solutions américaines ou chinoises ! »[8]. Si on ne fait que du droit, « on

[3] LEROY M. (2023), *La loyauté des plateformes à l'égard des consommateurs*, Dalloz.

[4] BLANDIN A. & LEHAGRE E. (2019), « La protection de l'individu face à l'automatisation de la présentation des contenus par les plateformes », *Études digitales*, Les plateformes, 2.

[5] Voir les travaux d'Éric Sadin et notamment la conférence donnée au séminaire IMT Atlantique de Saint-Jacut-de-la-Mer (juin 2023).

[6] Règlement 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques), JOUE n°L.277 du 27/01/2022, p. 1.

[7] NDIOR V. (2022), « Le Conseil de surveillance de Facebook et la protection des libertés », RDLF, chron. n°23.

[8] Entretien donné par Emmanuel Macron au fonds Atomico, https://medium.com/atomico/french-president-emmanuel-macron-niklas-zennström-europes-technology-future-dec-2020-238d477c4a01

va se faire balader », écrit l'économiste Joëlle Toledano[9]. Si le droit est ainsi stigmatisé, c'est d'abord pour la vision défensive qu'il est supposé incarner dans ce contexte précis. C'est aussi parce qu'on lui offrirait la préséance : « Face aux informaticiens de la Silicon Valley, nous n'avions chez nous, aux manettes, que des politiques, des juristes ou des communicants [10]» écrit Tariq Krim.

La régulation concurrentielle tardive du marché

La critique vaut pour la régulation concurrentielle qui est la grande réponse européenne apportée aux problèmes identifiés, alors que les positions sur le marché sont pour beaucoup figées. Réguler le marché revient d'une certaine manière à réguler les grandes plateformes. Dans quelle mesure poursuit-on dans ce domaine des objectifs souverains ? Il y a ici une différence entre le discours et la règle de droit. Le discours est volontariste, le droit est prudent. Pas question en tout cas de stigmatiser les entreprises dont on veut réduire la puissance, fussent-elles américaines ou justement parce qu'elles le sont. Il s'agit pourtant bien de restaurer le rôle de l'État dépossédé et de faire place à des entreprises européennes.

Le règlement sur les marchés numériques (DMA en anglais) identifie une catégorie particulière de plateformes numériques qui ont vocation à être régulées de manière asymétrique. Ce sont les contrôleurs d'accès. Aux fins de leur désignation, le règlement prévoit des critères assortis d'un système de présomptions. Les critères sont l'impact significatif sur le marché intérieur, l'exploitation d'un service de plateforme essentiel, la position bien établie et durable.

Si l'objectif avait été clairement souverain, il eût fallu que la définition couvre également les manifestations de la puissance des plateformes dans le champ non économique et en particulier régalien. C'est ce que proposait par exemple l'Arcep et le Conseil national du numérique, l'enjeu étant d'appréhender la dimension systémique ou structurante des plateformes et le fait que leur action dépasse le seul champ économique. L'avenir nous dira en tout cas quelle est l'efficacité du dispositif et son concours à des évolutions qui se font parfois plus par le marché que par le droit[11].

La propulsion au-delà du marché

Une fois le marché devenu plus concurrentiel et loyal, la voie serait libre pour que se déploient les valeurs incarnées par des entreprises européennes. C'est l'objet des règles relevant de l'éthique comme traduction de valeurs dans l'action[12]. Promouvoir la souveraineté numérique pour maîtriser notre destin sur les réseaux est indéniablement un objectif digne d'être poursuivi. Encore faut-il déterminer quel sens on veut donner à cette recherche de souveraineté, faute de quoi sa définition aurait des allures de tautologie.

C'est ici que la notion de « troisième voie » numérique prend tout son intérêt (entre les États-Unis et la Chine). Il y a manifestement des valeurs européennes dans le domaine du numérique. La voie européenne repose sur des acquis et de nouvelles trajectoires. Parmi les acquis figure par exemple la recherche d'un niveau élevé de protection de certaines valeurs et de certains droits (protection des données personnelles et de la vie privée, liberté d'expression, diversité culturelle…). Au titre des trajectoires, l'enjeu est par

[9] TOLEDANO J. (15 décembre 2020), « Si l'on ne fait que du droit, on se fera balader », *L'opinion*.

[10] KRIM T. (6 février 2023), « La souveraineté est morte… Vive la résilience ! », *Le Point*.

[11] BLANDIN A., ISAAC H. & EL ANDALOUSSI M. (2020), « Concurrence et régulation des plateformes, étude de cas sur l'interopérabilité des réseaux sociaux », Avis du Conseil national du numérique, https://cnnumerique.fr/files/2020-07/ra-cnnum-concurrence-web%281%29.pdf

[12] VANDERLINDEN J.-P., « L'éthique face aux incertitudes : l'adaptation au changement climatique », https://www.youtube.com/watch?v=H2S4FDgmi3M

exemple de contrebalancer l'approche « Marché intérieur » porté par la Commission européenne par une politique industrielle ambitieuse et une politique de concurrence mieux utilisée pour défendre les intérêts européens, notamment en termes d'investissements dans les infrastructures. On place également beaucoup d'espoir dans la mise en valeur de l'intérêt général, notamment à travers la construction d'un cadre pour le partage des données. La promotion des communs est à cet égard un marqueur de la troisième voie.

Le droit face à la norme du marché

Face à la norme du marché, le droit est appelé à trouver sa place. Une première approche consiste à éviter que le droit ne se construise au détriment de l'innovation conçue comme un impératif pour la souveraineté. C'est sûrement le dispositif de protection des données personnelles avec le RGPD qui offre la meilleure illustration de la tension entre droits fondamentaux et innovation. Un certain équilibre peut être atteint par le biais du pragmatisme des responsables de traitements de données, par exemple lorsqu'ils appliquent le RGPD dans une optique de gestion des risques, plutôt que de s'y conformer en tout point.

C'est aussi une tension mise en évidence à propos de la régulation de l'intelligence artificielle. Son fervent défenseur qu'est l'entrepreneur chinois Kai Fu Lee met en garde contre une certaine frilosité européenne en la matière. Évoquant l'attachement des Européens à la protection de la vie privée, il estime qu'un équilibre doit être trouvé entre encouragement à l'innovation et encadrement de l'IA[13]. Tout récemment, c'était au tour du président de la République Emmanuel Macron lors du salon VivaTech 2023, de dire que « Innover sans réguler est une folie. Réguler sans innover ce serait comme tailler des haies que l'on n'a pas »[14].

L'innovation en elle-même ne fait pas débat dans cette approche. C'est pourquoi il est nécessaire d'envisager aussi ou alternativement le droit comme un rempart contre le modèle civilisationnel évoqué plus haut. On peut en effet regretter que certains problèmes ne soient réglés qu'à la marge. Par exemple, ce n'est pas parce que le futur règlement sur l'IA s'intéresse aux biais algorithmiques que la solution promue constitue une carte blanche pour l'avenir.

Conclusion

Il n'y aurait donc pas de souveraineté numérique possible sans choix civilisationnels issus de la délibération collective. On renoue alors avec le sens originel de la souveraineté, celle du peuple. La souveraineté numérique n'est en tout cas pas un état qu'il s'agirait de sanctuariser mais un processus au sein duquel le fait et le droit se conjuguent. L'Union européenne aspire à créer un nouvel état de fait, un nouvel état du monde numérique. La critique de la place du droit est alors nécessaire sur le fondement d'une évaluation de son efficacité[15]. La tâche est difficile car c'est un peu comme si la force symbolique du droit interdisait d'en faire la critique. Le RGPD en est l'exemple type tant il fait parfois figure de totem pour ses concepteurs et destinataires. Nombreux sont pourtant les traitements de données qui échappent à son cadre, sans que soient véritablement inquiétés les auteurs de dérives majeures dans le domaine de la sécurité des données en particulier.

[13] KAÏ-FU L. (2021), *I.A., la plus grande mutation de l'histoire*, J'ai lu.

[14] https://www.liberation.fr/economie/economie-numerique/macron-annonce-500-millions-deuros-supplementaires-pour-lia-francaise-20230614_4INTV2VMYRHIPJMIYO747IFBAE/

[15] VERGNOLLE S. (2020), *L'effectivité de la protection des personnes par le droit des données à caractère personnel*, thèse de doctorat, Université Panthéon Assas (Paris 2).

La souveraineté numérique, un instrument de politique étrangère

Par Julien NOCETTI
Chercheur, GEODE (Géopolitique de la datasphère, Université Paris 8) et IFRI

La pandémie de Covid est venue renforcer des tendances préexistantes : des interdépendances technologiques encore réelles, mais contrariées par la compétition entre les États-Unis et la Chine, et la problématique de la diversification des chaînes de valeur. La guerre en Ukraine, depuis février 2022, n'a fait qu'accélérer un mouvement global vers la prise en compte de logiques souveraines dans le champ numérique. Les États y agissent de façon naturellement différenciée en fonction de leur régime politique, suscitant des réponses et contre-réponses mêlant outils juridiques, financiers et technologiques. Instrumentalisée à des fins (géo)politiques, la souveraineté numérique est donc plus qu'une ambition industrielle – cette tendance devrait se renforcer à la faveur de la superposition des crises internationales.

Le champ numérique et, plus largement, technologique, est traversé de façon croissante par des logiques souveraines. La pandémie de Covid, la guerre en Ukraine, l'actualité juridique entre l'Union européenne (UE) et les États-Unis, mais aussi les choix d'investissements des plateformes numériques américaines et chinoises, participent à cette mise en lumière.

Dans un système international profondément travaillé par la dissémination globale des technologies numériques, certains États souhaitent s'approprier les bénéfices de l'interdépendance technologique *lato sensu* tout en protégeant leur marché intérieur. La maîtrise des interdépendances est ainsi devenue un enjeu structurant des rapports internationaux, donnant un nouveau caractère d'urgence à des logiques de défense économique et commerciale.

La souveraineté numérique, par les rivalités qu'elle suscite, est également devenue un enjeu de modèle, de projection de valeurs politiques. Dans un monde marqué par le retour d'une forme de brutalisation, dans lequel le rôle des idées n'a jamais disparu, la souveraineté numérique apparaît comme une composante clé à travers laquelle les États en opposition voire en conflit viseront à porter leur propre lecture du droit, de la technologie et de la politique.

La souveraineté numérique dans la « chaîne de valeur » diplomatique

La souveraineté numérique est devenue l'un des points de friction désormais incontournable des rapports géopolitiques. Cette caractéristique a été clairement renforcée au cours de la crise pandémique puis à travers ses multiples implications. Deux d'entre elles méritent d'être relevées.

La première a trait à la montée en puissance du facteur géoéconomique dans les relations internationales, qui dépasse le seul cadre de l'économie numérique, pour englober des pratiques d'« arsenalisation » des principales interdépendances économiques. En d'autres termes, les vecteurs de la mondialisation (flux financiers, technologiques, exportations de matières premières agricoles et énergétiques, mais aussi réseaux informationnels) sont utilisés comme des armes. Selon cette approche, les mesures économiques coercitives – comme les sanctions – ne sont plus un substitut à la guerre mais son prolongement. L'objectif est d'assécher les ressources qu'un ennemi peut mobiliser pour le combat et donc d'alourdir le fardeau de la guerre à partir de la dimension économique. Il s'agit également d'affaiblir le moral de la population adverse afin de miner sa combativité et son soutien au gouvernement. Dans ce cadre, la souveraineté numérique peut constituer une réponse politique et industrielle à une situation de contrainte imposée de l'extérieur, dans une perspective d'« autosuffisance » (terme employé par les autorités chinoises depuis 2015) ou de « substitution aux importations » (vocable utilisé par Moscou depuis 2014).

Dans le cas de la Russie, précisément, la souveraineté numérique ou technologique est depuis lors invoquée pour contourner les sanctions internationales, tout particulièrement dans l'industrie stratégique des semi-conducteurs, dans laquelle la Russie n'a pas de capacités de production propres (surtout les composants les plus sophistiqués), ni de chaîne de valeur souveraine. Le pays dépend principalement des architectures ARM pour les processeurs conçus par l'acteur national Baikal Electronics et de l'outil de production de l'entreprise taïwanaise TSMC. Toutes ces sociétés étrangères ont suivi les jeux de sanctions internationales, plaçant la Russie devant un risque de pénurie de composants, que le partenaire chinois n'est pas nécessairement enclin à prendre en charge, devant lui-même affronter les sanctions américaines visant ses approvisionnements en processeurs.

La seconde implication concerne les interactions entre les plateformes systémiques du numérique et les États. Ce sont les premières qui, pendant la crise du Covid, ont assuré les connexions entre pays, individus et organisations. Elles façonnent les rapports politiques et sociaux et sont désormais au cœur des rapports de puissance. La coopération, la compétition et la confrontation entre la Chine et les États-Unis se jouent notamment à travers elles. L'enjeu de la régulation des Gafam est de plus en plus perçu – en Europe tout particulièrement – comme celui devant permettre d'imposer une souveraineté numérique qui a longtemps fait défaut au continent. Elle se mue donc en un enjeu classique des relations internationales, susceptible, régulièrement, de déclencher des polémiques et de tendre les relations entre alliés (UE – États-Unis par exemple). Depuis 2019, l'Union européenne a fait de la taxation des Gafam l'un des axes politiques phares de sa « Commission géopolitique »[1]. Les multiples initiatives communautaires en la matière sont désormais inscrites dans une volonté de défendre la « souveraineté numérique » de l'Europe face aux stratégies technologiques et d'innovation prédatrices des écosystèmes américains et chinois.

La souveraineté numérique, un enjeu de modèles

La souveraineté numérique ne représente pas qu'un enjeu de politique intérieure ; elle concerne également la projection d'une vision, d'un modèle à l'international. En la matière, une partie des débats actuels se focalise sur l'opposition de valeurs entre l'approche défendue par les démocraties libérales et celle projetée par les États autori-

[1] COMMISSION EUROPÉENNE (2020), *État de l'union 2020. La Commission von der Leyen : bilan de la première année*, https://ec.europa.eu/info/sites/default/files/von-der-leyen-commission-one-year-on_fr.pdf.

taires[2]. Plus précisément, la ligne de fracture s'articule à un double niveau. Le premier concerne le degré d'ouverture d'écosystèmes numériques aux interdépendances globales – ou, du moins, à la capacité de ces États à maîtriser leurs dépendances critiques. Des régimes autoritaires comme la Chine, la Russie ou l'Iran visent, depuis la fin des années 1990 et à des degrés divers, à s'affranchir de leurs dépendances vis-à-vis des technologies américaines, perçues comme un moyen d'intrusion voire de subversion.

Le second a trait aux divergences d'appréciation même de l'expression de souveraineté numérique. Internet, défiant le contrôle de toute forme d'autorité, n'est pas unanimement perçu dans le monde comme devant à tout prix favoriser l'émancipation des peuples. C'est ici la couche cognitive de l'internet qui est concernée par cette approche. Distincte de la conception européenne, la souveraineté numérique telle qu'envisagée par la Russie ou la Chine met ainsi l'accent sur la préservation de l'espace informationnel « national » d'influences étrangères perçues comme subversives – tout en suivant les tendances internationales observées depuis une décennie (relocalisation des données, davantage d'importance accordée aux infrastructures numériques, etc.). Cette approche sino-russe se distingue également par un recours décomplexé au droit, mobilisé tous azimuts pour renforcer le primat du politique dans le domaine numérique et maintenir la stabilité – sinon la survie – des régimes. Dans les deux pays évoqués, la « sécuritisation » de l'espace numérique national s'est manifestée par l'emploi d'une rhétorique de la menace existentielle pour justifier des actions et des dispositions plus restrictives des libertés d'expression et de réunion. Une nouvelle fois, l'hostilité à la politique américaine – promotion de la liberté de circulation de l'information (*free flow of information*), rôle central du secteur privé, etc. – structure la ligne politique de ces États.

Cette forme d'autoritarisme numérique – intégrant une conception particulière de la souveraineté – est projetée de façon exponentielle dans les débats internationaux. D'une part, un État comme la Russie projette la notion de « souveraineté » ou de « sécurité » de l'information dans les enceintes internationales, tout particulièrement onusiennes, depuis 1998, cherchant à rallier les pays déjà américano-sceptiques à son propre positionnement[3]. Ligne de fracture dans les débats sur la gouvernance mondiale de l'Internet, la « souveraineté » est aussi exploitée par les mêmes États à des fins de politique étrangère. Ainsi, avant son interdiction dans l'Union européenne à compter de mars 2022, la chaîne d'État russe RT diffusait-elle, en France, des émissions et des articles pointant « l'absence » de souveraineté numérique en Europe, avec en contrepoint les différents scandales d'espionnage impliquant les alliés de façon à susciter des débats déjà polarisés au sujet des États-Unis.

Par-delà cette dichotomie liée à la nature des régimes, l'approche européenne se distingue, selon un nuancier complexe, par une ligne politique qui lui est désormais propre. L'absence d'acteurs numériques européens de premier plan conduit l'UE à défendre un modèle spécifique de société numérique autour de valeurs (protection des données personnelles, concurrence loyale, fiscalité suffisante…) dont la dimension défensive est parfois perçue comme une forme d'antiaméricanisme. En février 2021, Charles Michel, président du Conseil de l'UE, déclarait qu'il n'y a « pas d'autonomie stratégique sans souveraineté numérique », plaçant officiellement au cœur des débats le concept d'« autonomie stratégique », qui dénote une connotation sécuritaire voire militaire – ici appliquée à la politique numérique et aux infrastructures de données. Le curseur placé sur l'ambition d'« autonomie » suggère une lecture géopolitique devant permettre à l'UE de rivaliser avec les deux superpuissances numériques que sont la Chine et les États-Unis, tout en

[2] Voir par exemple WEBSTER G. & SHERMAN J. (2021), "The fall and rise of techno-globalism", *Foreign Affairs*, 28 octobre.

[3] NOCETTI J. (2015), "Contest and conquest: Russia and global internet governance", *International Affairs*, vol. 91, n°1, pp. 111-130.

protégeant ses propres intérêts vitaux. Cependant, les États membres ne soutiennent pas tous le développement d'une autonomie stratégique européenne ; ceux qui le font ne s'accordent ni sur ce qu'elle recouvre, ni sur le niveau d'ambition géographique et fonctionnel qu'ils devraient adopter pour la mettre en œuvre. L'attitude à adopter vis-à-vis des États-Unis est au cœur des discussions sur l'autonomie stratégique européenne et constitue l'un des points de crispation quant aux risques qu'elle pourrait faire peser sur les relations transatlantiques, particulièrement en matière de défense.

Souveraineté versus interdépendances : l'exemple de la 5G

Pour les Européens, les débats sur la 5G sont venus questionner l'équilibre et l'avenir du rapport entre les interdépendances globales et les ambitions formulées de souveraineté ou d'autonomie stratégique en matière technologique. À cet égard, souveraineté numérique et souveraineté technologique sont souvent mêlées à propos de la 5G. Si la souveraineté numérique associe une longue liste de craintes (perte de contrôle des données, risques en matière de cybersécurité, rivalité numérique dans l'offre de services publics, menaces sur les libertés publiques et les valeurs démocratiques), la seconde recouvre la première mais se réfère plus globalement à la perte d'indépendance de l'Europe sur des technologies clés pour des secteurs stratégiques, comme l'industrie de défense et les infrastructures de télécommunications, ou pour l'avenir comme l'intelligence artificielle et l'Internet des objets (IoT).

Traditionnellement, deux lectures s'opposent lorsque la « souveraineté » de l'Europe est convoquée en matière technologique. Une première considère l'Europe « vassalisée », car dépourvue de capacité d'autonomie politique et économique sur ce plan. Une seconde avance, quant à elle, une croyance dans la capacité d'action de l'Europe dans le numérique et les technologies critiques, du fait de la formation d'une expertise scientifique de haut niveau et de la singularité d'un modèle de gouvernance fondé sur les valeurs européennes[4]. Ces deux lectures ne sont en réalité pas opposables : l'Union européenne sait tirer profit de son excellence technologique mais bute sur l'impensé géopolitique de son projet politique, qui se reflète parfois crûment dans le jeu technologique international.

Avec la 5G, l'évolution la plus notable concerne la question chinoise. Auparavant limitée à l'expansion des Gafam américains, l'ambition de souveraineté numérique de l'Europe est désormais décentrée des seuls États-Unis pour aussi englober la Chine. Cette donnée alimente un certain nombre de défis pour l'Union européenne et interroge autant son rapport à la mondialisation économique, centrée autour de la capacité productive de la Chine, que la nature « géopolitique » de la Commission telle qu'avancée dès son installation en décembre 2019 – soit en pleine phase de tensions transatlantiques. Ainsi, pour l'Europe, le dossier de la 5G témoigne jusqu'à présent de son absence de cohésion dans son rapport à la Chine de Xi Jinping. Diversement appréciée sur le continent, la compétition sino-américaine illustre pleinement la difficulté pour les Européens de déterminer leur positionnement commercial et stratégique par rapport à la Chine – et aux États-Unis – alors que s'affirme un « nationalisme technologique » que Pékin viserait à exporter[5].

[4] NOCETTI J. (2021), « L'Europe reste-t-elle une colonie numérique des États-Unis ? », *Politique étrangère*, n°3, pp. 51-63.

[5] INKSTER N., *The great decoupling*: *China, America, and the struggle for technological supremacy*, Londres, Hurst, pp. 193-254. Pour une lecture du techno-nationalisme opposant les modèles politiques, voir WEBSTER G. & SHERMAN J. (2021), "The fall and rise of techno-globalism", *Foreign Affairs*, 28 octobre 2021.

La capacité de l'Union européenne à agir dans la sphère technologique, souvent reléguée au second plan dans les débats, pourrait être l'alpha et l'oméga d'une stratégie « en mouvement » du Vieux continent en matière de 5G. C'est une perspective qui semble se dessiner chez l'exécutif européen qui, en identifiant ses dépendances critiques dans des secteurs jugés stratégiques pour l'Europe, cherche à élaborer des mesures pour protéger les intérêts européens. En d'autres termes, la « souveraineté technologique » de l'UE serait mieux défendue en évaluant finement les dépendances critiques des États membres avant d'y répondre de façon ciblée tout en conservant une ouverture au monde[6] plutôt qu'en adoptant une approche classique de la souveraineté, qui masque les logiques d'interdépendances qui restent les marqueurs de notre époque[7].

Contrer la « fragmentation »

À l'échelle internationale, les logiques souveraines sont de longue date débattues sous l'effet supposé de celles-ci sur l'Internet voire le spectre complet du numérique et des technologies dites émergentes (intelligence artificielle, 5G, etc.). Une partie des débats place une emphase particulière sur le terme de « fragmentation », qui décrirait l'émiettement en cours du réseau global sous l'effet de politiques « souveraines », c'est-à-dire en contradiction avec la nature « globale, ouverte et interopérable » de l'internet des pères fondateurs. Il s'agit principalement de l'approche américaine, qui resitue l'enjeu dans une stratégie diplomatique visant à empêcher le morcellement de nos univers numériques à des fins politiques et commerciales[8].

Cette « fragmentation » est parfois débattue à travers l'idée d'une sécession de certaines parties de nos réseaux. La « balkanisation », terme à la connotation négative, a été pour la première fois abordée dans une étude du MIT de 1997, laquelle prévenait que la croissance d'une infrastructure globale de communication ne conduirait pas nécessairement à l'émergence d'un « village global de l'internet » – elle pourrait aussi fragmenter les sociétés et « balkaniser » les interactions dans l'espace numérique[9]. Le « Splinternet », lui, désigne le fait d'avoir, en lieu et place d'un seul réseau mondial, des îlots numériques distincts, sans interopérabilité. Cela signifie que ces réseaux ne se parlent pas les uns les autres, voire même qu'ils opèrent sur des technologies différentes et incompatibles. Loin d'être accessoire, l'enjeu a pris un caractère géopolitique, la guerre en Ukraine ayant réveillé le spectre d'une fragmentation élargie. La Chine n'a pas le monopole de la fermeture de son réseau ; la Russie, elle, a renforcé son contrôle depuis l'invasion et bloque les grandes plateformes numériques. Dans ces cas précis comme ailleurs, la ligne de défense reste bâtie autour de la notion de souveraineté…

[6] FIOTT D. & THEODOSOPOULOS V. (2020), "Sovereignty over supply? The EU's ability to manage critical dependencies while engaging with the world", EUISS, Brief, n°21, décembre 2020.

[7] Sur le sujet, voir HÉRAULT P. (2021), « Comment renforcer la souveraineté à l'heure des chaînes de valeur mondiales ? », Études de l'Ifri, décembre.

[8] Voir Confronting reality in cyberspace: Foreign policy for a fragmented internet, Independent task force report n°80, Council on Foreign Relations, 2022.

[9] VAN ALSTYNE M. & BRYNJOLFSSON E. (1997), "Electronic communities: Global village or cyber Balkans?", Massachusetts Institute of Technology, mars.

Bibliographie

COMMISSION EUROPÉENNE (2020), *État de l'union 2020. La Commission von der Leyen : bilan de la première année*, https://ec.europa.eu/info/sites/default/files/von-der-leyen-commission-one-year-on_fr.pdf

COUNCIL ON FOREIGN RELATIONS (2022), "Confronting reality in cyberspace: Foreign policy for a fragmented internet", Independent task force report n°80, Council on Foreign Relations, https://www.cfr.org/task-force-report/confronting-reality-in-cyberspace/download/pdf/2022-07/CFR_TFR80_Cyberspace_Full_SinglePages_06212022_Final.pdf

FIOTT D. & THEODOSOPOULOS V. (2020), "Sovereignty over supply? The EU's ability to manage critical dependencies while engaging with the world", EUISS, Brief n°21, décembre, www.iss.europa.eu

HERAULT P. (2021), « Comment renforcer la souveraineté à l'heure des chaînes de valeur mondiales ? », Études de l'Ifri, décembre, www.ifri.org

INKSTER N. (2021), *The great decoupling: China, America, and the struggle for technological supremacy*, Londres, Hurst.

NOCETTI J. (2015), "Contest and conquest: Russia and global internet governance", *International Affairs*, vol. 91, n°1, pp. 111-130.

NOCETTI J. (2021), « L'Europe reste-t-elle une colonie numérique des États-Unis ? », *Politique étrangère*, n°3, pp. 51-63.

VAN ALSTYNE M. & BRYNJOLFSSON E. (1997), "Electronic communities: Global village or cyber Balkans?", Massachusetts Institute of Technology, mars, https://web.mit.edu/marshall/www/papers/CyberBalkans.pdf

WEBSTER G. & SHERMAN J. (2021), The fall and rise of techno-globalism, *Foreign Affairs*, 28 octobre, https://www.foreignaffairs.com/articles/world/2021-10-28/fall-and-rise-techno-globalism

L'avenir incertain des flux de données transatlantiques

Par Florence G'SELL
Professeure de droit privé à l'Université de Lorraine, titulaire de la chaire Digital, Gouvernance et Souveraineté à Sciences Po Paris, Professeure invitée à l'Université de Stanford (Cyber Policy Center)

La légalité des transferts de données entre l'Union européenne et les États-Unis constitue une problématique de longue date compte tenu des approches très différentes de la protection de données personnelles de part et d'autre de l'Atlantique. Les accords permettant d'encadrer et légaliser les flux de données transatlantiques – *Safe Harbor*, puis *Privacy Shield* – ont été successivement annulés. Le nouveau mécanisme mis en place, le récent *Data Privacy Framework*, est d'ores et déjà contesté, ce qui laisse planer une réelle incertitude sur la possibilité, pour les entreprises, de transférer effectivement des données aux États-Unis.

Bien qu'essentiels à tous les secteurs de l'économie, les flux de données entre l'Europe et les États-Unis se font aujourd'hui dans une grande insécurité juridique, alors même que les grandes entreprises technologiques américaines implantées en Europe transfèrent massivement les données des utilisateurs européens vers les États-Unis. Originellement, toutefois, la protection des données n'était pas exclusivement une préoccupation européenne. Dès 1973, un rapport du ministère fédéral de la Santé, de l'éducation et du bien-être américain avait énoncé des principes en matière de collecte des données personnelles[1], qui ont ensuite été publiés, sous forme de lignes directrices, par l'OCDE en 1980[2] et eu une grande influence internationale.

Il reste que c'est en Europe que les premiers cadres contraignants ont été imposés avec l'adoption des lois allemandes[3] et françaises[4], puis la conclusion, sous l'égide du Conseil de l'Europe, de la Convention sur la protection des données, également connue sous le nom de Convention 108, qui a fourni une première définition de la notion de « donnée personnelle » comme « toute information concernant une personne physique identifiée ou identifiable ». L'adoption, en 1995, de la directive 95/46/CE relative à la protection des données a permis à l'Union européenne de se doter d'un cadre global de protection des données personnelles et d'encadrer les transferts de données en direction des pays tiers.

Dans le même temps, les États-Unis n'ont pas adopté de règlementation d'ensemble destinée à garantir une protection effective des données personnelles. À partir du début

[1] "Records, computers and the rights of citizens", report of the Secretary's advisory committee on automated personal data systems, US Department of Health, Education & Welfare, July 1973.

[2] Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel, adoptées le 23 septembre 1980.

[3] Loi du 21 janvier 1977 portant protection contre l'emploi abusif de données d'identification personnelle dans le cadre du traitement des données.

[4] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

des années 2000 et de l'adoption du *Patriot Act*[5], des programmes de surveillance ont été mis en place qui ont consisté à permettre aux agences de renseignement américaines de collecter en masse les informations circulant sur les réseaux. Dans un tel contexte, les garanties très sommaires offertes aux citoyens américains en matière de protection des données personnelles sont très insuffisantes aux yeux des Européens, alors même que les entreprises établies aux États-Unis y transfèrent massivement les données collectées en Europe.

Dans ce cadre, les autorités américaines et européennes ont tenté de pallier le décalage entre les approches européennes et américaines en se mettant d'accord sur des cadres permettant de faire en sorte que les transferts se font dans des conditions jugées satisfaisantes par les européens. Plusieurs mécanismes se sont succédés : la « sphère de sécurité » (*Safe Harbor*), le « bouclier de protection des données » (*Privacy Shield*), et désormais le *Data Privacy Framework* qui vient d'être adopté.

Le *Safe Harbor*, première tentative d'encadrement des flux de données transatlantiques

Dès 1990, la Commission européenne, craignant que la disparité des législations nationales nuise au marché intérieur, a proposé un texte relatif à la protection des données personnelles qui est devenu, en 1995, la directive 95/46/CE relative à la protection des données[6]. L'article 25 de cette directive prévoyait, en particulier, que les données à caractère personnel ne pouvaient être transférées vers un pays extérieur à l'UE que si ce pays assurait un niveau de protection « adéquat », c'est-à-dire équivalent à la protection garantie par le droit de l'Union.

La directive de 1995 a habilité la Commission à constater que certains pays tiers garantissent un niveau de protection adéquat du fait de leur législation ou de leurs engagements internationaux. Ces décisions d'adéquation s'imposent aux États membres et permettent de transférer légalement les données en direction des pays concernés. En revanche, lorsqu'aucune décision d'adéquation n'a été adoptée à propos du pays destinataire, les entreprises souhaitant y exporter des données personnelles doivent garantir par contrat qu'elles sont elles-mêmes en mesure de fournir un niveau de protection adéquat. C'est ainsi qu'a été consacré l'usage de « clauses contractuelles types », qui sont des clauses standards préapprouvées par les autorités qui permettent aux exportateurs de données de transférer celles-ci vers des pays pour lesquels aucune décision d'adéquation n'a été adoptée. Des clauses contractuelles types sont ainsi publiées par la Commission européenne et reprises par les entreprises qui le souhaitent.

S'agissant des États-Unis, le caractère adéquat de la législation américaine, peu protectrice des données personnelles, n'allait pas de soi. Les États-Unis et l'Union européenne se sont alors mis d'accord sur un mécanisme devant permettre aux entreprises américaines d'offrir un niveau de protection adéquat. En 2000, le Département du Commerce américain a publié sept *Safe Harbor Privacy Principles* que les entreprises devaient s'engager à respecter si elles voulaient pouvoir transférer des données depuis l'Europe vers les États-Unis. Ces entreprises devaient certifier chaque année, dans une lettre adressée au Department of Commerce, qu'elles adhéraient à ces principes, dont le respect effectif devait être contrôlé par la Federal Trade Commission. Le caractère « adéquat » de la protection ainsi

[5] Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA Patriot Act) of 2001.

[6] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, Journal officiel n°L 281 du 23/11/1995, pp. 31-50.

offerte fut reconnu par la Commission européenne dans une décision d'adéquation du 26 juillet 2000[7], qui fondait juridiquement les transferts de données personnelles vers les États-Unis. Plus de 5 000 entreprises ont ainsi adhéré au *Safe Harbor*.

Cet accord n'a toutefois pas résisté au scandale provoqué par les révélations d'Edward Snowden qui a, en 2013, divulgué au grand public l'existence de programmes de surveillance de masse menés par les autorités américaines[8]. La section 702 du *Foreign Intelligence Surveillance Act* (FISA) permet, en effet, aux services de renseignement américains de procéder à une surveillance ciblée de personnes étrangères situées en dehors des États-Unis en contraignant les fournisseurs américains de services de communication électronique à leur communiquer des données[9]. Il leur suffit simplement d'obtenir annuellement l'autorisation de principe d'une juridiction spéciale, la Foreign Intelligence Surveillance Court (FISC), qui approuve les programmes de surveillance de manière globale mais n'est pas consultée sur la détermination des personnes ciblées. Par ailleurs, l'*Executive Order* 12333, adopté en 1980, autorise les activités de surveillance menées hors des États-Unis et autorise notamment la « collecte en vrac » des données sans aucun contrôle judiciaire, ce qui permet l'acquisition de quantités massives de données. Dans ce cadre, les informations divulguées par Edward Snowden ont permis de montrer que la National Security Agency (NSA) avait obtenu un accès quasi illimité aux données collectées par des grandes entreprises technologiques américaines, notamment dans le cadre d'un programme appelé PRISM. Ironie du sort, les entreprises impliquées dans PRISM participaient toutes également au *Safe Harbor*.

Dans la foulée de ces révélations, la Commission européenne a publié, le 27 novembre 2013, treize recommandations destinées à améliorer le fonctionnement du *Safe Harbor*[10]. Au même moment, Maximilian Schrems, un étudiant en droit autrichien utilisateur de Facebook, déposait plainte contre Facebook auprès de l'autorité de protection des données irlandaise pour avoir massivement transféré ses données personnelles vers les États-Unis tout en participant au programme PRISM. Saisie d'une question préjudicielle par les juridictions irlandaises, la Cour de justice de l'Union européenne a invalidé, le 6 octobre 2015, la décision d'adéquation relative au *Safe Harbor*[11]. La CJUE a jugé que la Commission européenne aurait dû davantage examiner les lois et les engagements internationaux des États-Unis avant d'adopter la décision d'adéquation. Elle a par ailleurs estimé que l'accès généralisé, par les services de renseignement américains, aux données des utilisateurs et l'absence de recours efficaces contre cet accès compromettait l'essence du droit fondamental au respect de la vie privée, tel qu'il est garanti par l'article 7 de la Charte des droits fondamentaux de l'Union européenne.

L'intermède du *Privacy Shield*

À la suite de l'invalidation du *Safe Harbor*, les autorités européennes et américaines se sont rapidement mises d'accord sur un nouveau mécanisme appelé « bouclier de la

[7] Décision 2000/520/CE : Décision de la Commission du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité », Journal officiel n°L 215 du 25/08/2000 pp. 7-47.

[8] "NSA Files: Decoded", *The Guardian*, November 1, 2013.

[9] G'SELL F., « Quel avenir pour les transferts transatlantiques de données après la sanction de Meta par l'autorité de protection des données irlandaise ? », Blog de la Chaire Digital, Gouvernance et Souveraineté, Sciences Po, 1er juin 2023.

[10] Recommandation de la Commission du 27 novembre 2013 relative à des garanties procédurales en faveur des personnes vulnérables soupçonnées ou poursuivies dans le cadre des procédures pénales, Journal Officiel n°C 378/8 du 24/12/2013, pp. 8-10.

[11] CJUE 6 octobre 2015, affaire C-362/14.

protection des données » (*Privacy Shield*). Dès le 12 juillet 2016, la Commission européenne a adopté une nouvelle décision d'adéquation[12] justifiée par les nouvelles garanties fournies dans le cadre du *Privacy Shield*. Les autorités américaines se sont, en particulier, engagées à s'abstenir de pratiquer une surveillance de masse et indiscriminée sur les données transférées aux États-Unis. Il a également été convenu qu'un médiateur (*ombudsman*) indépendant des autorités américaines traiterait des recours formés par les européens dont les données personnelles sont transférées aux États-Unis.

Pendant que la Commission européenne et les autorités américaines négociaient le *Privacy Shield*, les instances européennes rédigeaient le Règlement général sur la protection des données (RGPD), qui a été définitivement adopté en 2016 pour une entrée en vigueur le 25 mai 2018[13]. Le RGPD a renforcé et uniformisé les principes de protection des données personnelles figurant dans la directive de 1995. Comme celle-ci, il prévoit que les transferts de données vers des pays extérieurs à l'UE ne sont possibles que si ces transferts sont fondés sur une décision d'adéquation adoptée par la Commission ou, à défaut, lorsque les entreprises se livrant aux transferts offrent des garanties appropriées, par exemple grâce à des clauses contractuelles types (article 46). Il faut, en ce cas, que les personnes concernées disposent de droits opposables et de voies de recours effectives. C'est sur ce point que le contentieux relatif aux transferts de données réalisés par Facebook (devenu Meta) s'est poursuivi, Max Schrems ayant maintenu son opposition au transfert de ses données après l'invalidation du *Safe Harbor*. Selon Schrems, les clauses contractuelles types, qui ne sont pas contraignantes pour les services de renseignement américains, ne peuvent constituer une base juridique valable pour les transferts vers les États-Unis.

C'est dans le cadre de ce contentieux que le 16 juillet 2020, la Cour de justice de l'Union européenne a invalidé la décision d'adéquation relative au *Privacy Shield*[14]. La Cour a, en effet, rappelé que la législation des États-Unis, en ce qu'elle permet largement l'accès des services de renseignement américains aux données personnelles n'offre pas de garanties suffisantes aux européens dont les données sont transférées. Elle a, en outre, jugé que les mesures prévues par le *Privacy Shield* n'étaient pas suffisantes, notamment dans la mesure où elles ne garantissaient pas un droit de recours effectif aux citoyens européens. Elle a, enfin, confirmé que les clauses contractuelles types peuvent offrir un fondement juridique approprié aux transferts des données hors de l'Union, en précisant que les responsables de traitement et les autorités de protection des données doivent suspendre ou interdire les transferts de données en cas de conflit entre les obligations prévues par ces clauses et les législations des pays destinataires des données. C'est donc principalement sur le fondement de clauses contractuelles types que les transferts de données vers les États-Unis ont été réalisés depuis la décision du 16 juillet 2020.

Vers un nouveau cadre de transferts des données ? Le *Data Privacy Framework*

Au printemps 2022, l'Union européenne et les États-Unis ont conclu un nouvel accord politique en vue de mettre sur pied un nouveau mécanisme permettant de faciliter les transferts des données outre-Atlantique. Dans ce cadre, les États-Unis se sont engagés à faire en sorte que les activités des services de renseignement soient « nécessaires et

[12] Décision d'exécution de la Commission 2016/1250 du 12 juillet 2016 relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis, Journal Officiel 2016, L 207, p. 1).

[13] Règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, Journal Officiel 2016, L 119, p. 1.

[14] CJUE, 16 juillet 2020, affaire C-311/18.

proportionnées », deux garanties auxquelles les Européens sont attachés. Ils se sont également engagés à créer une autorité indépendante chargée d'encadrer et contrôler la manière dont les données sont collectées et traitées aux États-Unis, et notamment par les services de renseignement américains.

Dans la foulée de cet accord, le Président américain Joe Biden a signé, le 7 octobre 2022, le décret présidentiel (*Executive Order*) on *Enhancing Safeguards for United States Signals Intelligence Activities* (EO 14086) destiné à mieux encadrer les activités de surveillance. Le texte prévoit que les autorités ne peuvent collecter des données que pour un objectif de sécurité nationale, lorsque cela est nécessaire en vue d'un objectif expressément défini et seulement d'une manière proportionnée à cette priorité. Les exigences de « nécessité » et de « proportionnalité » sont explicitement mentionnées dans le texte. Les services de renseignement devront, dans ce cadre, modifier leurs procédures afin de respecter les nouvelles garanties, sous le contrôle d'un nouveau Conseil de surveillance de la vie privée et des libertés civiles qui réalisera un audit annuel de ces procédures.

Par ailleurs, le décret prévoit un mécanisme de recours au profit des personnes concernées devant le responsable de la protection des libertés civiles du bureau du directeur du renseignement national (Civil Liberties Protection Officer). Les décisions du CLPO pourront elles-mêmes être contestées devant une nouvelle Cour de contrôle de la protection des données (Data Protection Review Court). Toutes les décisions prises par ces autorités seront contraignantes pour les services de renseignement. Destinées à répondre aux préoccupations européennes, ces possibilités de recours constituent la seule véritable nouveauté du *Data Privacy Framework*. Il faut toutefois souligner que ce droit au recours n'est offert qu'aux citoyens des pays désignés comme « États éligibles » par l'*attorney general* des États-Unis. Celui-ci doit donc décider si la législation des pays concernés en matière de collecte de données et de surveillance respecte suffisamment le droit à la vie privée des citoyens américains. Le 30 juin 2023, Merrick Garlan, *attorney general* des États-Unis, a désigné l'Union européenne ainsi que l'Islande, la Norvège et le Liechtenstein (l'Espace Économique Européen) comme États éligibles à ce titre.

Par ailleurs, dans la foulée de la publication de l'*Executive Order* 14086, la Commission européenne a publié, le 13 décembre 2022, un projet de décision d'adéquation prenant en considération les garanties supplémentaires désormais accordées. Comme cela avait été le cas lors de la publication du projet de *Privacy Shield*, ce projet de décision d'adéquation a fait immédiatement l'objet de critiques. En particulier, le Comité européen de protection des données (CEPD), composé de représentants de l'ensemble des autorités nationales de protection des données, a rendu, le 28 février 2023, un avis réservé[15]. Certes, le CEPD relève les améliorations substantielles apportées par le nouveau cadre. Cependant, il estime souhaitable de clarifier un certain nombre de dispositions relatives, par exemple, à la conservation des données. Le CEPD regrette, en outre, que la collecte de masse ne soit pas soumise à l'exigence d'une autorisation préalable par un organe indépendant. Le CEPD insiste, par ailleurs, sur le fait que la procédure d'autorisation fondée sur la section 702 FISA n'est en rien modifiée dans le nouveau mécanisme : la FIS Court ne fait qu'autoriser globalement les programmes de surveillance sans être sollicitée sur la détermination des cibles, ce dont il découle qu'il n'y a pas de véritable contrôle effectif des programmes de surveillance par une autorité judiciaire indépendante. D'ailleurs, la section 702 du *Foreign Intelligence Surveillance Act* (Fisa), qui doit expirer au 31 décembre 2023, devrait probablement être reconduite par le Congrès sans modification, ce qui est, du reste, le souhait de l'administration Biden. Enfin, si la création de la nouvelle Data Protection Review Court (DPRC) est bienvenue, les conditions de sa saisine doivent, selon le CEPD, être clarifiées, notamment la condition selon laquelle le demandeur doit démontrer que ses droits ont été atteints (*adversely affected*).

[15] CEPD, Avis n°5/2023, 28 février 2023.

De son côté, le Parlement européen s'est prononcé, le 11 mai 2023, dans une résolution adoptée en séance plénière, qui conclut que le nouveau cadre de protection des données UE-États-Unis ne crée pas d'équivalence substantielle du niveau de protection et invite la Commission à poursuivre les négociations. Le texte relève, entre autres choses, que la collecte en masse de données personnelles est toujours permise dans certains cas et n'est pas soumise à une autorisation préalable indépendante. La résolution souligne également que la nouvelle DPRC rendra des décisions confidentielles, que les juges de la cour pourront être révoqués par le président des États-Unis, et que celui-ci pourra également annuler ses décisions, de sorte que la Cour n'est pas vraiment indépendante. Si la résolution du Parlement ne lie pas la Commission européenne, elle est toutefois importante politiquement.

Le 10 juillet 2023, la Commission européenne a adopté définitivement la décision d'adéquation relative au *Data Privacy Framework* (DPF)[16] après avoir constaté que les garanties prévues par l'Executive Order 14086 et la *Data Privacy Framework* UE-États-Unis offrent un niveau de protection adéquat pour les données à caractère personnel transférées depuis l'Union européenne. La décision détaille notamment les recours désormais possibles dans le nouveau cadre. Elle souligne également le nouveau système de certification prévu par le DPF, aux termes duquel les entreprises souhaitant transférer les données devront s'engager à respecter un certain nombre de principes établis par le Department of Commerce américain, et obtenir, sur cette base une certification qui pourra être retirée en cas de violation des règles du DPF.

Il était temps que le nouveau cadre entre en vigueur. Depuis l'invalidation du *Privacy Shield* le 16 juillet 2020, les transferts transatlantiques de données étaient majoritairement fondés sur des clauses contractuelles types, ce qui posait des difficultés de plus en plus insurmontables. Le 12 mai 2023, la Data Protection Commission irlandaise[17] a lourdement sanctionné Meta, à la demande du Comité Européen de Protection des Données, en condamnant l'entreprise à payer une amende de 1,2 milliard et à cesser à brève échéance de transférer des données aux États-Unis[18]. En l'état, ont dit les autorités européennes de protection des données, la législation américaine est telle qu'il n'est pas possible de garantir une protection adéquate avec des clauses contractuelles types. La nouvelle décision d'adéquation ne va toutefois apporter qu'une sécurité juridique relative aux entreprises se livrant à des transferts transatlantiques de données. La décision pourrait fort bien, en effet, faire l'objet d'une nouvelle décision d'invalidation, Max Schrems ayant d'ores et déjà annoncé vouloir contester le nouveau cadre. L'enjeu est de taille. À défaut d'un cadre juridique suffisamment sûr, les entreprises concernées pourraient être tentées de renoncer à transférer les données aux États-Unis pour les traiter exclusivement sur des serveurs situés en Europe. Une telle logique de localisation des données pourrait cependant avoir pour conséquence de rendre plus difficile le développement et le partage, en Europe, d'applications sophistiqués et ambitieuses. Il faut donc espérer que, malgré les critiques, le nouveau *Data Privacy Framework* puisse enfin aboutir à ce que les flux de données se fassent en toute sécurité et dans le respect des droits des personnes concernées.

[16] Commission implementing decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework C(2023) 4745 final.

[17] Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act 2018 and Articles 60 and 65 of the General Data Protection Regulation.

[18] G'SELL F. (2023), « Quel avenir pour les transferts transatlantiques de données après la sanction de Meta par l'autorité de protection des données irlandaise ? », Blog de la Chaire Digital, Gouvernance et Souveraineté, Sciences Po, 1er juin.

Confiance numérique ou autonomie, il faut choisir

Par Jean-Paul SMETS
Fondateur de l'éditeur de logiciels libres Nexedi

Le numérique de confiance, le rôle exorbitant de l'Agence nationale de sécurité des systèmes d'information et l'inflation réglementaire européenne créent des conditions de marché défavorables aux nombreuses technologies européennes du numérique et aux logiciels libres. Ils accélèrent ensemble l'adoption en France de technologies américaines de *cloud* non immunes à des accès non autorisés par un État tiers. Ils augmentent le risque de panne générale en favorisant des offres de *cloud* centralisées peu résilientes. En matière de gestion du risque cyber, la notion de « transparence » offre une alternative à la « confiance » pour renforcer l'autonomie industrielle européenne dans le numérique sur une base technologique résiliente et immune à un accès non autorisé par un État tiers.

Lancée le 17 mai 2021 par Bruno Le Maire, la Stratégie nationale du *cloud*[1] introduit « le *cloud* de confiance » avec pour objectifs « la protection maximale des données (…), l'accès aux meilleurs services mondiaux (...) et la cohérence avec les initiatives européennes » comme Gaia-X. Elle postule que « les meilleures entreprises de services mondiaux (...) sont américaines. » et annonce que « Microsoft ou Google, pourraient licencier tout ou partie de leur technologie à des entreprises françaises ». Deux ans après cette annonce, nos données hébergées sur des *clouds* américains ne sont pas protégées, que ce soit chez les grands opérateurs de santé comme Doctolib[2] qui subit des fuites de données sensibles ou avec le *Health Data Hub*[3] qui poursuit son activité en violation du Règlement général pour la protection des données (RGPD)[4]. Des technologies de *cloud* de Google et de Microsoft ont été acquises sous licence par des entreprises françaises mais ne sont toujours pas commercialisées[5]. L'adoption des services américains de *cloud* s'est accélérée[6] et notre dépendance technologique accrue. L'accès des technologies européennes de *cloud* aux marchés publics français a été entravé. L'innovation européenne dans le *cloud* a parfois été freinée. Le logiciel libre européen a été discriminé. Et l'on charge désormais un comité stratégique de filière d'appliquer la notion de « confiance numérique » à l'intelligence arti-

[1] LE MAIRE B. (2021), « Déclaration de M. Bruno Le Maire, ministre de l'économie, des finances et de la relance, sur la stratégie nationale du *cloud* », mai, Paris, France.

[2] JONNIAUX A. (2023), « Doctolib perd des milliers de données médicales sensibles », *Journal du Geek*, 5 mai.

[3] VITARD A. (2022), « Microsoft restera l'hébergeur du *Health Data Hub* jusqu'en 2025 », *L'usine digitale*, 13 septembre.

[4] CNIL (2020), « Le Conseil d'État demande au *Health Data Hub* des garanties supplémentaires pour limiter le risque de transfert vers les États-Unis », octobre, Paris, France.

[5] THALES (2022), « Thales présente S3NS en partenariat avec Google *cloud* et dévoile son offre de transition vers le *cloud* de confiance », juin, Paris, France.

[6] FOUILLAND F. & GALAS G. (2022), « Souveraineté numérique – La guerre du *cloud* doit avoir lieu », Soutenance finale à l'école des mines de Paris, juin, Paris, France.

ficielle, au logiciel, aux technologies immersives et au quantique[7] avec comme probable résultat une perte d'autonomie généralisée si les effets de la « confiance » y sont les mêmes que dans le *cloud*.

Nous allons illustrer sur le cas du *cloud* les mécanismes qui conduisent une politique publique de « confiance numérique » à engendrer une perte d'autonomie. Nous proposerons ensuite la notion de « transparence » comme une alternative à la « confiance » dépourvue de ses effets délétères sur l'autonomie.

Le *cloud* « made in USA » privilégié au nom de la confiance

L'Europe a créé plus de 300 technologies de *cloud* qui ont fait leurs preuves avec plus de 1 200 références ou études de cas identifiées par le fonds de dotation du libre[8]. On y trouve des technologies d'infrastructure (IaaS), des technologies pour accélérer le travail des équipes de développement de logiciels (PaaS) et des services destinés aux utilisateurs finaux (SaaS). Environ 15 % des entreprises à l'origine de ces technologies ont pour clients de grands opérateurs de *cloud* américains qui en ont équipé leur infrastructure. Ainsi, le service de base de données sur le *cloud* d'Amazon Web Services (AWS) s'appuie sur la base de données suédo-finlandaise MariaDB et sur le logiciel autrichien de stockage hautes performances Linbit[9]. On trouve dans cette liste de nombreux autres fournisseurs européens de technologies d'infrastructure de *cloud*, matériel comme logiciel.

Le 31 mai 2023, la Première ministre annonçait une actualisation de la doctrine d'utilisation du *cloud* par l'État visant à préciser la notion de données sensibles[10]. Il est ainsi rappelé l'obligation, depuis une précédente circulaire du 5 juillet 2021 en matière d'achat public de *cloud* commercial, d'assurer « l'hébergement des données d'une sensibilité particulière par des solutions disposant de la qualification SecNumCloud délivrée par l'Agence nationale de sécurité des systèmes d'information ». La nouvelle circulaire précise les conditions d'application en exigeant de la solution retenue qu'elle soit « immunisée au droit extracommunautaire » et « immunisée contre tout accès non autorisé par des autorités publiques d'État tiers ».

Elle définit par ailleurs les données sensibles comme celles « dont la violation est susceptible d'engendrer une atteinte à l'ordre public, à la sécurité publique, à la santé et la vie des personnes ou à la protection de la propriété intellectuelle » ainsi que celles comportant des « secrets protégés par la loi, notamment au titre des articles L.311-5 et L.311-6 ». Cette définition comprenant à la fois « le secret de la vie privée » et le « le secret des affaires », son champ d'application est potentiellement large et peut inciter les services de l'État à considérer toutes leurs données comme sensibles, comme lors d'un appel d'offres

[7] POLLET M. (2022), « Numérique de confiance : les premiers pas du nouveau comité stratégique de filière », *L'usine digitale*, 22 novembre.

[8] FRANCK S. (2022), "Cloudrepo.eu – A directory of European cloud technologies [vidéo]", Euclidia NOW! Towards a resilient cloud infrastructure in Europe, 29 septembre, Bruxelles, Belgique, repéré à https://www.euclidia.eu/news/euclidia-Website.Euclidia.Now.Brussels

[9] FRANCK S. (2022), "Linbit: high performance storage architecture [vidéo]", Euclidia NOW! Towards a resilient cloud infrastructure in Europe, 29 septembre, Bruxelles, Belgique, repéré à https://www.euclidia.eu/news/euclidia-Website.Euclidia.Now.Brussels

[10] BORNE E. (2023), « Actualisation de la doctrine d'utilisation de l'informatique en nuage par l'État (*cloud* au centre) », 31 mai, Paris, France.

pour l'hébergement des sites Web d'information du gouvernement ouvert uniquement aux solutions qualifiées « SecNumCloud »[11].

Pour les projets existants, la circulaire précise qu'une « dérogation (…) pourra être accordée (…) sans qu'elle ne puisse aller au-delà de douze mois après la date à laquelle une offre de *cloud* acceptable (…) sera disponible en France. ». En l'absence d'offre jugée « acceptable », ce qui ne signifie pas qu'il n'existe pas de solutions fonctionnelles, la dérogation est de durée indéfinie comme pour le *Health Data Hub*[12].

Nous avons donc consulté, sur le site de l'Agence nationale de sécurité des systèmes d'information, la liste des solutions d'infrastructure (IaaS) qualifiées « SecNumCloud » au 20 juillet 2023[13]. On y trouve trois offres fondées sur un cœur logiciel d'infrastructure VMWare (Atos, Cloud Temple, OVH) et une offre fondée sur un cœur logiciel d'infrastructure CISCO Unified Computing System (Outscale). La quatrième offre (Oodrive) ne concerne pas l'infrastructure (IaaS).

	Date de début de la qualification	Date de fin de la qualification	Niveau de recommandation	IaaS	PaaS	SaaS	Référence de la qualification
Informatique en nuage (SecNumCloud)							
Cloud Temple							
Secure Temple	15/03/2022	15/03/2025	✓	×			569
Oodrive							
Oodrive platform avec le service Oodrive_meet	09/05/2023	22/01/2025	✓			×	766
Oodrive platform avec le service Oodrive_work	09/05/2023	22/01/2025	✓			×	768
Oodrive platform avec le service Oodrive_work_share	09/05/2023	22/01/2025	✓			×	770
Outscale SAS							
IaaS Cloud on Demand	09/06/2023	30/11/2023	✓	×			958
OVH							
Private Cloud	05/06/2023	23/12/2023	✓	×			937
Worldline							
Worldline Cloud Services - Secured IaaS	22/10/2021	22/10/2024	✓	×			2686

Figure 1 : Offres d'informatique en nuages qualifiées « SecNumCloud » au 20 juillet 2023.

Or, comme l'a révélé Edouard Snowden[14], des portes dérobées sont systématiquement introduites dans les logiciels et matériels conçus aux États-Unis. C'est aussi probablement le cas des matériels et logiciels produits en Chine ou en Europe.

VMWare et CISCO UCS étant des logiciels d'origine américaine fournis sous forme binaire et sans accès au code source, il est difficile d'en supprimer les portes dérobées éventuelles. On peut donc conclure qu'aucune offre commerciale ne répond aux exigences simultanées

[11] SPM (2021), « Appel d'offres pour l'hébergement internet des sites des services du Premier ministre », 22 septembre, Paris, France.

[12] LATOMBE P. (2023), « Communiqué de presse : Le *Health Data Hub* refuse d'engager sa migration *cloud* vers une solution souveraine européenne avant le T3 de 2025 (...) », 3 mai, Assemblée nationale, Paris, France.

[13] ANSSI (2023), « Liste des produits et services qualifiés », 20 juillet, Paris, France.

[14] SNYDER B. (2014), "Snowden: The NSA planted backdoors in Cisco products", *Infoworld*, 15 mai.

de qualification « SecNumCloud » et d'immunité « contre tout accès non autorisé par des autorités publiques d'État tiers ». Seule une offre déconnectée de tout réseau public pourrait éventuellement répondre à ces deux critères.

Quant aux *clouds* internes de l'État « Nubo » et « Pi », ils s'appuient tous deux sur le logiciel libre « OpenStack » édité par une fondation de droit américain, dont 85 % des sponsors « platine » sont américains ou chinois[15]. Ce sont les seules offres de *cloud* éventuellement conformes aux deux critères de qualification et d'immunité. Le logiciel « OpenStack » a depuis été abandonné par une grande partie de ses intégrateurs[16] en raison de difficultés techniques : on peut s'interroger sur sa viabilité notamment en termes de cybersécurité. À moins de déconnecter ces *clouds* d'Internet, l'usage de processeurs Intel ou AMD sur les *clouds* internes de l'État ne permet pas non plus de garantir l'immunité « contre tout accès non autorisé par des autorités publiques d'État tiers » en raison de l'intégration à ces processeurs de dispositifs techniques de prise de contrôle à distance[17].

Il existe pourtant de nombreuses offres européennes de logiciel d'infrastructure (OpenNebula, OpenSVC, Proxmox, Nexedi, Vates, Virtuozzo, etc.) et de microprocesseur (Kalray, NXP, ST, etc.). Plusieurs opérateurs de *cloud*, dont Scaleway, ont proposé de fournir le code source et les plans de leur infrastructure de *cloud* pour que l'État en opère une copie sous son contrôle.

Toutes ces informations étaient connues de l'État avant 2021[18]. L'État a néanmoins choisi une stratégie conduisant dans les faits à exclure des marchés publics les offres de *cloud* d'origine technologique européenne et à favoriser des offres d'origine technologique américaine. Cette stratégie creuse la balance extérieure, détruit les compétences européennes dans les PME du numérique et ne garantit ni l'absence de portes dérobées ni l'immunité de nos infrastructures.

L'ANSSI, frein à la résilience

Le mécanisme clef de l'exclusion des marchés publics des offres technologiques européennes est la qualification « SecNumCloud »[19] délivrée par l'Agence nationale de sécurité des systèmes d'information (ANSSI). Il prolonge un préjugé exprimé devant l'Assemblée nationale par son directeur à l'époque : « le développement logiciel n'est pas le point fort de la France et ne l'a jamais été »[20]. Ce préjugé peut s'expliquer par les nombreux échecs de grandes entreprises françaises dans le domaine du logiciel : défaillances du système d'écoutes de la justice[21], échec du projet de *cloud* souverain Cloudwatt[22], fiches de paie loufoques dans l'armée[23], etc.

---

[15] OPENINFRA FOUNDATION (2022), "2022 Annual Report", Austin, Texas, USA.

[16] VAUGHAN-NICOLS S. (2019), "SUSE drops OpenStack Cloud", *ZDNet*, 9 octobre.

[17] CLABURN T. (2017), "Intel Management Engine pwned by buffer overflow", *The Register*, 6 décembre.

[18] FDL (2020), « Gaia-X : un *cloud* européen sans les industriels européens du *cloud* ? », 25 août, La Madeleine, France.

[19] ANSSI (2022), « Prestataires de services d'informatique en nuage (SecNumCloud) – référentiel d'exigences », version 3.2, 8 mars, Paris, France.

[20] BRIDEY J.-J. (2018), « Audition de M. Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information, sur le projet de loi de programmation militaire », Assemblée nationale, 8 mars, Paris, France.

[21] DUMOULIN S. (2016), « Thalès embarrassé par la panne de son système d'écoutes judiciaires », *Les Échos*, 14 mars.

[22] DEBES F. (2019), « Une page se tourne pour le *cloud* souverain français », *Les Échos*, 1er août.

[23] RELTIEN P. (2018), « Louvois, le logiciel qui a mis l'armée à terre », *France Inter*, 27 janvier.

Ces mêmes entreprises, pourtant à l'origine de nombreux échecs, n'ont pas eu de difficulté à obtenir la qualification « SecNumCloud » auprès de l'ANSSI. Ce que privilégie cette qualification, c'est avant tout la centralisation des infrastructures et la formalisation des procédures : centralisation de la gestion des risques, procédures d'agrément des fournisseurs, procédure de vérification d'antécédents des candidats à l'embauche, procédure de contrôle d'accès aux installations physiques, etc. Les grandes entreprises françaises du numérique excellent dans ce domaine, tout comme leurs consœurs à l'international.

Ce préjugé de l'ANSSI s'explique aussi par l'omission du tissu de PME européennes extrêmement compétitives dans le domaine du logiciel et dont les principaux clients sont à l'export. La société grenobloise VATES, éditeur du logiciel d'infrastructure XCP-NG, propose un équivalent français de VMWare, le logiciel propriétaire américain utilisé dans la quasi-totalité des *clouds* qualifiés « SecNumCloud » à ce jour. VATES réalise 95 % de son chiffre d'affaires à l'export. Le projet scikit-learn, hébergé par la fondation INRIA, est le *leader* des outils d'apprentissage, l'une des branches les plus utilisées de l'intelligence artificielle. Il a parmi ses financeurs Microsoft, Fujitsu et le Boston Consulting Group.

Ensemble, les PME européennes sont capables de proposer des offres de *cloud* compétitives, pionnières et complètes, du IaaS au PaaS en passant par le *edge computing* industriel et la 5G virtualisée[24]. Leur organisation sous forme de réseau de petits fournisseurs indépendants les uns des autres permet en outre de se prémunir contre une « panne générale », phénomène observé régulièrement sur les grands réseaux de télécommunication malgré toutes les précautions prises par les opérateurs[25] ou sur le *cloud* de Google dont l'incendie[26] parisien en mai 2023 a perturbé l'ensemble des services dans le monde. Lorsqu'une infrastructure s'appuie sur plusieurs opérateurs de centres d'hébergement gérés selon des procédures distinctes, sur plusieurs fournisseurs de transit Internet indépendants, sur des logiciels d'infrastructure et sur des services applicatifs aux fonctions similaires mais d'origines diverses, il est rare que l'ensemble des services tombe en panne au même moment. Au lieu de pannes géantes mais peu fréquentes, une approche répartie multi-fournisseurs conduit à des pannes plus fréquentes mais limitées et sans interruption de service grâce à la redondance entre fournisseurs.

C'est ce que l'on appelle la résilience[27].

Mais la qualification « SecNumCloud » est d'autant plus coûteuse qu'elle nécessite d'agréer un grand nombre de sous-traitants indépendants. Cela favorise des offres monolithiques gérées par une seule grande entreprise – moins résilientes – au détriment des offres issues d'un district industriel de PME – plus résilientes.

La doctrine de l'ANSSI tend par ailleurs à promouvoir une gestion centralisée du risque au travers d'outils de surveillance appelés « boîtes noires » qu'il est plus simple et moins coûteux de placer en un seul point de passage de l'information plutôt qu'en des milliers de points de passage. Les « boîtes noires » ont été légalisées en 2015 par la loi sur le renseignement[28], étendues en 2021 par une nouvelle loi sur le renseignement[29] et renforcées en 2023 par la loi de programmation militaire sous le nom de « sondes » de recueil de

[24] EUCLIDIA (2021), "Strategic autonomy now", p. 10, Luxembourg Internet Days, Luxembourg.

[25] LEROY T. (2023), « Orange : une panne nationale empêche de passer des appels sur mobiles », *BFM Tech & Co*, 30 mai.

[26] SHARWOOD S. (2023), "Google Cloud's watery Parisian outage enters third week, with no end in sight", *The Register*, 10 mai.

[27] FERMIGIER S. (2013), « Groupe thématique logiciel libre. Contribution au plan industriel *cloud* », p. 7, Systematic Paris Region, 20 décembre.

[28] REES M. (2015), « Surveillance et boîte noire au menu de la loi sur le renseignement », Nextinpact, 18 mars.

[29] ADAM L. (2021), « Loi renseignement 2 : Le retour des boîtes noires », *ZDNet*, 28 avril.

données[30]. C'est une même agence qui est donc en charge de déployer des outils d'atteinte à la vie privée ou au secret des affaires, et d'instruire une qualification de services de *cloud* visant à protéger la vie privée et le secret des affaires.

Les conflits de missions auxquels l'ANSSI fait face ont pu la conduire à freiner des projets de recherche dans le domaine de la résilience et des architectures réparties, bien que ce ne soit pas son rôle. Le projet de recherche « SimpleRAN » lancé dans le cadre de la stratégie d'accélération 5G de l'État a par exemple subi un retard d'un an à cause de l'ANSSI qui souhaitait que son architecture résiliente soit modifiée pour fonctionner de façon centralisée et qu'elle puisse accueillir des boîtes noires, ce qui revenait à vider une partie du projet de son sens. Ce n'est qu'après avoir accepté formellement ces exigences que le projet a été approuvé. Les membres du projet ont en réalité pris la décision d'abandonner le marché français de la résilience et de ne rien faire qui conduise à violer la vie privée ou le secret des affaires ; il existe par ailleurs suffisamment de besoins de résilience à l'export alors que les pannes de grandes infrastructures ne cessent de croître[31] et que le Splinternet menace la continuité d'Internet[32].

Loin de se cantonner aux marchés publics d'État ou à un rôle de censeur de la politique industrielle, les pouvoirs exorbitants de l'ANSSI seront étendus avec la directive NIS2[33] qui lui confèrent « la possibilité d'émettre des instructions contraignantes » et d'agir comme une « police répressive à l'encontre des entreprises, de plus en plus guidées et ralenties par des contraintes législatives et réglementaires », accélérant ainsi la concentration du marché français autour des technologies de quelques multinationales américaines au détriment de notre résilience.

Le logiciel libre européen discriminé

Les logiciels libres, en associant de nombreux développeurs à la création d'une œuvre partagée, sont une des formes les plus abouties de district industriel[34]. Les logiciels libres sont créés et édités en Europe principalement par des PME et par des auteurs individuels, plus rarement par des organismes à but non lucratif. Leur sécurité s'appuie sur des mécanismes sociaux de confiance partagée fondés sur la reconnaissance mutuelle entre pairs et non sur des procédures bureaucratiques d'audit.

Les mécanismes sociaux de confiance partagée sont proscrits par la qualification « SecNumCloud » qui oblige les utilisateurs de logiciels libres à vérifier ligne à ligne chaque contribution au code de chaque logiciel libre utilisé dans le cadre d'un processus d'audit formel. Ce n'est pas le cas avec un logiciel propriétaire d'infrastructure (par exemple VMWare) pour lequel un contrat peut suffire à condition qu'il comprenne les clauses requises par l'ANSSI. Ce n'est pas le cas non plus avec un logiciel propriétaire d'infrastructure « à base de logiciel libre » issu d'un grand éditeur américain (par exemple IBM) et doté d'un contrat similaire.

Une PME européenne éditrice de logiciel libre n'est hélas pas en mesure de proposer ce type de contrat en raison des risques et des lourdeurs qu'il ferait peser sur elle et qu'elle ne pourra pas financer. La création européenne de logiciels libres, souvent remarquable

[30] ALOMAR B. (2023), « La loi de programmation militaire risque de percuter la doctrine du "*cloud* de confiance" », *Le Monde*, 24 mai.

[31] SMETS J.-P. (2023), "Cloud outages are on the rise. Here's why", *Fortune*, 7 juin.

[32] KRIM T. (2023), "Is the Breakup of the Internet inevitable?", DLD, Munich, Allemagne, 12 janvier.

[33] PETIOT L. (2022), « Directive NIS2 : les enjeux de la nouvelle cybersécurité européenne », *Contrepoints*, 4 décembre.

[34] TWOWINGS *et al.* (2009), « District industriel », Wikipedia.

et majoritairement issue de PMEs, se retrouve ainsi discriminée par rapport aux logiciels propriétaires issus de grands éditeurs, majoritairement américains.

Ce n'est pas la première attaque récente contre les solutions libres européennes.

En 2021, la direction générale des Entreprises[35] lançait un processus de rapprochement européen en vue de constituer des projets importants d'intérêt européen commun (PIIEC) dotés de larges subventions. Cependant, elle favorisait les grands intégrateurs français et omettait de nombreux fournisseurs européens de logiciels d'infrastructure de *cloud*. Les projets finalement validés, portés par des intégrateurs partenaires de Google, favorisaient les logiciels libres de Google plutôt que ceux d'éditeurs européens de logiciels libres équivalents. Une note d'étonnement dénonçant une entente a été transmise par plusieurs éditeurs européens aux autorités nationales et européennes en charge de la concurrence.

Le 24 janvier 2023, la direction interministérielle du Numérique (DINUM) organisait une réunion de promotion de solutions propriétaires de *cloud* pour les équipes de développement[36]. Il existe pourtant une offre européenne compétitive de *cloud* libre dont la promotion auprès des administrations fait explicitement partie des missions de la DINUM conformément à la loi du 7 octobre 2016 pour une République numérique[37].

Le 15 septembre 2022, la Commission européenne posait avec le « Cyber Resilience Act »[38] un principe de responsabilité des ayants droit pour toute faille de sécurité présente dans un logiciel libre. L'ayant droit d'un logiciel libre s'expose ainsi à une amende de 15 millions d'euros dans le cas où son logiciel, intégré à un produit commercialisé par un tiers, serait à l'origine d'un incident de cybersécurité, et ce quand bien même il n'aurait jamais été rémunéré pour cela. Seule échappatoire pour l'ayant droit : céder son actif logiciel à une fondation de logiciel libre, le plus souvent américaine. Pour les autres, la Commission européenne estime dans son étude d'impact que cette régulation impliquera un minimum de 25 000 € de frais administratifs par logiciel et une augmentation de 30 % des coûts de développement[39], un niveau bien trop élevé pour favoriser la croissance de l'écosystème des éditeurs de logiciels libres dont la Commission reconnaît pourtant la nécessité pour atteindre l'indépendance numérique[40].

La proposition publiée le 28 septembre 2022 pour réviser la directive sur la responsabilité du fait des produits défectueux instaure un régime de responsabilité stricte qui pourrait accroître encore plus le risque pour les ayants droit de logiciels libres[41]. Tout comme dans le « Cyber Resilience Act », la notion d'usage non commercial d'un logiciel libre[42] n'exonère pas les ayants droit d'éventuelles poursuites pour des usages de leur logiciel quand bien même ils n'auraient pas été rémunérés.

[35] O C. (2021), « PIIEC *cloud* : Lancement du processus de rapprochement européen », 6 octobre, Ljubljana, Slovénie.

[36] DINUM (2023), « L'État dans le nuage : une journée dédiée au *cloud* », 24 janvier, Paris, France.

[37] LEMAIRE A. (2016), « Loi n°2016-1321 du 7 octobre 2016 pour une République numérique », *Journal Officiel*, 7 octobre.

[38] EUROPEAN COMMISSION (2022), "Cyber Resilience Act", 15 septembre, Bruxelles, Belgique.

[39] EUROPEAN COMMISSION (2022), "Impact Assessment Report", 15 septembre, Bruxelles, Belgique.

[40] EUROPEAN COMMISSION (2020), "Open source software strategy 2020-2023", 21 octobre, Bruxelles, Belgique.

[41] BUSINESSEUROPE *et al.* (2023), "Proposed Product Liability Directive revision may undermine Europe's competitiveness", 15 mai.

[42] DE LUCA S. (2023), "New Product Liability Directive", European Parliamentary Research Service, Mai, Bruxelles, Belgique.

La proposition de règlement du 15 mai 2023 sur l'intelligence artificielle[43] propose de subordonner le droit de publier un logiciel – libre ou non – à la vérification d'une dizaine de critères allant du respect de la démocratie à la réduction des émissions de gaz à effet serre en passant par la vérification de l'adéquation de toute nouvelle ligne de code produite à l'ensemble des lois de l'Union européenne au moyen d'un système de gestion de la traçabilité. Ces exigences, qui impliquent un surcoût important pour un logiciel propriétaire sont fondamentalement incompatibles avec le processus de développement des logiciels libres. Avec un logiciel libre, on commence par publier son code avant de collaborer. Avec le règlement, on commence par faire un audit avant de pouvoir collaborer, ce qui freine la collaboration au point de la rendre impraticable.

Quant à la révision de mai 2023 de la doctrine « *cloud* au centre », elle restreint l'obligation d'usage de logiciels libres aux seuls « communs numériques contributifs », une définition qui exclut les éditeurs européens de logiciels libres contrairement à la notion de « bien public numérique » qui, elle, inclut le secteur privé[44]. La notion retenue de « commun numérique » offre ainsi aux services de l'État une base légale pour développer des logiciels concurrents de logiciels libres déjà disponibles au prétexte qu'un logiciel libre d'éditeur européen ne serait pas un commun et que l'on ne pourrait donc pas lui faire confiance.

La transparence, alternative à la confiance pour préserver l'autonomie

La politique « *cloud* de confiance » et la norme « SecNumCloud » ont été imaginées par certains comme un outil de protectionnisme déguisé sous une norme technique et donc compatible avec le traité de l'Organisation mondiale du commerce (OMC). En pratique, son effet a été l'inverse du protectionnisme. La « confiance » a multiplié les barrières à l'entrée pour les fournisseurs européens de technologies de *cloud* et a accéléré l'adoption de technologies américaines de *cloud* peu sûres. Il eut été plus simple d'appuyer une politique protectionniste sur des bases légales déjà éprouvées telles que l'exception culturelle, le Règlement général pour la protection des données (RGPD) ou des obligations fortes de réversibilité déjà présentes dans le code des marchés publics[45].

L'impératif de la cybersécurité pourrait néanmoins expliquer la poursuite en France d'une politique de numérique de confiance malgré des effets délétères désormais évidents en matière d'autonomie. L'accroissement des tensions internationales a fait de la cybersécurité une priorité absolue, y compris au détriment de notre résilience. L'État achète ses technologies de *cloud* aux États-Unis plutôt qu'en Europe pour les mêmes raisons que nos voisins européens achètent leurs avions de combat aux États-Unis plutôt qu'en Europe[46] : cela répond à un besoin de protection et d'assistance ; charge ensuite à des intégrateurs nationaux d'en assurer la distribution et l'entretien.

Nous ne sous-estimons pas ici l'importance des enjeux liés à la cybersécurité. Tous les systèmes informatiques que nous utilisons comportent un nombre de failles incommensurable que même les plus grandes entreprises dotées de processus formels d'audit rigoureux

[43] BENIFEI B. & TUDORACHE I.-D. (2023), "Proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts", Draft compromise amendments, European Parliament, 16 mai.

[44] NORAD, UNDP & UNICEF (2023), "Promoting digital public goods to create a more equitable world".

[45] SMETS J.-P. (2022), « Qu'est-ce qu'un *cloud* libre ? », *Les Annales des Mines - Enjeux numériques*, juin.

[46] SPINELLI F., SMETS J.-P. & LECHELLE Y. (2021), « Défense, *cloud* souverain : les PME au centre de notre indépendance », *Les Échos*, 12 juillet.

ne parviennent pas à contenir[47]. Ces failles existent car la charge cognitive nécessaire pour mesurer l'impact cyber d'une ligne de code écrite dans un langage de programmation de conception ancienne tel que « C » est supérieure à la capacité du cerveau humain. En l'absence d'une nouvelle génération de systèmes d'exploitation et de langages de programmation intégrant la cybersécurité dans leurs principes de conception, éliminer les failles de cybersécurité revient à boucher les trous d'un tamis dont la surface grandirait plus vite que les zones déjà bouchées.

Plutôt que de faire croire aux clients du *cloud* qu'une qualification les protégera de tout risque, comme par magie, il serait plus honnête et conforme au devoir de conseil de leur décrire en toute transparence l'absence relative de cybersécurité. Cela leur permettra d'organiser leur défense en ayant conscience de la réalité des risques.

Peut-on garantir en France qu'un processeur Intel ne comporte pas de portes dérobées destinées à un État tiers ? non ; qu'un processeur ST ne comporte pas de portes dérobées destinées à un État tiers ? oui, à condition qu'il ait été audité par des autorités françaises compétentes et produit en France ; que le code de Linux ne comporte pas de failles permettant un accès à distance à un État tiers ? non ; qu'un code écrit en python n'accédera pas aux données d'un autre processus sans en avoir les permissions ? non, mais cela arrivera moins souvent qu'avec un code écrit en C grâce à la protection mémoire partielle offerte par l'interpréteur.

Ces faits étant acceptés par le client, une discussion peut alors s'engager sur la base d'une grille d'analyse de risque partagée en toute transparence avec le fournisseur. Où sont stockés les mots de passe et les clés de chiffrement pour accéder aux bases de données ? Peut-on dédier un serveur physique à un seul client ? La police peut-elle demander une copie du disque dur du serveur ? Quel est le délai moyen entre l'annonce publique d'une vulnérabilité et sa prise en compte dans une mise à jour ? Quels moyens sont proposés au client pour vérifier la véracité des réponses fournies ? Les autres questions de cette grille sont le résultat d'un effort collaboratif entre clients et fournisseurs.

Les réponses à cette grille d'analyse permettent ensuite au client de décider contre quels risques il souhaite se protéger et comment il souhaite se protéger. On a remplacé la notion binaire de « confiance » par une notion de « transparence » à plusieurs dimensions.

Chaque client, chaque application ayant des besoins et des priorités différents en matière de risque, une grille d'analyse permet de comparer les offres en fonction des réels besoins plutôt qu'en sélectionnant l'offre dite de « confiance », c'est-à-dire l'offre qui cocherait tous les besoins de cybersécurité de toutes les applications de tous les clients… et n'existe pas. On ouvre ainsi le marché à une grande diversité de fournisseurs, certains – souvent européens – disposant de meilleurs services dans le domaine de la résilience ou du temps réel et d'autres – souvent américains – disposant d'interfaces utilisateur intuitives moins génératrices d'erreurs par les utilisateurs ou permettant de se connecter au bouclier cyber du commandement américain

Alors que la confiance produit de l'obscurité sur le marché, la transparence fluidifie le marché en évitant les phénomènes de concentration, d'entente ou de barrières non douanières. Alors que la confiance favorise les technologies américaines, la transparence accélère l'adoption des fournisseurs européens de technologies numériques dont le succès à l'export reste la meilleure démonstration de leurs avantages compétitifs et dont l'existence est indispensable à notre autonomie.

[47] ARGHIRE I. (2023), "Severe Azure vulnerability led to unauthenticated remote code execution", SecurityWeek, 31 mars.

Politique chinoise de l'IA : comment la Chine joue au go

Par Paul JOLIE
Ingénieur général des mines, Conseil général de l'économie

Les dirigeants chinois actuels entendent que la Chine revienne à la première place mondiale, devant les États-Unis, d'ici 2049, centenaire de l'arrivée du PCC au pouvoir. Cela inclut une prédominance dans des technologies clés, dont l'IA, pour ses enjeux tant civils que militaires et de capacité d'influence géostratégique.

Les racines de cette stratégie sont anciennes (politiques : discours de Deng Xiao Ping en faveur de la science et la technologie en 1978, puis vision de la Chine numérique portée par Xi Jinping ; scientifiques, avec des mathématiciens chinois pionniers et des scientifiques chinois impatriés). Elle est portée par une planification qui s'est intensifiée pour l'IA à partir de 2016, amplifiée par les 13e et 14e plan. Ce dernier veut des industries de base de l'IA en Chine dépassant 1 000 Mds RMB en 2030 et que les industries du pays liées à l'IA dépassent alors les 10 T RMB. Un faisceau d'actions y concourent (4,7 Mds$ de R&D pour l'IA, liens privé-publics, brevets, *brain drain*, achats de *start-up* hors de Chine par des fonds dédiés, marchés publics, usage de données à grande échelle que permet la population).

Préambule – La prise de conscience

En avril 2023, le Chinois Ding Liren est devenu le dix-septième champion du monde d'échecs de l'histoire, succédant à celui qui détenait la couronne mondiale depuis 2013 et demeure toujours le numéro un au classement par points, le Norvégien Magnus Carlsen.

C'est d'autant plus remarquable qu'en Chine, on joue aux échecs chinois qui sont un jeu très différent des échecs tels que nous les connaissons en Occident. Les chinois pratiquent plusieurs jeux, dont le jeu de go, très pratiqué en Asie depuis plus de mille ans.

En 2016, AlphaGo, une intelligence artificielle développée par la société Deepmind (depuis rachetée par Google) a battu successivement en mars le troisième meilleur joueur de go, Lee Sedol, puis en mai, le meilleur joueur du monde de go, Ke Jie. Les victoires d'AlphaGo représentent une avancée historique de l'intelligence artificielle. Cela a été un choc, une prise de conscience collective de la puissance de l'intelligence artificielle. Pour de nombreux observateurs, 2016 est sans doute l'année du renouveau de l'IA, après que cette technologie ait subi pendant plusieurs décennies plusieurs longs « hivers ».

Rappels historiques sur l'intelligence artificielle en Chine

L'IA a mis du temps à s'imposer en Chine, où elle était considérée dans les années 1950 comme une invention de la pseudoscience bourgeoise occidentale, et dans les années 1960 et suivantes comme un symbole du révisionnisme soviétique et un fantasme impossible.

Trois événements décisifs ont changé l'implication de la Chine dans l'IA et, à long terme, par voie de conséquence probable, le monde lui-même :

- En mars 1978, Deng Xiaoping a prononcé un discours historique lors d'une conférence scientifique nationale à Pékin, intitulé « La science et la technologie sont des forces productives » qui a marqué le « printemps à venir » de la (ré)émergence de la Chine en tant que puissance scientifique et technologique. Bien que banale dans le contexte actuel, cette déclaration était révolutionnaire dans un pays dont les intellectuels avaient été persécutés pendant une décennie (1966-1976).
- Les intellectuels chinois eux-mêmes ont constitué un deuxième catalyseur. Trois d'entre eux sont considérés dans les sources chinoises comme les premiers pionniers : le mathématicien Wu Wenjun (1919-2017), Zhang Bo (1935-) et Qian Xuesen (1911-2009). Ce dernier a été un ardent défenseur au début des années 1980 de la recherche sur l'IA en Chine.
- Le troisième élément de l'acceptation de l'IA par la Chine a été l'impact des rapatriés en général, qui sont devenus « les *leaders* universitaires et les piliers de la recherche, du développement et de l'application de l'intelligence artificielle en Chine ».

La stratégie de jeu de go concernant l'IA

Premier principe du jeu de go : avoir une stratégie – la Chine numérique

De l'importance de la vision

Xi Jinping, l'actuel président de la République populaire de Chine (RPC), a étudié le génie chimique à l'université de Tsinghua à Pékin (l'une des meilleures universités chinoises) de 1975 à 1979, ce qui fait de lui un scientifique de formation et lui donne donc une certaine façon de voir et penser le monde.

Il a fait de la Chine numérique une clé de la réussite nationale, mais en retour la Chine numérique a également contribué à la réussite individuelle de Xi. Celui-ci a d'abord adopté le concept de « Fujian numérique » d'un universitaire local alors qu'il était secrétaire adjoint du parti et gouverneur de cette province, le Fujian, en 2000. Cette campagne était conçue comme un simple effort pour utiliser les technologies numériques nouvelles et émergentes afin d'améliorer la gouvernance locale et les performances économiques – en substance, les premières expériences de la Chine en matière d'administration en ligne. Cependant, au cours des vingt années suivantes, Digital Fujian a évolué et s'est étendu pour finalement réapparaître comme la vision du parti pour une « Chine numérique ».

La technologie soutient les deux approches de Xi Jinping que sont l'informatisation et la modernisation. Pour Pékin, bien que la compétition mondiale autour de la technologie soit fondamentalement une question d'idéologie, concrètement, la compétition elle-même sera de plus en plus axée sur les données massives (*big data*). Les données sont le nouveau « facteur de production » qu'il faut contrôler. Les données sont en train de reconstruire en profondeur l'économie mondiale et la Chine l'a compris très tôt.

La Chine a compris comme d'autres pays que la révolution numérique était la nouvelle révolution en cours dans laquelle il fallait prendre des positions aujourd'hui pour dominer le monde (économiquement dans un premier temps, idéologiquement dans un second temps) à l'avenir.

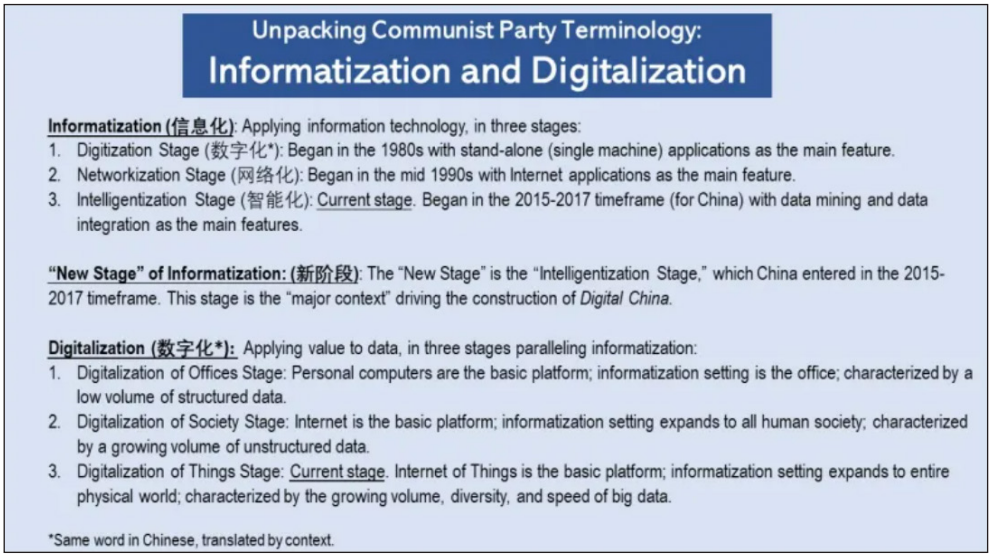
Pour gagner cette compétition, le succès réside dans une stratégie « du type du jeu de go », qui consiste à relier différentes industries qui se complètent et s'enrichissent mutuellement. D'où la volonté d'investir massivement dans le *big data*, la puissance de calcul

et l'intelligence artificielle, ainsi que de construire une infrastructure numérique et les systèmes de gouvernance *ad hoc*.

Le concept de modernisation à la chinoise

Le concept de modernisation a été revu, tant pour les sphères civiles que militaires. Autrefois décrite uniquement en termes d'« informatisation » (application des technologies de l'information), une nouvelle voie, peut-être plus critique, a été ajoutée : la « numérisation » (application de la valeur aux données).

Pékin se concentre à long terme sur la concurrence autour du *big data* et sur le développement des écosystèmes numériques complexes. Les nombreux projets de modernisation utilisent ces technologies « qui s'entrecroisent » dans les différents ensembles développés par la Chine. Le niveau local jouant son rôle, en cohérence avec la stratégie nationale, tout en utilisant les grandes entreprises chinoises du secteur pour créer de « l'harmonie » et de la cohérence technologique entre ces différentes initiatives.



Décomposition de la terminologie
du parti communiste : informatisation et numérisation.
Source : PRC State-Run Media, Multiple.

La Chine numérique

La Chine numérique, c'est en fait « gagner l'ère numérique » (la rejoindre) et « gagner dans l'ère numérique » (devenir *leader* de cette révolution). Xi Jinping affirme que la modernisation à la chinoise, qui repose en partie sur la transformation numérique de la modernisation socialiste, donne à la Chine un avantage à la fois sur le plan intérieur (en améliorant l'efficacité sociétale et l'équité sociale) et sur le plan mondial (en offrant une alternative supérieure au capitalisme).

Comme les deux objectifs, national et mondial, promettent d'élever le niveau de vie, ils constituent le fondement d'un récit de propagande interne et externe qui est aujourd'hui très important. La nation doit se rallier à la vision marxiste d'un avenir numérique conçue par le parti et ce dernier a fixé des objectifs élevés pour cette vision digne d'une « grande puissance ».

Gagner l'avenir

« Comment la Chine entend gagner l'avenir ? » est tiré de la section d'ouverture du « Rapport sur le développement de la Chine numérique » publié en 2017 par la Cyberspace Administration of China, mais l'expression elle-même trouve son origine dans les « Grandes lignes de la stratégie nationale de développement de l'informatisation » de 2016, qui ont été publiées par ce même organisme.

« Gagner l'avenir » est une expression idiomatique très répandue en Chine, tant à l'oral qu'à l'écrit. Le plus important est peut-être que peu de politiques sont liées aussi directement à Xi lui-même. La stratégie est en cours d'élaboration depuis près d'un quart de siècle et est en cours d'exécution depuis plus d'une décennie.

Une stratégie globale de développement de l'informatique au niveau national dans la nouvelle économie

Bien que d'autres stratégies numériques nationales de la RPC aient pu émerger en premier ou soient mieux connues en Occident (notamment la stratégie *Cyber Great Power* et la stratégie nationale *Big data*), la Chine numérique a progressivement évolué pour devenir LA stratégie numérique « globale » du parti.

Le succès de la Chine numérique sera finalement mesuré à l'aune de sa capacité à atteindre les « fins » (buts ou objectifs) les plus élevées de la stratégie par la mise en œuvre efficace de ses « moyens » (plans d'action) en utilisant les « moyens » (ressources nécessaires) mis à sa disposition.

Deuxième principe du jeu de go : mettre en place un plan de développement

Le gouvernement chinois documente ses ambitions en matière d'IA dans des plans et des politiques formels et transparents, qui sont rédigés et promulgués par les échelons les plus élevés du gouvernement et du Parti communiste (PCC) au pouvoir.

Les premières références à l'intelligence artificielle

Le premier plan officiel du gouvernement chinois à mentionner l'intelligence artificielle a été publié en 2015. Mais l'intérêt de la Chine pour les technologies de pointe remonte à bien plus loin comme on l'a vu.

En 1986, le PCC a fixé sa première série de plans concernant la science et la technologie, conçus pour combler les lacunes stratégiques de la Chine et « dépasser » les États-Unis sur le plan technologique et économique. Des initiatives stratégiques majeures telles que le programme 863 et le programme 973 ont accéléré les progrès technologiques de la Chine dans les années 1980 et 1990, et ont contribué aux avancées du pays dans les domaines de l'aérospatiale et des télécommunications.

Au milieu des années 2000, les dirigeants chinois ont commencé à reconnaître l'importance des systèmes et équipements « intelligents » parallèlement aux technologies numériques.

Plusieurs des politiques scientifiques et technologiques du PCC mettent l'accent sur le rôle de l'IA dans l'accroissement de la puissance nationale globale.

L'année 2016 : An 1 du lancement de l'IA en Chine

Quatre ministères chinois ont publié conjointement le plan d'action triennal 2016 « Internet + pour l'intelligence artificielle », qui s'inscrit dans le prolongement de la politique chinoise « Internet + » et met l'accent sur le développement de l'industrie de l'intelligence artificielle. Le plan appelait à un développement rapide de neuf technologies

d'IA majeures telles que les appareils ménagers intelligents, l'automobile intelligente, les systèmes sans pilote et les terminaux intelligents, entre autres…

Publié en 2017, le Plan de développement de l'Intelligence artificielle de nouvelle génération (AIDP) du Conseil des affaires d'État a marqué un tournant majeur en faisant de l'IA un aspect essentiel de la stratégie de développement économique national de la Chine. Le plan appelle les acteurs étatiques et non étatiques à soutenir le gouvernement central dans sa quête d'un *leadership* mondial en matière d'IA et à utiliser la technologie pour atteindre la prochaine phase de la croissance économique.

Elle mentionne pour la première fois officiellement l'IA, identifie onze actions spécifiques pour la transformation technologique et prévoit de porter la taille du marché de l'industrie chinoise de l'IA à 100 milliards de RMB (15,26 G$) d'ici à 2018.

Le 13e plan quinquennal (2016-2020)

Le plan chinois : des priorités claires

Le 13e plan quinquennal de la Chine pour la science, la technologie et l'innovation (2016-2020) a désigné quinze « mégaprojets » dans des domaines liés à l'IA tels que les sciences du cerveau, les réseaux intelligents, les réseaux quantiques, les réseaux espace-sol, le *big data*, la robotique, la fabrication intelligente et la cybersécurité.

Le 13e plan quinquennal pour le développement des industries stratégiques émergentes fixe des objectifs pour accélérer le développement de l'IA en promouvant la recherche fondamentale et l'application de la technologie dans divers domaines. L'IA apparaît comme un « moteur de développement économique » mais le plan quinquennal reconnaît les importants goulets d'étranglement technologiques de la Chine.

Le plan d'action triennal pour promouvoir le développement d'une industrie de l'intelligence artificielle de nouvelle génération (2018-2020) réaffirme les engagements pris dans le plan d'action triennal « Internet + » pour l'intelligence artificielle ; fixe des objectifs spécifiques pour le développement de l'industrie de l'intelligence artificielle dans une série de catégories de produits telles que les robots de service intelligents, le traitement des données et les drones intelligents, entre autres… Et cherche à renforcer et à réformer les instruments d'investissement public-privé pour soutenir les pôles technologiques d'importance stratégique, dont l'IA.

Le 14e plan quinquennal (2021-2025)

Publié en 2021, le 14e plan quinquennal est particulièrement important. Il a été élaboré et approuvé à la veille du centenaire de la fondation du PCC. Il réaffirme l'ambition de la Chine de devenir une puissance scientifique et technologique mondiale, en fixant des objectifs mesurables et en indiquant les outils qu'elle utilisera pour les atteindre.

Ce plan énumère les nouvelles « industries pionnières », au premier rang desquelles figure l'intelligence artificielle, et met l'accent sur le financement de la recherche fondamentale et la production de brevets de haute qualité (de façon générale la politique des brevets de la Chine, lancée en 2000, est partie d'une situation totalement marginale à une position dominante en termes de nombre de brevets, triple de celui des États-Unis en 2020 avec 1,5 million de brevets émis ; leur qualité est cependant variable, ce qui explique cette nouvelle orientation vers la qualité).

L'AIDP fixe des objectifs différents pour les industries de base de l'IA et les industries liées à l'IA. D'ici 2030, il vise à ce que les industries de base de l'IA de la Chine dépassent

les 1 000 milliards de RMB (150 G$) en taille de marché, soit neuf fois plus qu'en 2018, et à ce que les industries du pays liées à l'IA dépasseront les 10 trillions de RMB (1,48 T$).

L'IA est ainsi classée au premier rang des « industries frontières » sur lesquelles le gouvernement chinois se concentrera jusqu'en 2035.

Troisième principe du jeu de go : positionner des pierres « stratégiques » sur lesquelles prendre appui à long terme

Stratégie pour les industries émergentes - SEI

Lancée par la Commission nationale du développement et de la réforme (NDRC) en 2020, la stratégie des industries émergentes stratégiques appelée SEI, oriente les investissements chinois dans plusieurs « domaines d'investissement industriels clés », au premier rang desquels figurent les « technologies de l'information », qui incluent l'IA.

Le plan appelle spécifiquement les entreprises chinoises à « faire progresser régulièrement l'innovation intégrée et l'application combinée de l'Internet industriel, de l'intelligence artificielle (IA), de l'Internet des objets (IoT), de l'Internet des véhicules, du *big data*, du *cloud computing*, de la *blockchain* et d'autres technologies ».

Le SEI appelle les gouvernements locaux et les investisseurs privés à financer conjointement des projets essentiels à la croissance économique à long terme de la Chine. Plus précisément, il charge la NDRC, le ministère de la science et de la technologie (MOST), le ministère de l'Industrie et des Technologies de l'information (MIIT) et le ministère des Finances (MOF) de mobiliser des fonds et des ressources pour les industries émergentes.

Au-delà de la stratégie nationale, « la plupart des provinces et des villes ont également introduit activement des politiques telles que des plans de développement de l'intelligence artificielle », accélérant ainsi « l'intégration profonde de l'intelligence artificielle dans l'économie, la société et l'industrie ». Le SEI encourage également les petites et micro-entreprises à accélérer l'adoption de l'IA dans tous les secteurs de l'économie chinoise en intégrant l'analyse des données dans leurs activités quotidiennes.

Quatrième principe du jeu de go : concentrer les forces pour renforcer les positions acquises

Dans ce principe du jeu de go, il s'agit de connecter les pierres qui sont proches les unes des autres pour les rendre plus fortes et ainsi consolider sa position.

Premier groupe de pions : le mégaprojet NGAI

L'État est responsable du financement d'une part importante de la science et de la technologie en Chine, en particulier de la R&D fondamentale.

Le « Mégaprojet d'innovation scientifique et technologique 2030 - Intelligence artificielle de nouvelle génération 2030 (NGAI) » est une initiative chinoise visant à aligner tous les acteurs sur une ambition commune. Lancé en 2018 dans le cadre du plan de développement de l'IA de nouvelle génération, le mégaprojet NGAI rassemble les contributions d'un large éventail d'universités, d'entreprises et de laboratoires de recherche chinois et leur apporte son soutien pour le développement de l'IA.

Le MOST, la NDRC et le MOF administrent conjointement le financement du mégaprojet NGAI :

- en 2018, ils ont autorisé 134 millions de dollars (870 millions RMB) pour trente-neuf projets de recherche ;
- en 2019, le programme MOST a réitéré son appel à projets portant sur des questions relatives à la théorie fondamentale de l'IA, telles que le raisonnement causal et la théorie de la décision, la théorie de l'apprentissage continu, les memristors et le raisonnement analytique de la corrélation inter-domaine des données de séries temporelles.

L'objectif ultime est de surmonter les « goulets d'étranglement » du développement scientifique de la Chine, de combler les lacunes stratégiques et d'accélérer les progrès de la Chine en tant que « pays innovant ».

D'autres mégaprojets existent et sont autant de groupes de pions « stratégiques »

Plusieurs autres mégaprojets gouvernementaux consacrés au *big data*, à l'informatique quantique et à la recherche inspirée par le cerveau profiteront également au développement de l'IA en Chine.

Il apparaît clairement que parmi les plus grands programmes de financement de la recherche en Chine, l'IA a émergé comme une priorité.

Les laboratoires clés de l'État

Parmi les centres de recherche gérés par l'État, les laboratoires clés de l'État (*State Key Laboratories* ou SKL) sont les plus prestigieux et les plus importants. Comptant quelque 550 institutions dans tout le pays, ils sont principalement gérés par le MOST, la Chinese Academy of Sciences (CAS) et le ministère de l'éducation, tandis que d'autres *Enterprise* SKLs sont gérés par des entreprises privées et publiques.

Plusieurs SKL participent à la R&D en matière d'IA en Chine.

Deux laboratoires d'IA rendus publics sont particulièrement importants, axés respectivement sur la science du cerveau et les systèmes de réalité virtuelle :

- le CAS Shenyang Institute of Automation (SIA), par exemple, est un *leader* dans le domaine des véhicules autonomes ;
- le CAS Institute of Automation (CASIA) se concentre sur l'analyse des données et la reconnaissance des formes.

Les instituts de recherche sur l'IA

Les instituts de recherche sur l'IA au sein des universités chinoises, au nombre de trente-quatre en 2021 et se distinguent des SKL. Leur mission principale est de former les étudiants de premier cycle aux techniques d'apprentissage automatique. Ces instituts universitaires élaborent des programmes d'études et travaillent avec des entreprises chinoises et étrangères pour se familiariser avec les développements de pointe dans le domaine de l'IA. Chaque institut d'IA a une spécialisation de recherche spécifique « qui va du traitement du langage naturel à la robotique, l'imagerie médicale, la technologie verte intelligente et les systèmes sans pilote ».

Au cœur des avantages de la Chine en matière d'IA : les politiques industrielles

Le gouvernement chinois utilise les politiques industrielles pour promouvoir les industries qui font partie intégrante du développement technologique du pays et pour combler

les écarts avec les autres pays industrialisés. Le discours de Xi Jinping au programme MOST en 2013 illustre bien cet état d'esprit.

Le gouvernement chinois a fait appel à des mécanismes traditionnels tels que les subventions et les traitements fiscaux préférentiels pour fournir un soutien financier direct aux entreprises chinoises d'IA, ainsi qu'à des mécanismes émergents tels que les fonds d'orientation gouvernementaux pour mobiliser le soutien public et privé en faveur du développement de l'industrie de l'IA en Chine.

Renforcer le soutien financier direct de l'État aux entreprises chinoises liées à l'IA

Le développement des capacités d'IA nécessite d'importants investissements en capital. L'État a élaboré des politiques industrielles agressives afin de mobiliser et d'allouer des capitaux publics et privés aux industries émergentes.

Le gouvernement chinois fournit des fonds importants pour réduire les obstacles à l'entrée sur le marché des entreprises nationales dans des secteurs émergents tels que l'IA. Pour accélérer l'innovation dans le domaine de l'IA, le gouvernement accorde des subventions et des dons en espèces aux champions nationaux directement à partir des fonds publics. Pour « choisir les gagnants » dans le domaine de l'IA, le gouvernement chinois met en place des plateformes de collaboration public-privé, telles que l'Alliance de l'industrie de l'intelligence artificielle de Chine qui distribue des subventions et des liquidités aux entreprises d'IA prometteuses.

L'exemple de iDeepWise

iDeepWise est une entreprise inspirée du cerveau et de l'apprentissage profond. Elle a participé au concours d'IA médicale de 2018, a remporté la première place et a ensuite reçu 75 400 dollars (500 000 RMB) de récompenses en espèces et 3 millions de dollars (20 millions de RMB) de subventions à la R&D sur trois ans. Bien que ces sommes ne soient pas énormes, elles peuvent s'avérer décisives pour permettre aux entreprises en phase de démarrage de se faire connaître et de commercialiser leurs produits. L'année suivante, iDeepWise est devenue la première entreprise d'IA investie par la branche de capital-risque de Huawei, Hubble Technology Investment Co. Ltd.

Différents fonds d'investissement publics

Le Fonds d'orientation de l'innovation technologique du gouvernement, le Fonds national pour le transfert et la commercialisation des technologies (NFTTC) et la State Development Investment Corporation (SIDC) soutiennent la commercialisation de la recherche financée par le gouvernement et investissent directement ou indirectement dans des entreprises d'IA.

Le gouvernement achemine également des fonds par l'intermédiaire des entreprises publiques, des pensions, des banques d'État, des fonds de capital-risque de l'État et des investissements sur le marché des capitaux. Dans ce modèle, les voies de financement de l'État sont complexes ; les investissements de l'État, des entreprises et de l'étranger sont mélangés, opaques et difficiles à désagréger.

Le gouvernement offre également aux entreprises d'IA des terrains, des installations et un traitement préférentiel pour les achats, la recherche et le recrutement de talents.

Les entreprises d'IA travaillent également avec les services de sécurité de l'État chinois ce qui leur fournit d'importantes sources de revenus. Cette collaboration semble être à double sens : le gouvernement fournit un marché aux entreprises d'IA et, en retour, les utilise pour censurer, exercer une surveillance et soutenir d'autres fonctions de l'État en Chine et à l'étranger.

Cinquième principe du jeu de go : être créatif !

Un nouvel outil de politique industrielle : les fonds d'orientation gouvernementaux

En plus d'injecter des capitaux directement dans les entreprises chinoises spécialisées dans l'IA, le gouvernement chinois tente également d'introduire la notion de profit dans une politique industrielle afin d'obtenir des rendements financiers et d'atteindre ses objectifs stratégiques.

L'objectif est de mobiliser des capitaux et d'autres ressources pour les technologies émergentes par le biais de véhicules d'investissement public-privé, également connus sous le nom de fonds d'orientation gouvernementaux.

Le premier fonds d'orientation connu est le Zhongguancun Venture Capital Guidance Fund, créé en 2002 pour soutenir les sociétés de capital-risque. En 2016, le nombre de fonds d'orientation a culminé à plus de 500.

Par le biais de fonds d'orientation, le gouvernement peut offrir du capital patient aux industries émergentes, telles que l'IA, où un capital d'investissement stable et à long terme est potentiellement décisif pour permettre aux entreprises en phase de démarrage d'innover et de se développer. Même les jeunes entreprises d'IA prometteuses bénéficiant d'un financement initial important peuvent ne pas franchir la « vallée de la mort », où la capacité d'innovation et la possibilité de passer à l'échelle supérieure et de commercialiser leurs produits sont vouées à disparaître. Les fonds d'orientation peuvent combler cette lacune.

L'exemple de Cloudwalk Technology

Cloudwalk Technology, basée à Guangzhou, est l'un des quatre dragons de l'IA chinois – une collection qui comprend également SenseTime, Megvii et Yitu. Elle est née des fonds d'orientation de la province de Guangdong. Après avoir reçu 310 millions de dollars (2 milliards de RMB) directement du gouvernement municipal de Guangzhou en 2017, Cloudwalk a levé 160 millions de dollars (1 milliard de RMB) auprès du Guangzhou Industry Investment Fund et d'autres groupes de financement en 2018. En 2020, l'entreprise a encore levé 280 millions de dollars (1,8 milliard de RMB) auprès d'institutions d'investissement d'État telles que Guangzhou Nansha Financial Holdings qui gère un fonds d'orientation pour promouvoir les industries stratégiques émergentes.

Mais encore quelques difficultés pour lever de l'argent…

Cependant, malgré l'énorme soutien politique et financier du gouvernement chinois, les fonds d'orientation lèvent souvent moins d'argent que prévu. Fin 2020, 1 851 fonds

d'orientation n'avaient levé que 873 milliards de dollars (5 650 milliards de RMB), soit moins de la moitié de l'objectif enregistré de 1 780 milliards de dollars (11 530 milliards de RMB), auprès d'investisseurs publics et privés.

Sixième principe du jeu de go : ne pas laisser d'espace stratégique à son adversaire

Construire son écosystème d'entreprises spécialisées dans l'IA

Alors que la Chine cherche à devenir un centre mondial d'innovation en matière d'IA d'ici 2030, les États-Unis restent le *leader* mondial. La Chine est en retard sur les États-Unis en ce qui concerne les talents en matière d'IA, la recherche fondamentale et les logiciels, et elle cherche à combler ces lacunes par une collaboration avec l'étranger, en particulier avec les entreprises et les universités américaines. Les liens avec les centres d'IA américains et étrangers ont joué un rôle central dans le développement des capacités de la Chine. Bon nombre des meilleurs professionnels chinois de l'IA ont été formés aux États-Unis et ont travaillé pour des entreprises et des laboratoires américains[1]. Les États-Unis ont cependant réagi récemment pour en limiter les effets[2], et dans une moindre mesure l'Union européenne[3], en durcissant leurs dispositifs de coopération en termes de R&D sur les technologies sensibles.

Les entreprises chinoises spécialisées dans l'IA sont des acteurs hybrides. L'État oriente leurs activités, les finance et les protège de la concurrence étrangère par des mesures de protection du marché intérieur, ce qui crée des avantages asymétriques lorsqu'elles se développent à l'étranger.

D'une manière générale, ces entreprises peuvent être regroupées en cinq catégories :

- Les géants numériques diversifiés de la Chine, tels que les entreprises « BAT » (Baidu, Alibaba, Tencent) et Huawei. Ces entreprises mènent d'importantes activités dans le domaine de l'IA en Chine et à l'étranger. Elles utilisent l'IA dans toute une série de produits, qu'il s'agisse de services centrés sur l'IA, comme la reconnaissance vocale, ou d'autres domaines où l'IA est une composante moins omniprésente mais néanmoins vitale, comme les jeux, la banque, la logistique et la santé.
- Les grandes entreprises qui développent des technologies liées à l'IA dans le cadre de leur activité principale ont besoin d'un soutien de la part de l'État chinois pour développer leur gamme de produits. Parmi les exemples les plus marquants, citons iFLYTEK, qui se concentre principalement sur les applications de traitement du langage naturel, CloudWalk, qui se concentre sur la reconnaissance faciale, et Cambricon, qui développe des puces informatiques optimisées pour l'IA.
- Les grandes entreprises d'État qui fournissent les infrastructures nationales et les services d'information et de communication. La plupart de ces entreprises ont également leur propre secteur d'activité dans le domaine de l'IA. Elles opèrent dans des domaines tels que l'énergie, l'assurance, l'industrie manufacturière, les télécom-

[1] Le phénomène est général et ancien : https://www.annales.org/ri/2003/ri-decembre2003/fourel16-26.pdf

[2] https://foreignpolicy.com/2023/04/05/china-us-geopolitics-academia-university-partnership https://www.axios.com/2023/05/08/chinese-students-us-education

[3] Dans le cadre de travaux en cours du Core China Group sur la coopération en R&D faisant suite au sommet UE-Chine d'avril 2022, ainsi que par des dispositifs non ciblés sur un pays concernant le programme Horizon Europe. Ces éléments portent aussi sur le respect de la propriété intellectuelle et sur la réciprocité équilibrée des échanges.

munications et les transports. Citons par exemple State Grid China Railway Rolling Stock Corporation et China Telecom.

- Les entreprises technologiques étatiques ou liées à l'État, associées au secteur militaire et à l'industrie de l'armement. Les services de sécurité et les activités de recherche et de déploiement dans le domaine de l'IA. Citons par exemple Aviation Industry Corporation of China (AVIC), Datang Telecom, China Aerospace Science and Industry Corporation (CASIC), China Aerospace Science and Technology Corporation (CASC) et China Electronics Technology Group (CETC).
- Les *start-up* et les petites et moyennes entreprises actives dans toute une série de domaines de l'IA et des domaines d'application. Il est difficile d'obtenir des estimations fiables de leur nombre, compte tenu de la nature volatile des *start-up* et des lacunes en matière de données. En 2018, un rapport du gouvernement chinois a estimé que 2 167 petites et moyennes entreprises liées à l'IA avaient été créées. Ces entreprises – telles que Uisee, Tianrang et XYZ Robotics – reçoivent souvent des fonds d'amorçage et d'autres formes de soutien de la part des instituts de recherche chinois ou des entreprises d'État.

Le modèle d'entreprise hybride de la Chine

Les entreprises chinoises spécialisées dans l'IA sont des acteurs hybrides : elles fonctionnent comme des entités commerciales, mais sont soumises à l'influence, à l'orientation et au contrôle de l'État chinois.

La Chine ayant placé son industrie de l'IA au centre de l'innovation nationale, le gouvernement cherche à diriger le développement et le déploiement de l'IA en Chine, à gérer la concurrence entre ses entreprises et à assurer le contrôle de l'État, y compris lorsque les entreprises se développent à l'étranger. Les plans de la Chine en matière d'IA prévoient le développement d'« entreprises dorsales » de premier plan dans le domaine de l'IA à l'échelle mondiale.

Les entreprises d'IA bénéficient d'un financement, de préférences et d'un soutien substantiel de la part de l'État, et suivent les orientations du gouvernement central. Le gouvernement utilise les politiques industrielles – y compris les plans gouvernementaux, les projets, le financement, les préférences politiques, les alliances industrielles et les lois et règlements pertinents – pour façonner le comportement des entreprises.

En réponse aux exigences du PCC, les entreprises ont également des comités internes du Parti dont les membres ont souvent des rôles de cadres supérieurs ou de membres du conseil d'administration.

Le développement des Parcs industriels

Le gouvernement chinois utilise des zones technologiques et des parcs industriels pour promouvoir l'IA. Il a créé plusieurs zones pilotes, notamment à Pékin, Shanghai et Hefei, et vise à créer vingt zones de ce type d'ici 2023. Ces zones s'associent aux gouvernements locaux pour fournir des infrastructures, des financements et des incitations fiscales, et pour recruter des talents. Souvent, les zones disposent de leur propre véhicule d'investissement lié au gouvernement pour investir dans les entreprises d'IA. Les grands promoteurs immobiliers développent ces zones et investissent eux-mêmes dans les entreprises d'IA. China Evergrande en est un exemple.

La propriété intellectuelle

La propriété intellectuelle est un élément fondamental qui permettra aux entreprises chinoises spécialisées dans l'IA de développer des produits et des services et d'influencer la définition des normes. Baidu détiendrait le plus grand nombre de brevets liés à l'IA de toutes les entreprises ou instituts chinois.

Tencent, Huawei, Inspur, State Grid et l'université Tsinghua détiennent d'importants brevets dans le domaine de l'IA. Les entreprises chinoises spécialisées dans l'IA ont obtenu des brevets grâce à leurs acquisitions à l'étranger.

Septième principe du jeu de go : connecter des groupes de pierres

Alliances industrielles

Le gouvernement chinois a créé plus de 190 alliances industrielles dans le domaine de l'IA, dont l'Alliance nationale pour l'industrie et l'innovation technologique de l'IA en Chine (AIIA), qui comptait 567 membres en 2021. Ces alliances cherchent à harmoniser les travaux du gouvernement, des entreprises et des universités en matière de recherche, de normes, de propriété intellectuelle et de politique de l'IA.

Outre les principales entreprises chinoises spécialisées dans l'IA, ces alliances regroupent des entreprises publiques de télécommunications, des fournisseurs d'équipements et quelques entreprises étrangères. Les alliances régionales comprennent l'Alliance industrielle de l'IA de Pékin (BAIIA), dirigée par Baidu et comprenant d'autres grandes entreprises telles que ByteDance, Cambricon, BOE Technology Group, Didi Chuxing, Huawei, JD Com, Kuaishou, Megvii, Meituan, et 360 Vision.

L'alliance Shanghai AI promeut les applications chinoises de l'IA auprès des entreprises étrangères.

Les enjeux de normalisation

Les instituts gouvernementaux de recherche sur l'IA, tels que l'Institut de recherche sur les *big data* de Pékin et l'Académie d'intelligence artificielle de Pékin (BAAI), s'efforcent également d'harmoniser les efforts de la Chine en matière d'IA, de fixer des normes et de fournir des services d'aide à la décision à partir des données gouvernementales et de la puissance de calcul.

Les instituts travaillent en étroite collaboration avec les entreprises, les alliances et les organismes de recherche chinois dans le domaine de l'IA, tels que l'Académie chinoise des technologies de l'information et de la communication (CAICT) et l'Institut chinois de normalisation électronique (CESI).

La CAS joue un rôle de premier plan dans les alliances industrielles en matière d'IA, et l'Institut d'automatisation de la CAS (CASIA) mène des recherches qui sont commercialisées par les entreprises chinoises.

Alibaba et Baidu ont exploité les technologies vocales de la CASIA. Les applications de sécurité de l'État utilisent les technologies de vidéosurveillance intelligente et de reconnaissance faciale de la CASIA ; les entreprises pétrochimiques chinoises ont utilisé ses logiciels d'IA. La CAS possède aussi directement des entreprises d'IA, notamment Hanwang Technology (systèmes de surveillance électronique) et Sciample (équipements et systèmes de fabrication intelligents). La « licorne » de l'IA CloudWalkest est une entreprise dérivée de la CAS.

Les labels de « champion national » et « d'équipe nationale »

Le gouvernement chinois a désigné certaines entreprises comme « champions nationaux » dans des capacités et applications d'IA spécifiques.

Ainsi ont été désigné les entreprises « BAT » – Baidu, Alibaba et Tencent – et iFLYTEK comme chefs de file de ces plateformes nationales. Le gouvernement a chargé Baidu de se concentrer sur la conduite autonome, Alibaba de développer des plateformes pour les

applications des villes intelligentes, Tencent de développer des applications médicales et iFLYTEK de diriger les applications vocales et d'intelligence.

Quinze entreprises chinoises sont désignées comme faisant parties de l'équipe nationale d'IA de la Chine.

En affectant des entreprises à différents domaines d'application de l'IA, le gouvernement cherche à orienter l'activité commerciale vers ses priorités et à minimiser la concurrence qu'il considère comme faisant double emploi. En échange, ces entreprises reçoivent des fonds publics et des préférences politiques. Elles peuvent bénéficier du fait d'être les premières sur le marché et d'un statut de *leader* préférentiel ou protégé dans certains segments de marché qu'elles ont été appelées à développer. Renforçant le modèle de « plateforme ouverte », le gouvernement chinois a exigé en 2020 que ses champions nationaux de l'IA et d'autres grandes entreprises d'IA ouvrent leurs services propriétaires les uns aux autres afin de perturber les fiefs technologiques émergents et de maintenir le contrôle de l'État.

Les enjeux à l'export

Inciter les entreprises chinoises à aller à l'étranger

Les politiques chinoises encouragent les entreprises d'IA à « sortir » et à exploiter les capacités mondiales, et les entreprises chinoises d'IA ont bénéficié de manière significative de la recherche étrangère et des liens commerciaux et financiers. Leur présence mondiale croissante couvre la R&D, le recrutement et le développement de talents, le développement commercial, les investissements bilatéraux et les acquisitions de données, de technologies et d'entreprises.

Développement des entreprises par des acquisitions

Les entreprises chinoises spécialisées dans l'IA se développent rapidement à l'étranger et investissent dans des *start-up* étrangères. Il s'agit notamment de fabricants de matériel d'IA, tels que Huawei et Hikvision, et d'entreprises de services comme DiDi, qui détient une part importante du marché latino-américain du covoiturage.

L'Asie du Sud-Est est le premier et important marché étranger pour de nombreuses entreprises. Les algorithmes d'IA utilisés pour ces plateformes sont développés en Chine, et leurs organisations mères chinoises peuvent contrôler les opérations même si les opérations *offshore* sont censées être séparées.

L'exemple de Tencent

Tencent a réalisé des investissements dans l'application de paiement mobile Lydia et la banque B2B Qonto qui lui ont permis d'entrer sur le marché financier européen sans avoir à obtenir de licence. De même, Tencent est entrée en Amérique latine par le biais d'un investissement conjoint avec SoftBank dans la société fintech Uala, basée en Argentine.

Protéger son marché intérieur

Les obstacles à l'entrée des étrangers sur le marché chinois de la technologie – en particulier dans le domaine des logiciels et des activités liées à l'Internet – ont empêché de nombreuses entreprises et universités étrangères d'accéder aux possibilités offertes par la Chine, et ont obligé d'autres entreprises à s'associer à des institutions chinoises comme condition d'accès au marché.

Depuis 2020, le gouvernement a renforcé les contrôles et les protections dans le secteur de l'IA et les domaines technologiques et de données connexes. Le gouvernement a adopté

des lois qui limitent les exportations à double usage (par exemple, les exportations d'algorithmes) et exigent un examen plus approfondi des investissements étrangers et des transferts de données.

Viser une portée extraterritoriale

Ces mesures ont une portée extraterritoriale, ce qui suscite des inquiétudes quant à la capacité et aux intentions de la Chine de contrôler certains aspects des activités extraterritoriales de ses entreprises d'IA. Ces préoccupations alimentent les débats en dehors de la Chine sur la question de savoir si les entreprises chinoises devraient être exclues de certains marchés et activités liés à l'IA. Jusqu'à présent, cependant, une grande partie des activités chinoises d'IA *offshore* a échappé à l'examen des États-Unis et d'autres gouvernements, en partie parce qu'elles sont souvent structurées par des collaborations et des centres de recherche qui n'entrent pas dans le champ d'application actuel des autorités chargées de l'examen des investissements étrangers et du contrôle des exportations.

Les difficultés qui restent à surmonter

La pénurie des talents

Le 14e plan quinquennal de la Chine (2021-2025) incite les entreprises d'IA à établir des centres de R&D outre-mer et à recruter des talents étrangers. Les chercheurs des entreprises chinoises collaborent avec des scientifiques étrangers spécialisés dans l'IA et ont conclu des partenariats de recherche avec les meilleurs programmes universitaires mondiaux dans le domaine de l'IA.

De même, les liens entre les universitaires américains et les laboratoires d'entreprises en Chine développent les capacités chinoises en matière d'IA, y compris les talents. Dix pour cent des laboratoires de recherche en IA connus de Facebook, Google, IBM et Microsoft (considérés collectivement) étaient situés en Chine à la fin de 2020 (!)

> Le laboratoire Research Asia de Microsoft, basé à Pékin, est son plus grand laboratoire en dehors des États-Unis et a eu un impact énorme sur la capacité de la Chine à cultiver des « talents » en matière d'IA.

Le programme chinois des mille talents, géré par l'État, a attiré des milliers de scientifiques et d'ingénieurs en Chine entre 2008 et 2018, mais une étude a révélé que plus de 90 % des titulaires d'un doctorat en IA nés en Chine et formés aux États-Unis restaient aux États-Unis cinq ans après l'obtention de leur diplôme.

Les programmes d'État pour les talents chinois demandent aux chercheurs participants de « servir le pays » lorsqu'ils travaillent à l'étranger, ce qui peut impliquer le transfert de capacités vers la Chine.

L'attractivité des investisseurs

Les nouveaux atouts de la Chine en matière de production de données d'IA et d'adoption de technologies semblent également attirer les entreprises et les investisseurs américains. Pour s'assurer des partenariats étrangers, la Chine a proposé des financements, un accès aux données et des promesses d'accès futur au marché.

Les intérêts et le rôle de l'État impliquent des acteurs de la réglementation, des entreprises et des universités en Chine. Les récentes mesures prises par le gouvernement chinois pour renforcer le contrôle des données, des finances et des opérations *offshore*

de ses entreprises d'IA soulèvent des inquiétudes quant à l'influence de l'État sur les opérations mondiales des entreprises d'IA.

Les entreprises chinoises posent également des problèmes éthiques uniques, notamment l'utilisation par la Chine des capacités d'IA dans le pays et à l'étranger à des fins de surveillance, de propagande, d'espionnage et militaires.

Aussi certains hésitent aujourd'hui à investir dans l'IA en Chine.

La question des microprocesseurs

Les microprocesseurs restent le maillon faible de la stratégie chinoise concernant l'intelligence artificielle. Pour l'instant la Chine ne maîtrise pas suffisamment la technologie et reste très dépendante de ses approvisionnements à l'étranger. Les décideurs chinois reconnaissent la nécessité de disposer de semi-conducteurs avancés pour entraîner les algorithmes d'IA.

Le fait que le gouvernement américain ait restreint l'exportation de technologies de pointe dans ce domaine pose un problème à la Chine qui veut devenir moins dépendante de ses approvisionnements étrangers. Cela intensifie aussi les tensions sur Taiwan.

Elle essaie de développer son jeu sur ce terrain. Il y a de premiers résultats : les investissements massifs du gouvernement dans les semi-conducteurs ont rendu la Chine plus compétitive dans des segments de marché tels que la mémoire, les fonderies logiques à nœuds matures et la conception de puces sans usine.

Sur les autres segments de marché, c'est sans doute une question de quelques années…

Conclusion

La gouvernance numérique de la Chine est en pleine mutation, passant de la gouvernance avec la technologie numérique à la gouvernance sur la technologie numérique, puis à la mise en place d'un système de gouvernance de l'économie numérique.

La réintroduction de la pensée marxiste dans les relations internationales par la deuxième puissance économique et militaire internationale est un événement historiquement significatif.

Nous avons connu une période assez longue pendant laquelle le capitalisme et les théories néolibérales et démocratiques étaient considérés comme les mieux à même de répondre aux besoins des États et des sociétés. Pour la première fois depuis la fin de la guerre froide, cet état de fait est remis en question. Le marxisme est « de retour » dans une version 2.0, ayant été mis à jour dans une nouvelle condition que nous pourrions appeler « le marxisme numérique » dans laquelle les données (et de façon sous-jacente l'IA en tant que technologie exploitant les données) sont le nouveau facteur de production qu'il faut contrôler ! (pour mieux préparer la prochaine révolution).

Enracinée dans la théorie marxiste, la stratégie de la Chine numérique est à la fois profondément transformatrice et compétitive. Sur le plan interne, le contrôle habile des données par le parti créera la première « société intelligente » au monde, démontrant aux citoyens chinois et au reste du monde que le capitalisme n'a rien à offrir de plus que le socialisme. Sur le plan extérieur, la réussite de la stratégie de la Chine numérique ouvrira une ère d'innovation chinoise qui apportera un statut de grande puissance dans de multiples domaines stratégiques, civils et militaires. Bien qu'il s'agisse d'une tâche qu'ils décrivent comme monumentale, les dirigeants du parti sont convaincus que la Chine numérique est la stratégie qui permettra à la Chine de gagner l'ère numérique.

L'IMT au cœur de la stratégie nationale de souveraineté numérique

Par Francis JUTAND
Institut Mines Télécom (IMT)

La souveraineté a perdu sa connotation nationaliste pour émerger comme une nécessité dans l'agenda français et européen. Elle est une recherche d'autonomie par la capacité à choisir grâce à la maîtrise des sciences et technologies clefs, la capacité à construire des systèmes numériques complexes, et en étant acteur de l'écriture des règles mondiales qui organisent la concurrence, la sécurité et l'usage du *soft power*. La souveraineté industrielle de la France a été mis à mal par la mondialisation, la souveraineté européenne numérique court après la dynamique d'oligopoles mondiaux GAMAM et BAIDU.

L'IMT est au point nodal de la souveraineté, il forme les cadres de conception, d'ingénierie et de management pour porter la transformation numérique de l'économie et de la société et produit les connaissances sur les technologies, les architectures, la sécurité, les usages et la transformation des entreprises. L'IMT est source d'innovation au travers de l'accompagnement des entreprises et de l'incubation de *start-up*.

Cet article est rédigé sur la base de la stratégie d'ensemble 2023-2027 de l'Institut Mines Télécom (IMT) élaborée sous la responsabilité d'Odile Gauthier, sa directrice générale. Le montage de la priorité « souveraineté numérique » a été coordonné par Francis Jutand et Françoise Prêteux.

Introduction

La souveraineté a perdu sa connotation nationaliste pour émerger comme une nécessité dans l'agenda français et européen. Elle est une recherche d'autonomie par la capacité à choisir grâce à la maîtrise des sciences et technologies clefs, la capacité à construire des systèmes numériques complexes, en étant acteur de l'écriture des règles mondiales qui organisent la concurrence, la sécurité et l'usage du *soft power*. La souveraineté industrielle de la France a été mise à mal par la mondialisation, la souveraineté européenne numérique court après la dynamique d'oligopoles mondiaux GAMAM et BAIDU.

Les enjeux et risques de souveraineté liés à ce retard sont multiples : la dépendance stratégique des entreprises comme des organismes publics au titre de la cybersécurité et des risques « d'intelligence » ; la dépendance économique sur les infrastructures et les services ; la fragilisation de la démocratie (surveillance massive, captation des données personnelles, risque de développement des *infox* et manipulation) ; le risque de dépendance en termes de défense et de sécurité (il concerne l'espace, les *big data*, l'intelligence artificielle, le calcul à haute performance, la surveillance et le pilotage des armes intelligentes) ; les menaces sur la stabilité monétaire ou financière (illustrées par certaines applications des *blockchains* et les projets du type « Libra ») ; un risque de retard dans

les technologies pour répondre au défi climatique (développer les énergies renouvelables, implique des batteries et du logiciel, qui impliquent des technologies numériques, des nanotechnologies…) et enfin un enjeu culturel et de civilisation qui implique les normes éthiques, la production culturelle, les usages de l'intelligence artificielle (IA) et les problèmes liés à la fracture numérique.

L'accroissement des tensions géopolitiques tend par ailleurs à renforcer la préoccupation de compétition dans la souveraineté entre grandes puissances régionales mondiales, ce à quoi l'Union européenne et ses États membres ne peuvent rester indifférents.

Les missions et activités de l'IMT se situent au point nodal de la souveraineté, il forme les cadres de conception, d'ingénierie et de management pour porter la transformation numérique de l'économie et de la société et produit des connaissances sur les technologies, les architectures, la sécurité, les usages et la transformation des entreprises. L'IMT est source d'innovation au travers de l'accompagnement des entreprises et de l'incubation de *start-up*.

La souveraineté numérique

Les États-Unis ont porté la dynamique du numérique et assurent aujourd'hui un *leadership* économique, sociétal, militaire incontesté en ce domaine. La Chine percevant les dangers pour sa souveraineté a entrepris avec succès son rattrapage. L'Europe par manque de dynamisme industriel et du fait d'un moindre investissement en R&D que celui des États-Unis est restée pour l'essentiel sur ses bastions télécom et tente d'agir au niveau mondial en s'appuyant sur sa puissance de marché et ses capacités règlementaires.

Cependant la France et l'Europe ont exprimé depuis quelques années[1] la nécessité d'aller au-delà, et d'aborder sur le fond le problème de la souveraineté numérique.

« L'UE doit organiser l'univers numérique pour les vingt prochaines années » dit le commissaire européen au marché intérieur Thierry Breton.

« Notre souveraineté nationale dépend de notre capacité à construire notre souveraineté digitale, technologiquement, financièrement et industriellement » dit Bruno Lemaire avant que le gouvernement en place en mai 2022 n'ajoute au libellé du ministère de l'Économie et des Finances le titre de la Souveraineté industrielle et numérique.

« La souveraineté digitale doit aussi prendre en compte les fractures territoriales économiques et sociales du numérique » ajoute en sus Jean-Noël Barrot, ministre délégué à la transition numérique et aux télécommunications.

L'IMT, qui fédère huit grandes écoles en région, est riche d'environ 2 200 chercheurs, enseignants-chercheurs, ingénieurs de recherche, doctorants et post-doctorants ainsi que plus de 13 000 étudiants, est un acteur clef de la souveraineté numérique par ses activités de formation, de recherche technologique et industrielle, d'innovation et d'accompagnement du tissu économique au niveau national et territorial.

[1] Le 29 septembre 2017, un sommet des chefs d'États européens a été pour la première fois intégralement consacré au numérique, avec une volonté commune de faire de l'Europe une puissance numérique. Cela a donné des avancées sur les droits d'auteurs, sur les services audiovisuels, puis sur les intelligences artificielles lors des réunions de Tallin et Helsinki. L'organisation de la Commission suivant les élections européennes précédentes a conduit à donner à Thierry Breton un portefeuille qui couvre notamment cette priorité.

Un moment charnière dans l'histoire du numérique

Le numérique entre dans sa troisième phase de développement.

La première phase dans les années 1970 à 2000 a permis de construire la **convergence numérique des communications** autour des télécoms, de l'informatique et de la microélectronique. La dernière décennie étant marquée par l'arrivée des communications mobiles et du protocole IP pour l'acheminement de la voie et des données, et les microordinateurs comme interface intelligente. Elle a fait naître une forme d'*ubisphère* permettant d'accéder à un réseau de communication ubiquitaire.

La deuxième phase du numérique de 2000 à 2020 est celle de l'**internet**. Avec le *web*, elle est marquée par la création et l'échange de contenus numérique : données et vidéo, permis par les protocoles d'échange et la montée en puissance de traitement et débit des réseaux, puis par le développement des services délocalisés avec le *cloud*, et la naissance d'une interface intelligente et multifonction le « smart phone » ouvrant la porte au réseaux sociaux mobiles. Elle a fait naître une forme de *cybersphère* de systèmes d'information et base de connaissances se clippant sur l'*ubisphère*.

La troisième phase du numérique dans laquelle nous entrons est celle de la **transmutation numérique** de la société. Elle résulte de l'interpénétration des différents systèmes de communication, de traitement d'information et de commande, et de la création de nouveaux espaces de connaissances, de virtualisation et d'intelligence numérique. Cette évolution ouvre un champ de potentiels immense à explorer et à maitriser, tant pour la création des infrastructures numériques nouvelles, que pour l'organisation des services, et la coévolution des capacités humaines en interaction avec l'automatisation, l'intelligence artificielle et les coopérations intermédiées.

Cette troisième phase va enrichir les performances de l'*ubisphère*, densifier la *cybersphère* et créer ce que l'on pourrait appeler une *noosphère* autour de l'intelligence digitale et de la virtualisation.

La stratégie thématique et sectorielle de l'IMT

Un travail approfondi sur les besoins de la société et du monde économique, en termes de compétences, connaissances et ingénierie, ont conduit à mettre en avant dans la stratégie 2023-2027 de l'IMT dans ses activités de formation, de recherche et d'innovation, quatre domaines de compétences scientifiques et techniques : la transformation numérique, la transition écologique, la mutation industrielle et la santé, et pour chacun de prioriser un champ d'action intitulé : « Souveraineté numérique et sobriété », « Industrie du futur responsable », « Énergie et économie circulaire et société » et « Ingénierie pour la santé et le bien-être ».

Ils ne recouvrent pas l'ensemble des compétences et des expertises des écoles, mais organisent les thématiques sur lesquelles l'IMT rassemblé peut agir comme un acteur *leader* en France au niveau des technologies, des systèmes, des services et des connaissances, en jouant de l'expertise de ses chercheurs et des capacités à mener des initiatives et projets d'envergures, disciplinaires et interdisciplinaires associant innovation, performance et formation.

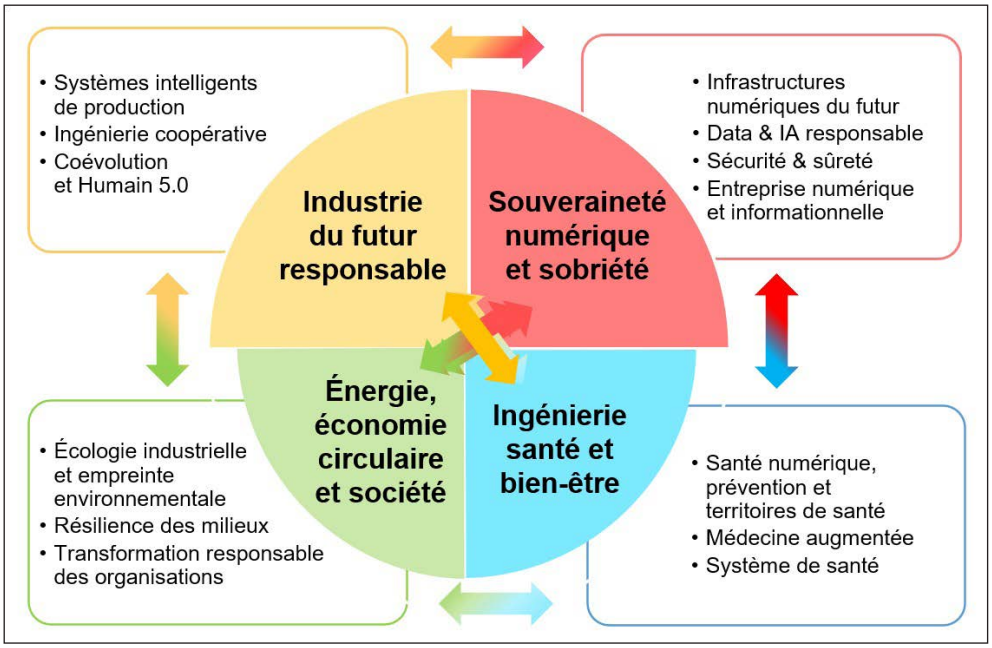


Figure 1 : Schéma de la stratégie 2023-2027 de l'IMT dans ses activités de formation.

La thématique stratégique « souveraineté numérique et sobriété »

Pour l'IMT, le concept de souveraineté numérique a été introduit en 2020 au lancement du travail stratégique. Sa pertinence a été validée par la nomination en 2022 d'un ministre délégué chargé de la transition numérique et des télécommunications auprès du ministre de l'Économie, des Finances et de la Souveraineté industrielle et numérique.

Quatre axes de travail ont été proposés dans une présentation préliminaire au conseil d'administration en mars 2021 et développés ensuite : infrastructures numériques, *datasphère*, sécurité, entreprise numérique et informationnelle.

Infrastructures numériques

Les infrastructures numériques sont entrées dans une phase de transformation profonde avec l'interpénétration des réseaux de transports d'information, des réseaux d'accès, des systèmes *cloud* de services, et des applicatifs sectoriels de commandes et contrôle. Cette évolution s'effectuant sur le fond d'une « softwarisation » accélérée des réseaux pour une commande ouverte ou partagée de l'utilisation des infrastructures matérielles de communication, de routage et de calcul. Les capacités nouvelles 5/6 G de communications permettent une augmentation des débits, une juxtaposition de réseaux spécifiques et des garanties de performances ouvrant la voie à la prise en compte de contraintes temps réel pour des applications critiques de commande et de contrôle.

Nous entrons dans une phase de récriture complète des infrastructures numériques, avec un élargissement sectoriel, une complexification liée à l'interpénétration, la définition de nouvelles architectures, le besoin de nouveaux outils de modélisation et méthodes d'exploitation. Et ce dans un cadre d'émergence de nouveaux acteurs enrichissant l'écosystème des opérateurs et équipementiers télécom et *cloud*.

La datasphère

Les données créent un espace miroir du fonctionnement des infrastructures de réseaux, des systèmes et services, ainsi que des usages et comportements. Elles sont la matière de sortes de doubles ou jumeaux numériques. Ils permettent d'analyser, de comprendre, de modéliser, de simuler, jusqu'à des pilotages en mode hybride, double numérique et fonctionnement physique.

Les recherches portent sur les capacités de traitement et d'échange fluide et sécurisé des données, les algorithmes distribués et répartis de calcul, les data sciences de modélisation et d'apprentissage.

L'IMT travaille aussi sur les conditions d'usage des données, leur mise en commun ou ouverture, les cadres juridiques et réglementaires de leur usage et la confiance des utilisateurs.

La *datasphère* contribue à la fois au développement de la *cybersphère*, et à l'émergence des technologies d'intelligence digitale.

La sécurité numérique

La sécurité s'entend principalement en termes de **sûreté** de fonctionnement des réseaux, des systèmes et des services, de **traçabilité** des échanges et interactions, de **cybersécurité** liée aux attaques malveillantes et de protection de la **vie privée**.

Les problématiques de sécurité numérique s'étendent du fait de la complexification des systèmes et services permise par le numérique, des interactions avec les problèmes de sûreté liés aux applicatifs des secteurs intégrant le numérique : réseaux d'énergie, de transport et d'eau, secteur hospitalier… S'y ajoutent des problèmes de traçabilité et de contrôles des automates et de l'usage de dispositifs d'intelligence artificielle pour la décision.

La cybersécurité doit elle aussi faire face à la complexification quantitative et qualitative des systèmes numériques, et l'élargissement des fronts : des systèmes critiques aux données personnelles et données d'entreprise. Il faut faire face à la montée simultanée en compétences des « *hackers* noirs » qui agissent individuellement ou collectivement dans l'anonymat pour voler des informations sensibles, causer des dégâts et commettre d'autres crimes et délits.

L'entreprise numérique et informationnelle

Il est dans l'ADN des écoles des Mines et Télécom d'être proches voire de travailler en osmose avec les entreprises. La métamorphose numérique est à l'œuvre dans la transformation des entreprises : technologies, chaînes de production des biens et des services, services de support et de soutien, compétences des collaborateurs, dispositifs de transaction et de coopération, gouvernance, missions et relations avec les parties prenantes.

Avec le numérique l'entreprise accélère dans ses évolutions vers un ensemble multidimensionnel de gestion de flux physiques et virtuels, de déstructuration des organisations de travail, de mobilisation de compétences internes et externes, de gestion des responsabilités sociétales de l'entreprise (RSE) et d'interactions coopératives avec ses parties prenantes. L'entreprise devient de plus en plus informationnelle.

Les écoles d'ingénieurs et la *business school* de l'IMT coopèrent pour mener les recherches et former les élèves sur l'entreprise informationnelle.

L'impact de l'IMT dans la politique numérique française et européenne

Depuis 2009 et son entrée dans l'Alliance Allistène, l'IMT (à l'époque Institut Télécom) est considéré comme un acteur national du numérique. Il a contribué à créer les principaux pôles de compétitivité numériques. Il est représenté depuis 2013 dans le Conseil national du numérique (CNN) et agit dans les filières industrielles du numérique.

Son impact est aujourd'hui manifeste pour les stratégies nationales d'accélération dans le domaine du numérique.

Dans le domaine de la recherche il est copilote du PEPR[2] 5G et Télécom du Futur, et impliqué au plus haut niveau dans les PEPR *Cloud*, Cybersécurité et IA. Il est un partenaire clef des projets nationaux 5G. L'IMT est membre fondateur de Gaia-X et membre résident du Campus Cyber.

Dans le domaine de la formation initiale et continue, l'IMT est lauréat de trois projets Compétences et métiers d'avenir (CMA) qu'il pilote : 5G+, cybersécurité et santé numérique qui complètent le projet Parcours de formation continue industrie et numérique.

Dans le domaine du soutien au développement économique : Diffusion des technologies innovation, création de *start-up*, accompagnement des PME. L'IMT a construit des plateformes de niveau international comme : *Open Air Interface* pour les réseaux mobiles, Tera Lab pour les données et l'IA, Arago pour les composants nano-optiques.

L'IMT pilote des chaires industrielles d'envergure : cybersécurité, data sciences et IA, communications numériques, *smart grid*, données personnelles et identités numériques, économie des communs de données.

Concernant l'innovation et la diffusion des technologies, l'IMT anime un réseau de douze incubateurs, est présent dans plusieurs e-DIH régionaux, développe des activités d'idéation avec ses élèves et les entreprises dans les week-ends « Tech The Future » ou dans des challenges innovation, et organise des bourses aux technologies pour le transfert des technologies matures.

L'IMT est un acteur clef de la souveraineté numérique

La souveraineté est affaire de travail collectif entre entreprises, programmes publics, et enseignement supérieur et recherche. L'IMT est un acteur de premier plan de l'écosystème académique numérique avec l'INRIA, le CNRS, le CEA et les Universités et présente des spécificités qui lui confèrent un rôle particulier.

L'IMT dépend du ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique, avec des missions de formation, de recherche et d'innovation et de soutien au développement économique.

Il fédère des écoles implantées sur les territoires à proximité du tissu économique et est un partenaire des collectivités locales.

Il est un des seuls grands acteurs nationaux à associer des activités de formation et de recherche, ce qui est particulièrement important en période de transition rapide dans laquelle il faut à la fois imaginer et développer les technologies et outils nouveaux et

[2] Programme et équipements prioritaires de recherche.

délivrer des formations initiales et continues de pointe pour les ingénieurs et chercheurs qui les développent et les portent.

Les écoles de l'IMT associent les entreprises aux évolutions en formation et recherche dans un écosystème enseignants-chercheurs-entreprises-élèves performant, pour l'innovation et le transfert vers l'ensemble du tissu économique.

La souveraineté ne se conquiert pas uniquement par l'excellence technologique et particulièrement dans le numérique où il faut maîtriser la complexité des algorithmes, des réseaux et des services, comprendre les champs d'usage et construire les infrastructures. De ce point de vue la capacité d'appréhender les interactions entre numérique, industrie, écologie est également un point critique, notamment pour la sobriété énergétique.

La force des élèves et leur désir de s'impliquer de plus en plus dans leur formation est également un atout fort pour prendre en compte leurs préoccupations écologiques et leurs projections d'avenir sur le sens de leurs métiers futurs. Nous sommes à un moment où il est plus que jamais nécessaire de penser l'avenir dans une approche large et inclusive avec l'ensemble des acteurs.

Enfin l'IMT traditionnellement ouvert à l'international pour la formation et la recherche, a inscrit dans sa stratégie une re-densification de ses actions européennes, une des clefs pour agir au niveau de la souveraineté qui doit associer les actions aux niveaux national, local et européen. Le programme européen de R&D Horizon Europe comporte en effet un *cluster* dédié au numérique et fortement doté, ainsi qu'un *cluster* sur la sécurité ; et au-delà le numérique est fortement intégré à d'autres *clusters*, sur le climat, l'énergie et les transports, sur la santé, sur l'alimentation. En outre les projets importants d'intérêt européen commun (PIIEC ou IPCEI) impliquent fortement des enjeux numériques (batteries, hydrogène…).

Conclusion

La souveraineté plus que jamais est l'objet d'affrontements au niveau mondial qui nécessitent la création d'entreprises françaises ou européennes de taille mondiale et travaillant en réseau avec un tissu de PME et ETI de pointes.

La bataille pour la souveraineté numérique est la mère des batailles car elle conditionne la souveraineté industrielle, militaire, éducative, culturelle, mais aussi écologique et géopolitique.

L'IMT est situé à un point nodal de l'écosystème de la souveraineté numérique. Son plan stratégique vise à **mobiliser** des ressources d'ensemble, personnels, enseignants chercheurs et élèves, **coopérer** au sein de ses réseaux de partenaires pour **innover** dans la recherche, **former** les compétences, **faire naître et croître** les entreprises nouvelles du numérique et **accompagner** les grandes entreprises et PME dans leur numérisation.

Europe : la souveraineté numérique au défi de l'autonomie technologique

Par Henri d'AGRAIN
Délégué général du Cigref

Le concept de souveraineté, et notamment dans le champ numérique, fait l'objet d'une utilisation sans cesse croissante dans l'espace public. Il est cependant bien souvent utilisé à tort et à travers et de façon peu propice à éclairer le débat sur les risques que nos pertes d'autonomie technologique font peser sur le continent européen et son économie. Cet article tente d'éclairer la notion de souveraineté numérique dans une première partie, de présenter dans une deuxième partie les principaux risques que ses dépendances technologiques font peser sur l'Europe, et enfin, dans une troisième partie, de tracer quelques perspectives sur les principaux leviers d'une politique de souveraineté numérique à l'échelle européenne.

La notion de souveraineté numérique fait l'objet depuis quelques années d'un usage débridé dans les acceptions les plus diverses, et souvent contradictoires. L'un des derniers avatars de l'usage fallacieux de cette notion nous est offert par Google Cloud, la filiale d'Alphabet qui commercialise ses services de *cloud computing*. Google Cloud définit la souveraineté numérique comme « la façon dont les organisations gardent le contrôle et leur autonomie à mesure qu'elles développent leurs stratégies de transformation numérique et de migration vers le *cloud*[1] ». Cette étonnante définition est donnée sur la page du site de Google Cloud qui propose aux entreprises un indicateur de leur « souveraineté numérique » afin de les inciter à exploiter ses technologies *cloud* pour répondre à leurs besoins supposés de protection de leurs données sensibles et de conformité aux législations européennes.

L'inadaptation du concept de « souveraineté numérique » ?

Nous observons que, de façon répétitive, les concepts de souveraineté, d'autonomie, d'indépendance et de confiance sont mobilisés, à tour de rôle, pour caractériser le numérique, en ne donnant que très rarement une définition claire de ceux-ci. Et nous pensons que, dans bien des cas, cette confusion est entretenue à dessein, la plupart du temps par inconsistance intellectuelle, parfois par évitement de ses propres responsabilités en la matière, et très souvent pour masquer des velléités de protectionnisme économique. Un conférencier expliquait récemment, s'exprimant sur le thème de la souveraineté numérique européenne, qu'aucun pays ne peut se considérer comme souverain puisqu'aucun d'eux ne peut prétendre à la pleine autonomie et indépendance technologique, notions qu'il semblait par ailleurs confondre avec celle d'autarcie. Cette aporie tant sémantique que

[1] https://cloudsovereignty.withgoogle.com/fr/questions/

conceptuelle jette une lumière crue sur les différents biais qui grèvent le débat autour des concepts de souveraineté, d'autonomie, et d'indépendance. La confusion apparaît totale et contrainte par de multiples arrière-pensées qui ne rendent service à personne. Nous savons que l'autarcie numérique, pour notre continent, pour les États européens, pour le fonctionnement de la société, de son économie et de ses entreprises, est une chimère. Ceux qui la prônent, ou qui font mine de penser qu'une telle hypothèse est crédible, sont au mieux des irresponsables, et parfois de dangereux cyniques dès lors qu'ils se trouvent en situation de responsabilité.

Rappelons-le, la souveraineté est un attribut exclusif des États, et il appartient aux seuls États de mettre en œuvre des politiques de souveraineté. Dans sa définition la plus orthodoxe, la souveraineté est le pouvoir suprême reconnu à l'État, qui implique l'exclusivité de sa compétence sur le territoire national, et son indépendance dans l'ordre international où il n'est limité que par ses propres engagements. Il n'y a pas de raison de retenir une définition différente de la souveraineté sous prétexte que l'on parle de numérique. Cette définition de la souveraineté numérique n'embarque aucune notion d'indépendance ou d'autarcie. Elle implique en revanche que l'État dispose de son autonomie d'appréciation, de décision et d'action pour choisir ses dépendances et les moyens de les maîtriser. Cette définition de la souveraineté n'a pas lieu d'être modifiée dès lors que l'on évoque l'Union européenne. En effet, le États européens peuvent décider souverainement – les Britanniques nous l'ont démontré par l'absurde – de déléguer aux institutions de l'Union, pour les mutualiser, des politiques de souveraineté, comme ils l'ont fait dans de nombreux domaines, et notamment dans le champ numérique.

Par ailleurs, et comme l'explique Théodore Christakis[2] avec une grande clarté, ce concept de souveraineté numérique, appliquée à l'échelle européenne, revêt un certain degré d'ambiguïté. D'une part, le concept de souveraineté numérique n'a pas beaucoup de sens d'un point de vue purement normatif, le terme de souveraineté étant l'un des plus équivoques de la théorie juridique. Mais, d'autre part, et d'un point de vue politique, le concept de souveraineté numérique européenne est particulièrement efficace. Théodore Christakis montre que l'Union européenne a acquis une puissance mondiale en matière de réglementation numérique. Il explique ce phénomène par « l'effet Bruxelles ». L'Union européenne s'est effectivement imposée comme un *hégémon* international de la réglementation, sans équivalent chez ses rivaux géopolitiques.

L'Union européenne en effet, dans le champ numérique, est confrontée à deux préoccupations structurantes qui s'expriment dans sa démarche législative. D'une part, elle doit exiger des acteurs qui agissent dans ce champ, au premier rang desquels les géants technologiques nord-américains, mais également chinois, de respecter un référentiel normatif qui traduit les valeurs de notre continent. D'autre part, elle tente de créer les conditions d'une restauration de son autonomie technologique. Celle-ci, malgré de nombreuses déclarations d'intention, et des efforts à l'évidence insuffisants, a été, depuis une vingtaine d'années, négligée de façon tout à fait inconsidérée.

Nous proposons donc, en conclusion partielle de ce propos, de considérer que le concept de souveraineté est inadapté pour qualifier les rapports qu'une organisation, autre qu'un État, entretient avec son environnement, même s'il peut être sollicité pour caractériser les transferts relatifs de responsabilité que les États eux-mêmes consentent à des organisations supranationales, comme l'Union européenne. En toute rigueur de terme, parler de souveraineté pour une entreprise ou pour un produit n'a, finalement, guère de sens. Dans ce contexte, l'usage du terme de souveraineté est en général une facilité pour exprimer les enjeux de maîtrise des différentes dépendances, notamment étrangères, auxquelles les entreprises, de toute taille et de tout secteur d'activité, sont normalement soumises.

[2] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3748098

Europe : un triple risque systémique

En corollaire, nous faisons, sans surprise et sans originalité, le constat préoccupant des abandons successifs d'autonomie technologique de l'Europe, et de la dépendance croissante qui en découle, pour nos États et pour nos entreprises, vis-à-vis des *leaders* technologiques, américains aujourd'hui, et sans doute chinois demain. Le poids des trois principaux *hyperscalers* américains n'a fait que croître sur le marché européen au cours de ces dernières années. En 2017, Microsoft, AWS et Google Cloud concentraient déjà, en Europe, environ 60 % de parts de marché. Aujourd'hui, ces même MAG[3] préemptent plus de 70 % de ce marché, laissant aux opérateurs européens à peine 10 % de celui-ci. Ne nous y trompons pas : le *cloud* n'est pas, ou n'est plus, un sous-domaine du numérique. C'est celui qui commande désormais tous les autres. Comme la crise sanitaire l'a concrètement montré, les données sont au cœur de la transformation numérique, et le *cloud* est, à présent, un socle incontournable pour nos entreprises et nos administrations publiques. Par ailleurs, quasiment tous les champs de l'innovation et de la transformation numérique utilisent les environnements et les outils du *cloud*. *Big Data*, intelligence artificielle, calcul haute performance, réseaux télécom de nouvelle génération, informatique quantique, ces nouveaux territoires du numérique se développent dans les espaces, et avec la puissance de calcul et de stockage, que leur apporte le *cloud*. Si l'Europe ne parvient pas à s'organiser pour maîtriser ses dépendances numériques, notamment sur le marché du *cloud*, si les démarches qu'elle a engagées, en matière législative et en termes d'investissement, ne produisent pas les effets escomptés à court terme, son économie sera confrontée, à l'horizon de la fin de la décennie, à trois risques systémiques qui ne cessent de se renforcer.

Le premier est un risque géostratégique. Nul ne peut prétendre aujourd'hui caractériser la qualité de la relation entre l'Union européenne et les États-Unis à l'horizon des deux prochaines administrations américaines. Que se passerait-il en cas d'entrave de nature politique sur l'accès de l'Europe aux ressources des *cloud providers* américains, lesquels préemptent plus de 70 % du marché continental, ces entraves ciblant une entreprise, un secteur d'activité, un État voire l'ensemble de l'UE ? Des précédents existent dans de nombreux domaines. Nous serions bien inspirés de ne pas oublier qu'un désalignement des intérêts entre membres de l'alliance transatlantique, même conjoncturel, est toujours possible et peut se traduire par des sanctions d'acteurs européens portant sur leur usage des technologies numériques. Et dans ce domaine des services *cloud*, ce qui vaut pour les opérateurs américains est transposable aux opérateurs chinois, même si leur surface est encore faible en Europe.

Le deuxième risque est de nature économique. À l'horizon de la fin de la décennie, et compte tenu de la dynamique du marché mondial du *cloud*, la majeure partie des processus métiers les plus essentiels des entreprises européennes, voire des administrations publiques, pourraient être enfermés dans les solutions proposées par des contrôleurs d'accès de services *cloud*. Cette situation pourrait susciter chez ces derniers la tentation de valoriser cette position de grande dépendance, dans laquelle ils auront verrouillé leurs clients, en faisant évoluer leurs modèles de rémunération. Cette mise sous tutelle de secteurs d'activité de plus en plus nombreux permettrait à ces tuteurs de préempter une part croissante de la valeur créée par l'économie européenne, et devenir rapidement insoutenable. En d'autres termes, pour les activités européennes les plus consommatrices de ses services, le *cloud* public pourrait être le pendant numérique de la doctrine « sans usines ou *fabless* en anglais » de funeste mémoire, dès lors que les nouvelles usines de production informatiques, en l'absence d'alternative sur notre continent, sont détenus par des acteurs non européens.

[3] MAG : Microsoft, Amazon Web Services, Google Cloud.

Le troisième risque, enfin, d'ordre juridique, est d'ores et déjà une réalité. Il s'agit de la dépendance de l'Europe et de son économie à des législations non européennes à portée extraterritoriale, comme l'arrêt du 16 juillet 2020 de la CJUE l'a justement mise en exergue. Que ce soit, par exemple, la section 702 du *Foreign Intelligence & Surveillance Act* américain, pointé par la CJUE, ou la loi chinoise du 28 juin 2017 sur le renseignement national, ces législations autorisent les agences de renseignement de ces États à réaliser, légalement et secrètement, une collecte massive, *a priori* et sans mandat judiciaire, des données des personnes morales ou physiques étrangères dès lors que celles-ci, et les traitements associés, sont hébergés par leurs opérateurs nationaux normalement soumis à ces législations. Ces législations sont largement mobilisées, notamment par les États-Unis, pour déployer, de façon secrète mais légale, une intense activité d'intelligence économique avec des capacités technologiques jamais égalées dans l'histoire du renseignement américain.

Des réponses nécessairement politiques

Pour répondre à ces défis systémiques auxquels le numérique confronte nos États européens, l'économies continentale et l'ensemble de la société, l'Union européenne doit apporter des réponses de nature politique. Dans ce domaine du numérique, comme dans les autres domaines nous semble-t-il, les politiques de souveraineté doivent se développer, à l'échelle du continent comme de chacun des États de l'Union, en articulant de manière cohérente et coordonnée les trois principaux leviers auxquels elles ont accès.

Le premier levier est celui du législatif et du réglementaire, et l'Europe bénéficie depuis quelques années d'une efflorescence en la matière qui donnera à certains l'illusion qu'ils peuvent s'affranchir de travailler sérieusement sur les deux autres leviers.

Le deuxième levier est celui de l'investissement public. À l'évidence, tant au niveau national qu'européen, les mécanismes mis en œuvre et les montants mobilisés ne sont pas à la hauteur des besoins d'une restauration, tant qualitative que quantitative, de l'autonomie technologique de notre continent, notamment dans le domaine des microprocesseurs, du *cloud computing*, de l'intelligence artificielle ou de l'informatique quantique. Soyons honnêtes, ce ne sont pas les moyens qui manquent, mais la volonté politique de réaliser des arbitrages ambitieux, de long terme et probablement incompatibles avec les attentes d'une opinion publique peu informée des enjeux numériques pour notre continent et des risques que nos dépendances technologiques font courir à notre avenir commun.

Le troisième levier, enfin, sur lequel nous souhaitons appeler tout particulièrement l'attention des lecteurs, car il nous semble plus compliqué à actionner à l'échelle européenne notamment en raison de ses propres engagements dans le cadre de l'Organisation mondiale du commerce, est relatif à la commande publique. Chacun observera que la puissance considérable acquise par les *hyperscalers* américains s'est significativement nourrie, au cours des dix ou quinze dernières années, de la commande publique de l'État fédéral des États-Unis d'Amérique et de ses grandes agences. À titre d'exemple, Amazon Web Services maintient sa position de *leader* dans les services *cloud*, avec une part de plus de 30 % du marché mondial et européen, position acquise en 2013 lorsque la société a gagné le marché de *cloud computing* de la CIA pour un montant, record à l'époque, de 600 millions de dollars. Il nous apparaît dès lors indispensable que la commande publique des États européens, mais également celle des administrations et collectivités publiques, des opérateurs de réseaux et de services publics soumis à des obligations réglementaires analogues, puissent être mobilisées et orientées en fonction des besoins exprimés, de manière simple et sans entrave excessive, vers une offre plurielle articulant, d'une part, les services proposés par les grands *hyperscalers*, dès lors que les conditions de sécurité sont réunies, et, d'autre part, les services de confiance des opérateurs européens de *cloud*.

Un tel dispositif pourrait être opéré par une agence européenne, à l'image de ce que notre continent a su faire pour l'acquisition de vaccins anti-Covid. Il constituerait un signal fort en direction du marché du *cloud* et de ses clients publics et privés.

Conclusion

Les entreprises, publiques et privées, et les administrations expriment en effet un besoin croissant de produits et services numériques de confiance. Le Cigref a défini les principaux critères de confiance appliqués au numérique. Ils s'articulent autour de quatre axes : la sécurité des données et des traitements sensibles, l'immunité des données et des traitements aux législations non européennes à portée extraterritoriale, la maîtrise de la dépendance des utilisateurs vis-à-vis de leurs fournisseurs de produits et services numériques, et enfin la maîtrise de l'empreinte environnementale et énergétique du numérique, de ses infrastructures et de ses usages. Ces critères de confiance appliqués au numérique sont cohérents, dans une large mesure mais sans se confondre avec eux, avec les enjeux de souveraineté numérique portés tant par la France que par l'Union européenne.

Dans le contexte actuel d'accélération de l'histoire numérique de l'humanité, l'autonomie stratégique à laquelle la France aspire pour l'Europe, et qui commence à porter ses fruits en termes de conviction auprès de nos partenaires, appelle une accélération d'un ordre supérieur dans le champ technologique et numérique, sans quoi la dystopie glaçante de la vassalisation de notre continent pourrait devenir une réalité à plus ou moins long terme. Nous ne pouvons nous y résoudre pour notre génération, et encore moins pour celle de nos enfants.

Retrouver des leviers de souveraineté dans le cyberespace grâce à une meilleure organisation des missions dans le champ de la cybersécurité

Par Hugo ZYLBERBERG
Chef d'État-Major de la sous-direction Stratégie de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)

Dans un environnement cyber désormais caractérisé par l'instabilité numérique, il est essentiel de retrouver des leviers d'action pour mieux prendre en compte le risque cyber à tous les niveaux des organisations. À cet effet, l'organisation de l'État semble utile pour identifier des fonctions prioritaires et des objectifs stratégiques qui permettent de répondre concrètement à ces enjeux majeurs de cybersécurité.

Introduction

La transformation numérique des dernières décennies plonge les organisations publiques et privées dans un environnement nouveau : après une longue période de développements numériques tous azimuts, le risque cyber qui caractérise désormais l'environnement numérique les force à s'intéresser à leur cybersécurité.

Dans ce contexte de plus en plus marqué par l'instabilité numérique où de grandes cyberattaques font régulièrement l'actualité, les dirigeants s'intéressent de plus en plus fréquemment et intensément aux risques cyber. Dans les *Global Risks Report* annuels du World Economic Forum[1], le risque cyber est par exemple mentionné comme l'un des risques majeurs en 2012 puis en 2014, avant d'être systématiquement mentionné depuis 2019.

Cependant, cette rapide transformation numérique peut donner la sensation de manquer de leviers d'action pour traiter ces risques. Dès 2014, Pierre Bellanger écrit ainsi « nous sommes à cet instant le garde-manger, le minerai numérique ou encore l'éventuel champ de bataille » des puissances numériques[2], un rôle essentiellement passif où les leviers d'action appartiennent à d'autres acteurs. Pourtant, les leviers de gouvernance et de décision dont disposent les dirigeants n'ont pas miraculeusement disparus : ils doivent être adaptés à l'ère cyber – voire remplacés par de nouveaux lorsqu'ils sont devenus obsolètes.

[1] Voir par exemple l'édition 2023 du WEF Global Risks Report accessible en ligne : https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

[2] BELLANGER P. (2020), « Trois empires et un garde-manger », *Le Débat*, vol. 209, n°2, pp. 57-64.

Le risque cyber et ses caractéristiques

Description de l'environnement de risque cyber

L'environnement numérique se caractérise par son instabilité. Selon le baromètre annuel du Club des experts de la sécurité de l'information et du numérique (CESIN), « plus d'une entreprise sur deux considère toujours que le niveau de menaces en matière de cyber espionnage est élevé (50 %) »[3]. L'impact du risque cyber dépend cependant de la taille de l'organisation qui en est victime. L'Association pour le management des risques et des assurances de l'entreprise (AMRAE) indique que les entreprises de taille moyenne ont déclaré des sinistres à hauteur de 4,5 millions d'euros en 2022, un chiffre qui a presque doublé par rapport à une enquête similaire réalisée en 2021. Pour les plus petites entreprises, la situation est probablement du même ordre, même si les chiffres manquent pour venir étayer cette situation. Plus globalement, les assureurs ont encaissé 316 millions d'euros de primes dédiées à la couverture des risques numériques en France, soit un bond de 72 % par rapport à 2021[4].

En outre, à l'inverse d'autres catégories de risques accidentels pour lesquels il est possible de bénéficier de modélisation afin de les rendre plus prévisibles, le risque cyber est par nature stratégique : un acteur malveillant se trouve de l'autre côté du clavier, et tente de faire réussir l'attaque. Pour se défendre, il est donc nécessaire de se prémunir de toutes les attaques qu'il peut concevoir – alors que pour l'attaquant, une seule faille est suffisante.

La prise en compte du risque cyber dans les organisations

Pour y faire face, les stratégies de gestion des risques commencent nécessairement par leur identification : quels sont les risques cyber majeurs auxquels je dois faire face, et comment puis-je y répondre ? Afin de caractériser ces risques cyber, la méthode EBIOS RM[5] propose deux composantes : une source de risque et un objectif visé.

La source de risque est définie comme un « élément, personne, groupe de personnes ou organisation susceptible d'engendrer un risque ». Une source de risque peut être caractérisée par sa motivation, ses ressources, ses compétences, ses modes opératoires (de prédilection). À titre d'exemple, des groupes criminels, des services étatiques, des concurrents ou des employés internes peuvent tous être considérés comme des sources de risque. L'objectif visé est la finalité de l'attaque : par exemple obtenir le paiement d'une rançon, obtenir des informations privilégiées à des fins d'espionnage industriel, exercer une vengeance…

Pour identifier des risques, la méthode EBIOS RM permet d'abord d'identifier des scénarios stratégiques d'attaque : qu'est-ce qu'un attaquant pourrait vouloir attaquer ? L'objectif de cette première étape est de comprendre ce que des attaquants pourraient vouloir attaquer. Une entreprise de services numériques pourra par exemple vouloir préserver la confidentialité des informations de ses clients, alors qu'une entreprise de biotechnologies pourra s'attacher davantage à l'intégrité de ses données de recherche. Dans tous les cas, le risque opérationnel portant sur la continuité d'activité peut consti-

[3] L'édition 2022 du baromètre du CESIN est accessible en ligne : https://www.cesin.fr/articles-slug/?slug=1432-8%C3%A8me%20%C3%A9dition%20du%20barom%C3%A8tre%20annuel%20du%20CESIN

[4] L'édition 2023 de l'étude LUCY - Lumière sur la cyberassurance est accessible en ligne : https://www.amrae.fr/bibliotheque-de-amrae?combine=&ref_id=4626&ref_type=publication&items=4626

[5] Les documents relatifs à la méthode EBIOS RM sont disponibles en ligne : https://www.ssi.gouv.fr/guide/la-methode-ebios-risk-manager-le-guide/

tuer une cible privilégiée des attaquants car cela leur permet de demander une rançon aux victimes afin de pouvoir redémarrer leur activité.

Une fois ces risques identifiés, il s'agit de trouver des leviers d'action permettant soit de réduire leur probabilité d'occurrence, soit de réduire leur impact lorsqu'ils surviennent. S'il existe des modèles permettant aux organisations de mesurer leur maturité ou leur niveau de cybersécurité, il n'existe pas encore de modèle général d'organisation des activités relatives à la cybersécurité des organisations.

Afin de gérer leurs risques cyber en mettant en œuvre une stratégie, les dirigeants doivent donc répondre à la question suivante : comment concevoir et gouverner les leviers d'action dont disposent les organisations pour maîtriser leurs risques cyber ?

De quels leviers d'action disposent les organisations pour répondre à ce nouvel environnement de risque cyber ?

L'organisation de l'État pour assurer ses missions dans le champ de la cybersécurité permet d'éclairer les différents leviers dont disposent les organisations. Les travaux de la *Revue stratégique de cyberdéfense* de 2018 ont en effet abouti à la définition de plusieurs missions, et à la création d'un ensemble d'instances qui forment la gouvernance cyber de l'État en matière de lutte informatique défensive.

Cette gouvernance cyber recouvre désormais trois champs d'action prioritaires qui font chacun l'objet d'une comitologie dédiée :

- l'amélioration du niveau de cybersécurité de l'État ;
- la prise en compte des enjeux de sécurité numérique dans les politiques publiques ;
- la réponse aux agressions.

Transposés aux organisations publiques comme privées, ces trois champs d'action offrent une structure qui permet de catégoriser et d'identifier les leviers d'action à la disposition de leurs dirigeants.

L'amélioration du niveau de cybersécurité

Ce premier champ d'action concerne autant les mesures de cybersécurité mises en place au sein des infrastructures numériques que les outils et les services spécifiquement dédiés à la cybersécurité. Il s'agit donc d'une part d'exigences vis-à-vis des équipes qui déploient et maintiennent le système d'information et d'autre part de ressources informatiques en propre destinées à assurer la cybersécurité de l'organisation. La sécurité de la chaîne d'approvisionnement matérielle et logicielle des organisations constitue en particulier un point d'attention majeur pour maîtriser ses dépendances et obtenir une compréhension de son environnement de risque la plus fidèle possible.

L'objectif de ces activités est de parvenir à identifier les éléments les plus sensibles au sein d'un système d'information parfois tentaculaire et de définir une stratégie permettant d'atteindre un niveau de sécurité suffisant pour prévenir les risques au sein du système d'information.

La prise en compte des enjeux de sécurité numérique dans les projets

Ce second champ d'action concerne l'intégration de la sécurité dans les projets de l'organisation et la sensibilisation des métiers au risque cyber. Il s'agit donc de définir un

processus par lequel les projets doivent anticiper, prendre en compte et répondre à leurs propres risques de cybersécurité.

L'objectif de ces activités est de parvenir à anticiper les nouveaux risques que les projets issus des métiers peuvent occasionner et de conseiller les porteurs de projets pour leur permettre d'y répondre.

La gestion des incidents de cybersécurité

Ce troisième champ d'action concerne la réaction d'une organisation face à ses incidents de cybersécurité. Il s'agit donc de parvenir, le plus rapidement possible, à lever le doute concernant les incidents en cours et d'en limiter la durée et l'impact.

L'objectif de cette troisième activité est de mettre en place des processus d'escalade permettant d'éviter que les incidents ne se transforment en crise et de gérer les crises qui doivent l'être.

Chaque champ d'action constitue ainsi une fonction qui peut être confiée à différentes personnes au sein d'une organisation mais sans laquelle la prise en compte des risques cyber sera insuffisante.

Conclusion

La stratégie cyber de grandes organisations pourrait utilement s'appuyer sur cette structure afin d'effectuer un diagnostic des missions, rationaliser leur gouvernance et fixer des objectifs qui permettent de retrouver des leviers d'action dans le cyberespace. Cependant, cette prise en compte se heurte à un autre obstacle : celui des talents.

Selon certaines études[6], le secteur de la cybersécurité (estimé à plus de 4,5 milliers de personnes en 2022), manquerait encore de près de 3,5 milliers de professionnels. Pour la France, l'Observatoire des métiers de la cybersécurité de l'ANSSI a publié en 2022 une étude sur l'attractivité et la représentation des métiers de la cybersécurité[7]. Il reste cependant beaucoup à faire pour favoriser la croissance d'un écosystème de formations, techniques et non techniques, initiales et continues, qui attirent une diversité de profils afin de garantir qu'outre une bonne organisation des missions de cybersécurité, ces missions soient attractives et pourvues pour faire face à cet immense défi.

[6] Voir par exemple le Cybersecurity Workforce Study de (ISC)² accessible en ligne : https://www.isc2.org/-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx

[7] L'enquête 2022 de l'Observatoire des métiers de la cybersécurité de l'ANSSI est accessible en ligne : https://www.ssi.gouv.fr/uploads/2021/10/20221115_observatoire_enquete_2022.pdf

Pourra-t-on tendre vers une souveraineté quantique ?

Par Alice PANNIER
Responsable du programme Géopolitique des technologies
à l'Institut français des relations internationales (Ifri)

Les sciences et technologies de l'information quantiques sont un champ vaste qui inclut notamment l'informatique, les télécommunications, la détection et les capteurs, avec une grande diversité de domaines d'application. L'ensemble de ces technologies promettent d'enclencher des ruptures dans nos systèmes d'information. Les avancées significatives des technologies quantiques ces dernières années et leurs implications en termes de sécurité et en termes économiques notamment, ont entraîné un réel élan dans l'intérêt des gouvernements, y compris en Europe.

Malgré les avancées impressionnantes des deux géants que sont la Chine et les États-Unis, et contrairement à la plupart des autres technologies numériques, l'Europe (au sens géographique) est bien placée dans la course mondiale aux technologies quantiques. Sur ces bases prometteuses, l'Europe peut-elle espérer atteindre la souveraineté technologique dans le quantique ? Deux défis, notamment, se posent : d'une part, concilier objectif de souveraineté et coopération internationale, et d'autre part, parvenir à ancrer toute stratégie pour le quantique dans une perspective holistique et de long terme.

Les technologies quantiques et leurs implications en termes de souveraineté

Les technologies quantiques : la promesse de ruptures

Les sciences et technologies de l'information quantiques sont un champ très vaste qui inclut notamment l'informatique, les télécommunications, la détection et les capteurs, avec une grande diversité de domaines d'application. Chacun de ces champs promet, à plus ou moins brève échéance, d'enclencher des ruptures dans nos systèmes d'information et de communication – ruptures stratégiques et économiques qui présentent autant d'opportunités que de menaces.

Les technologies de télécommunication quantiques tirent avantage des propriétés de la physique quantique (« l'intrication » des particules) en vue de transmettre des messages de façon sécurisée. Si des défis techniques persistent à ce jour pour permettre la transmission de messages sur une très longue distance et/ou à vitesse rapide, par des câbles de fibre optique ou par des satellites, cette technologie promet des avancées spectaculaires dans la sécurité des communications et peut-être un jour par l'avènement d'un internet quantique.

Un deuxième pan des technologies de l'information quantiques concerne la détection et les capteurs, avec des applications dans le champ militaire notamment. La sensibilité des capteurs quantiques pourrait par exemple permettre d'identifier des installations

nucléaires souterraines, là où des radars quantiques pourraient déjouer la furtivité des aéronefs et résister à des formes avancées de brouillage. Dans un autre domaine, les gravimètres quantiques pourraient considérablement améliorer la précision des forages en détectant les fluctuations de densité qui indiquent la présence de gisements de pétrole ou de minéraux.

Enfin, l'informatique quantique est sans conteste le domaine avec le plus large spectre d'applications, et donc les implications les plus grandes. En dépassant les limites physiques inhérentes aux ordinateurs classiques, l'informatique quantique, promet un changement radical d'échelle dans la puissance de calcul, la multipliant potentiellement par un milliard d'ici cinq ou dix ans. Différentes technologies de processeurs quantiques sont actuellement en phase d'expérimentation dans les laboratoires de recherche et *start-up*, reposant notamment sur la photonique ou les matériaux supraconducteurs. En fonction des types de processeurs développés, l'émergence de l'informatique quantique s'accompagne donc aussi d'avancées dans d'autres domaines scientifiques et technologiques : les nanotechnologies, la cryogénie, la science des matériaux, les lasers, etc.

La simulation complexe constituera probablement une part essentielle de l'utilisation des ordinateurs quantiques, avec des usages en médecine, ou dans l'agriculture. Les ordinateurs quantiques pourront également être utiles pour l'optimisation de tâches, nécessaires aux véhicules autonomes comme pour la gestion de la consommation énergétique dans le contexte de l'électrification. L'informatique quantique sera aussi particulièrement adaptée à des tâches de factorisation, utile pour le décryptage de clé de chiffrements, avec des implications massives en termes de cybersécurité.

Implications pour la souveraineté européenne

Ces différents champs des technologies quantiques ont connu des avancées significatives au cours des cinq dernières années – des avancées plus rapides, en fait, que ce qui avait été envisagé. Leurs implications en termes de sécurité et en termes économiques notamment, ont entraîné un réel bond dans l'intérêt des gouvernements pour le développement de technologies nationales.

Le contexte de compétition technologique entre les États-Unis et la Chine – dans lequel se déroulent ces avancées technologies, est ici significatif. Cette compétition exerce une pression sur l'ensemble des acteurs cherchant à développer ou accéder à des technologies quantiques, entre course de vitesse et course d'obstacles. Les technologies chinoises se développent dans un écosystème de recherche sous contrôle étatique, et sur lequel on a une visibilité limitée, notamment en termes de financements publics (Julienne, 2022). Côté américain, la volonté de freiner les développements technologiques chinois, à l'aide de restrictions au commerce des technologies, a des effets y compris sur l'Europe (Velliet, 2022).

Par ailleurs, le développement de technologies quantiques doit s'accompagner de travaux sur les normes techniques (matériels, mesure de la performance des machines, protocoles de chiffrement, langages de programmation et logiciels) et les normes internationales en ce qui concerne leurs usages, notamment les usages militaires. À défaut d'être proactifs dans la définition de ces normes, les États et entreprises devront subir les normes imposées *de facto* par les premiers entrants. Une coordination internationale sur ces normes paraît nécessaire, mais le contexte international marqué par la compétition entre grandes puissances y est défavorable, ce qui renforce d'autant les arguments en faveur de technologies « souveraines ».

Face à ces risques et incertitudes, l'ancienne ministre des Armées, Florence Parly, avait en effet estimé que les technologies quantiques présentaient un intérêt « absolument stratégique pour la protection du peuple français » (Parly, 2022). De son côté, la Commission européenne, notamment sous l'égide de Thierry Breton, a pour objectif, dans le quantique

(comme dans le domaine spatial), de créer des capacités européennes indépendantes dans le développement et la production de ces technologies d'importance stratégique avec des applications duales (Kelly, 2021).

Vers une souveraineté quantique : stratégies européennes

L'Europe dans la compétition internationale dans le quantique

La puissance combinée des grandes universités américaines, des investisseurs privés et des grandes entreprises numériques comme IBM, Google, Intel ou Amazon ont donné une longueur d'avance aux États-Unis dans l'informatique quantique. À titre d'exemple, la plateforme IBM Quantum Expérience est un simulateur de programmation quantique, mis en ligne dès 2016, et IBM a exporté son tout premier ordinateur quantique commercial (certes encore expérimental), le Quantum System One, en Allemagne et au Japon en 2021.

Côté chinois, de solides efforts de recherche, et des collaborations internationales, ont mené à un progrès rapide et même à un *leadership* dans la cryptographie et les communications quantiques – domaines où la Chine mène la course en termes de dépôts de brevet (Garisto, 2021). Pékin l'a montré dès 2016 en lançant le premier satellite de communication quantique au monde, et le gouvernement a annoncé l'année suivante un investissement de 10 milliards de dollars dans un nouveau centre de recherche quantique.

Malgré les avancées impressionnantes des deux géants, et contrairement à la plupart des autres technologies numériques, l'Europe (au sens géographique) est bien placée dans la course mondiale aux technologies quantiques (Pannier, 2021). Le Royaume-Uni, l'Allemagne, la France, les Pays-Bas, l'Autriche et la Suisse disposent tous d'importantes capacités de recherche quantique et d'écosystèmes de *start-up* florissants. Leurs gouvernements, ainsi que l'Union européenne, réalisent des investissements importants dans les sciences et technologies quantiques, dont de nombreux chercheurs européens ont été les précurseurs.

En France, l'écosystème est riche et s'appuie sur les organismes de recherche nationaux ainsi que sur de grandes entreprises impliquées dans l'informatique, les télécommunications, et les technologies habilitantes (cryogénie, microélectronique). Mais la France a aussi vu des jeunes pousses quantiques – issue des laboratoires universitaires – prospérer ces dernières années. Pasqal est une entreprise d'ordinateurs quantiques, créée en 2019, qui équipe déjà le centre de supercalcul français GENCI, et le centre de recherche allemand Jülich. Elle a récemment fusionné avec la *start-up* néerlandaise Qu and Co, spécialisée dans les logiciels et prévoit de fournir un ordinateur quantique de 1 000 qubits en 2024 (à titre de comparaison, la machine la plus puissance d'IBM à ce jour, le processeur Eagle, affiche une puissance de 127 qubits). Début 2023, Pasqal a réalisé une levée de fonds internationale de 100 millions d'euros, illustrant à la fois le rayonnement mondial des acteurs européens, et les limites du continent pour le financement de ces entreprises.

Objectifs et défis de l'Europe

Sur ces bases prometteuses, l'Europe peut-elle espérer atteindre la souveraineté technologique dans le quantique ? Deux défis, notamment, se posent : d'une part, concilier objectif de souveraineté et coopération internationale, et d'autre part, ancrer le quantique dans une perspective holistique et de long terme de poursuite d'une souveraineté technologique.

La question de l'ouverture de l'écosystème quantique européen

Comment développer des technologies quantiques européennes souveraines ? De nombreux objectifs stratégiques et économiques ayant trait aux technologies quantiques sont partagés par les États européens et les institutions de Bruxelles : la nécessité de garantir un accès aux technologies quantiques et la possibilité de bénéficier de l'accélération et des innovations apportées par celles-ci ; l'objectif de développement d'applications et l'adoption des technologies par les chercheurs, les gouvernements et l'industrie ; la sécurisation des données et des infrastructures face aux menaces quantiques ; et la constitution d'un écosystème européen dynamique, y compris *via* des synergies entre les écosystèmes nationaux.

Certaines divergences apparaissent toutefois au sein de l'Europe, selon deux axes. La première ligne de fracture concerne la question de savoir s'il faut donner la priorité au développement d'écosystèmes locaux de matériel et de logiciels quantiques européens, ou s'il faut acquérir des technologies étrangères pour viser une adoption rapide de ces technologies en Europe. Cette question s'est notamment posée du fait du caractère précurseur de certaines technologies non européennes, comme celles d'IBM évoquées plus haut. Mais la question va demeurer même à mesure que des solutions européennes se développent. L'exemple des supercalculateurs, acquis dans le cadre de « l'entreprise commune » EuroHPC, et déployés dans plusieurs centres de recherche en Europe, est parlant : pour le centre de calcul de Barcelone, le choix avait été fait d'acquérir une machine IBM-Lenovo (un consortium américano-chinois), plutôt qu'une machine « européenne » Atos, car la priorité était donnée au coût et à la puissance de calcul de la machine, plutôt qu'à une forme de « préférence européenne ». Il aura fallu une intervention politique d'Emmanuel Macron pour revenir sur ce choix.

La deuxième ligne de fracture – qui découle de la première – concerne les coopérations internationales dans le quantique. Pour résumer, le débat oppose, d'une part, les communautés de recherche et certains États membres de l'UE qui souhaitent maintenir l'ouverture de la recherche et coopérer avec des partenaires qui disposent d'écosystèmes dynamiques (le Royaume-Uni, les États-Unis, la Suisse, le Canada, Israël, la Corée du Sud ou encore le Japon) et, d'autre part, les acteurs qui considèrent que les technologies quantiques sont trop sensibles et disruptives pour être aussi ouvertes que d'autres domaines et que les partenariats doivent donc être sélectifs.

L'enjeu concerne surtout le niveau de maturité des technologies. Les technologies dites « émergentes » découlent de découvertes scientifiques issues d'une recherche sur le long terme – une recherche scientifique qui se déroule, par défaut, dans un cadre ouvert et globalisé. Si ces coopérations sont nécessaires à la recherche et souhaitables pour des technologies à faible niveau de maturité, la cohérence des stratégies française comme européenne, avec les objectifs politiques de maîtrise de l'ensemble des technologies quantiques au sein de l'UE, suggère que la coopération internationale devrait être limitée et encadrée, pour les technologies à plus haut niveau de maturité.

La nécessité d'une approche holistique et de long terme

Le développement de technologies quantiques repose sur le travail conjoint de physiciens, d'ingénieurs, de mathématiciens, de développeurs, de *data scientists*... Les machines quantiques ainsi développées reposent sur un ensemble de composants, des matières premières, des chaînes de production, des semi-conducteurs, des logiciels et applications, et des *cloud* sur lesquels les utilisateurs peuvent et pourront accéder à la puissance de calcul quantique. Quant aux communications quantiques, elles s'appuient sur des satellites et des réseaux de câbles. Les usages des technologies quantiques sont, ensuite, encadrés par des réglementations en termes de protection des données. Au regard de ces multiples imbrications, on comprend bien qu'une approche holistique, transversale et

de long terme est nécessaire dans la poursuite d'une souveraineté dans les technologies quantiques.

Aux États-Unis, les efforts de recherche dans les sciences et technologies quantiques sont largement menés par des grandes entreprises de la tech qui pourraient, à terme, maîtriser l'ensemble de la chaîne de valeur quantique, du logiciel au matériel en passant par le *cloud*. De la même manière, en Chine, les liens entre le gouvernement chinois, les écosystèmes de recherche et les grandes entreprises technologiques, permettent un effort conjoint et sur l'ensemble de la chaîne de valeur. Il n'y a pas d'acteur ou de fonctionnement équivalent en Europe, ce qui peut s'avérer être un handicap.

En Europe, s'il n'y a pas un acteur unique possédant toutes ces caractéristiques, il y a néanmoins un ensemble d'outils, d'initiatives et de lois, couvrant l'ensemble du spectre – du financement de la recherche au soutien à l'industrie des semiconducteurs en passant par le développement d'acteurs européens du *cloud* – qui, s'ils sont orientés vers des objectifs cohérents, concourront à faire émerger un secteur quantique européen fort. L'enjeu des investissements privés, et notamment du capital-risque, bien qu'identifié de longue date et qui ne relève pas de la puissance publique, reste toutefois un vrai frein à la montée en puissance de l'écosystème européen dans les technologies quantiques.

Bibliographie

GARISTO D. (2021), "China is pulling ahead in global quantum race, New studies suggest", *Scientific American*, 15 juillet.

JULIENNE M. (2022), « Le rêve quantique chinois : les aspirations d'un géant dans l'infiniment petit », Études de l'Ifri, février.

KELLY E. (2021), "Viewpoint: EU will be 'shooting itself in foot' if it bars UK, Switzerland, Israel from quantum and space projects", *Science Business*, 18 mars.

PANNIER A. (2021), « Calcul stratégique : le calcul haute performance et l'informatique quantique dans la quête de puissance technologique de l'Europe », Études de l'Ifri, octobre.

PARLY F. (2022), *Déclaration sur la plateforme de calcul quantique* [discours de la ministre des Armées], Paris, 4 janvier.

VELLIET M. (2022), « Convaincre et contraindre : les interférences américaines dans les échanges technologiques entre leurs alliés et la Chine », Études de l'Ifri, février 2022.

Souveraineté et résilience numérique : mission impossible ?

Par Olivier BEAUREPAIRE
Directeur programme Data & CDO, TER-SNCF Voyageurs

Thomas BOLLE
Lieutenant-colonel, officier professeur au centre de formation des dirigeants de l'école des officiers de la Gendarmerie nationale

Sophie LAFON
Directrice adjointe Statistiques et Valorisation des Données, RTE

& Stanislas SMIEJAN
Directeur Marketing, ADISSEO

Mentor de la mission :
Romain NICCOLI,
cofondateur et co-CEO de Pigment

Le présent article synthétise les réflexions de la mission réalisée dans le cadre de la Fondation Nationale Entreprise et Performance, consacrée au thème général de la souveraineté numérique. Les auteurs se sont concentrés sur deux sujets particuliers, l'ordinateur quantique et l'éthique de l'intelligence artificielle, deux sujets sur lesquels les membres de la mission estiment que la France et l'Europe peuvent maintenir leur souveraineté, et montrent, dans leurs recommandations, comment y parvenir et les écueils à éviter.

Les quatre membres de la mission ont réalisé leur enquête sur le thème de la « souveraineté numérique » au cours de l'année 2022 en rencontrant les acteurs du domaine en France et à l'étranger et grâce à des voyages d'étude en Allemagne, en Finlande et en Estonie. L'article qui suit est extrait de leur ouvrage, disponible sur le site de la Fondation Nationale Entreprise et Performance à l'adresse www.fnep.org.

Réflexions sur la souveraineté numérique

« Ce sont ceux qui peuvent détruire une chose qui la contrôlent vraiment »[1].

Cette phrase est prononcée par le protagoniste principal de *Dune*, le célèbre roman de science-fiction de Frank Herbert qui y raconte les tentatives de grandes puissances ou d'organisations pour dominer l'exploitation d'une ressource naturelle critique, l'Épice, substance rare produite sur une seule planète de l'univers, et qui ne peut être créée artificiellement.

Ce roman aborde donc, entre autres, le thème de la souveraineté qui trouve son illustration dans au moins deux événements récents : la guerre en Ukraine et la crise sino-taïwanaise.

[1] HERBERT F. (1980), *Dune*, Volume 2, Robert Laffont, ISBN : 2-266-02664-X.

La Russie, sous le coup de sanctions internationales, détenant les plus grandes réserves prouvées de gaz naturel au monde, a brûlé le gaz qu'elle fournissait auparavant aux Européens[2].

Taïwan, face aux menaces d'invasion par la Chine, a menacé de rendre inopérantes les fonderies de semi-conducteurs du *leader* mondial TSMC (Taiwan Semiconductor Manufacturing)[3].

Les semi-conducteurs sont l'Épice du roman de Frank Herbert, qui permet, entre autres, aux navigateurs de la Guilde spatiale d'améliorer leurs capacités de vision dans l'avenir. Les semi-conducteurs sont eux essentiels aux nouvelles technologies. Ces composants, produits à Taïwan, et en Corée du Sud ont subi des ruptures d'approvisionnement.

L'Europe, où des millions de véhicules automobiles n'ont pu être fabriqués, a décidé de réagir par le EU Chip Act afin de redevenir un *leader* mondial des semi-conducteurs à l'horizon 2030.

À cette dépendance actuelle, l'Union européenne répond par l'interdépendance, se proposant de « construire une Europe « usine », capable de conquérir une part croissante du marché mondial en pleine expansion », en faisant le choix de financer, à hauteur de plusieurs milliards d'euros, l'installation d'entreprises américaines alors que l'Union dispose de champions européens comme le Franco-Italien ST Microelectronics, l'Allemand Infineon et le Néerlandais ASML (*leader* mondial de la fabrication de machines de photolithographie).

L'avenir dira si l'Union européenne n'a pas troqué sa dépendance pour une autre.

Dans le domaine de la souveraineté numérique, la France et l'Europe semblent donc avoir déjà perdu plusieurs batailles, même si quelques *leaders* mondiaux y ont émergé. Dans le domaine des télécommunications, par exemple, les principaux réseaux sociaux sont Américains ou Chinois, les composants électroniques sont fabriqués en Chine ou à Taïwan, les plus grands systèmes d'exploitation sont Américains.

Cependant, il reste encore au moins deux domaines, identifiés par la mission, dans lesquels la France, au sein de l'Europe, a des cartes à jouer pour maintenir, ou reconstruire, sa souveraineté : le développement de l'ordinateur quantique et l'encadrement de l'éthique de l'Intelligence Artificielle (IA).

L'ordinateur quantique, ses enjeux, ses risques et ses opportunités

Un ordinateur quantique utilise les propriétés quantiques de la matière afin d'effectuer des opérations sur des données. À la différence d'un ordinateur classique basé sur des transistors travaillant sur des données binaires (codées sur des bits, valant 0 ou 1), l'ordinateur quantique travaille sur des qubits[4] dont l'état quantique peut posséder plusieurs valeurs, ou plus précisément une valeur quantique comportant plusieurs possibilités

[2] PEZET J. (2022), « Est-il vrai que la Russie brûle depuis juin le gaz qu'elle aurait pu livrer à l'Allemagne », *Libération* (en ligne), 1er septembre 2022, disponible à l'adresse : https://www.liberation.fr/checknews/est-il-vrai-que-la-russie-brule-depuis-juin-le-gaz-quelle-aurait-pu-livrer-a-lallemagne-20220901_YVVQAWYTJZDLNCHJ2OV5ONKZ3I/

[3] CRISTIANI J. (2022), « Si Pékin envahit Taïwan, l'économie chinoise sera bloquée », *La Tribune* (en ligne), disponible à l'adresse : https://www.latribune.fr/economie/international/si-la-chine-envahit-taiwan-son-economie-sera-bloquee-avertit-le-pdg-de-tsmc-leader-mondial-des-semi-conducteurs-927517.html

[4] Unité de mesure de l'information en informatique quantique.

simultanées. L'ordinateur quantique promet de révolutionner le calcul. Cette technologie apporte la capacité de résoudre, en quelques minutes, des calculs insolubles aujourd'hui au regard de la vitesse de calcul possible.

Les domaines d'application sont concrets et nombreux. Pour n'en citer que quelques-uns :

- des usages ont d'ores et déjà été imaginés dans le domaine de la métrologie, militaire ou non ;
- les apports pour la médecine et la chimie auront pour finalité la compréhension des mécanismes de maladies et le développement de nouveaux médicaments, adaptés à chaque personne ;
- dans la logistique, le quantique s'attaquera à la résolution de nombreux problèmes, trop complexes pour les algorithmes actuels ;
- une amélioration des performances des systèmes d'IA est attendue, notamment dans l'apprentissage automatique ;
- cependant, et c'est une menace réelle, dans le domaine de la sécurité numérique, l'ensemble des codes de cryptographie actuels, reposant sur des technologies non quantiques, seront susceptibles d'être craqués de manière quasi instantanée.

Concernant la technologie quantique, la France a lancé sa stratégie nationale en 2021, avec un financement public-privé d'un montant de 1,8 milliard d'euros sur cinq ans. C'est moins que l'Allemagne (plus de 2 milliards d'euros) et cinq fois moins que la Chine ou les États-Unis. Néanmoins cette ambitieuse stratégie semble comprendre tous les ingrédients nécessaires à sa réussite : la recherche fondamentale, un écosystème de *start-up*, du capital-risque ainsi que des fonds publics. Elle anticipe l'enjeu stratégique de formation de 5 000 talents en technologies quantiques.

Avec onze lauréats de la médaille Fields, et une dizaine de lauréats du prix Nobel de Chimie et du prix Nobel de Physique, la France se classe parmi les premières nations au niveau mondial. Pour autant, la relève est-elle assurée pour entrer dans la quatrième révolution industrielle ? La baisse importante du niveau des élèves français en mathématiques, la désaffection pour les sciences n'amène, selon une note du ministère de l'éducation nationale et de la jeunesse de décembre 2020, « que 3 % des élèves au niveau avancé en sciences alors qu'ils sont en moyenne 10 % dans les pays de l'UE et de l'OCDE »[5].

Le plan d'investissement France 2030 a pour ambition affichée de « développer la compétitivité industrielle et les technologies d'avenir ». Dans ce sens le ministre de l'Éducation nationale a pris la décision de rendre à nouveau les mathématiques obligatoires dans le programme de première générale à partir de la rentrée de septembre 2023 ; cependant certains professeurs pointent du doigt la faiblesse d'activité scientifique sur ordinateur : on peut légitimement se poser la question de savoir si l'ambition de « maîtriser les technologies numériques souveraines et sûres » est réaliste.

De nombreux États ont pris conscience de la criticité de cette technologie pour l'avenir de leur souveraineté. Les États-Unis et la Chine, en premier lieu, rivalisent dans leurs investissements. La France n'est pas en reste dans ce domaine, et dispose d'atouts indéniables. Plusieurs technologies émergent et des choix devront être faits pour réussir à les concrétiser, demain, par la création de vrais champions et une industrie du quantique.

[5] Note d'information n°20-48 de la direction de l'évaluation, de la prospective et de la performance, décembre 2020, disponible à l'adresse : https://www.education.gouv.fr/timss-2019-sciences-au-niveau-de-la-classe-de-quatrieme-les-resultats-de-la-france-en-retrait-l-307821

Les analyses et les entretiens menés par la mission, ont permis de dégager sept recommandations, afin de donner une chance de construire une place d'avenir au quantique, chacune de ces recommandations permettant de pallier un risque avéré :

Risque de sous financement	Recommandation 1	Concentrer les financements sur les phases d'industrialisation en sélectionnant quelques champions
	Recommandation 2	Ne pas saupoudrer et focaliser l'approche industrielle sur les technologies quantiques les plus proches de la mise en production
Risque du manque ou de perte des talents	Recommandation 3	Définir dès maintenant une stratégie RH du quantique
	Recommandation 4	Encourager les allers-retours public-privé des chercheurs
Risque lié à l'appropriation tardive de la part des entreprises	Recommandation 5	Préparer les entreprises à la transformation quantique
	Recommandation 6	Permettre aux entreprises de disposer des infrastructures nécessaires à l'irruption du quantique
	Recommandation 7	Mettre en place les conditions pour l'industrialisation

L'intelligence artificielle et les enjeux liés à l'éthique

L'ouvrage de la mission 2022 s'intéresse également au sujet de l'intelligence artificielle, comme étant une des technologies de rupture de ces dernières années pouvant avoir un impact majeur sur la souveraineté des États. Le sujet n'est pas nouveau mais les réflexions engagées aujourd'hui autour de l'encadrement de l'IA ont poussé la mission à approfondir cette thématique.

Comment caractériser de manière succincte l'IA ?

L'intelligence artificielle est un domaine de la technologie qui vise à faire en sorte que les machines puissent accomplir des tâches qui nécessitent habituellement de l'intelligence humaine, comme comprendre le langage, résoudre des problèmes ou apprendre par elles-mêmes.

Il y a plusieurs façons d'apprendre pour les machines. L'une des plus courantes aujourd'hui est appelée apprentissage automatique, fondée sur l'exploitation de gigantesques bases de données d'exemples. Récemment, le concept de réseaux de neurones profond, associé à des algorithmes d'apprentissage appropriés, a permis la résolution spectaculaire de tâches réputées complexes.

De très nombreux cas d'usages sont aujourd'hui accessibles aux IA, et pour en citer quelques-uns :

- la reconnaissance vocale et faciale : pour les systèmes de sécurité notamment ;

- les transports : pour l'optimisation des itinéraires et la conduite des voitures autonomes ;
- le commerce électronique : avec la recommandation de produits en ligne et la personnalisation de l'expérience d'achat ;
- la santé : pour *designer* des médicaments, diagnostiquer des maladies, recommander des traitements ;
- la finance : pour les transactions financières complexes et sécurisées, ou encore la recommandation des investissements ;
- le marketing et le *retail* : pour personnaliser les campagnes de marketing, prédire les tendances de consommation, recommander des actions de marketing ;
- l'éducation : pour personnaliser des plans d'étude, détecter des difficultés d'apprentissage, évaluer les performances des étudiants.

À défaut d'être *leader* en matière d'intelligence artificielle, l'Union européenne légifère.

L'intelligence artificielle est un enjeu stratégique pour la France et l'Europe, qu'il est nécessaire de traiter de manière dépassionnée, car il en va de l'autonomie stratégique de l'Union européenne. Cela commence par la parfaite compréhension de ces sujets par nos dirigeants, or, il y a à ce sujet de réelles inquiétudes. Ainsi, l'ancien haut-commissaire à l'énergie atomique, Yves Bréchet, souligne « l'inculture scientifique et technique de notre classe politique », qui les empêche de cerner toute la complexité des problèmes, et l'incapacité des conseillers à apporter des réponses « sur des sujets qu'ils ne maîtrisent généralement pas ».

Risque de manque de confiance	Recommandation 8	Définir et déployer une stratégie *open source*
Risque de données	Recommandation 9	Créer un comité éthique pluridisciplinaire de l'IA[a]
Risque de manque de compétences des futurs travailleurs de l'IA en entreprise	Recommandation 10	Démarrer la formation continue sur le quantique et l'IA en entreprise

[a] Note de la rédaction des *Annales des Mines* :

Le ministre chargé du Numérique a mentionné dans le numéro de juin 2023 d'*Enjeux numériques* consacré aux mondes virtuels : « J'ai saisi le comité national d'éthique du numérique sur un projet pilote en 2019. Il a été pérennisé cette année par le président de la République, et le comité rendra cet été un avis sur l'éthique de l'IA et des agents conversationnels comme ChatGPT. De même, nous pourrions envisager de le saisir également sur la notion de mondes virtuels ». À la lumière de ces évolutions, la recommandation pourrait consister à faire référence à ces travaux du comité national d'éthique du numérique.

L'éthique de l'IA fait également l'objet d'auto saisine d'organismes internationaux. Cela a été le cas à l'Unesco avec une recommandation de 193 États en novembre 2021. Le 7 mai 2023 a donné lieu à une déclaration des ministres du G7 en vue de l'adoption d'une réglementation sur l'intelligence artificielle « fondée sur le risque » et qui devrait également « préserver un environnement ouvert et propice » au développement des technologies d'intelligence artificielle et se fonder sur les valeurs démocratiques.

Dans le cas de l'intelligence artificielle, l'Union européenne, qui pense avant tout à légiférer, met davantage en avant les problèmes d'éthique et de gouvernance que le potentiel

que l'on peut tirer de l'IA et devient le champion de la régulation à défaut de l'innovation. Elle assiste en spectateur au duel entre la Chine et les États-Unis qui dépensent davantage que les deux milliards d'euros annoncés par la Commission. La vision à long terme doit changer radicalement afin de sensibiliser le public par une vision positive et non biaisée.

Là encore, les États ont bien identifié le sujet et ont proposé, notamment en Europe avec « L'AI Act », cadre réglementaire pour tenter de juguler une partie des risques que l'IA pourrait représenter sur la souveraineté. Au-delà de ce cadre, la réflexion menée par la mission a permis de proposer trois recommandations pour remédier à certains risques majeurs et contribuer à maintenir la souveraineté de la France et de l'Europe dans le contexte du déploiement accéléré de l'IA.

L'ouvrage de la mission n'a pas vocation à être exhaustif, mais ses conclusions pourraient aider le régulateur et le législateur dans le soutien au développement absolument critique d'une industrie de l'ordinateur quantique compétitive en France, au développement et à l'encadrement de l'industrie de l'IA, et inspireront peut-être les entreprises.

Notre vie numérique dépend-elle des câbles sous-marins ?

Par Ophélie COELHO
Membre du Conseil scientifique de l'Institut Rousseau
et de l'Observatoire de l'éthique publique

Les premiers câbles sous-marins télégraphiques du XIXe siècle étaient déjà un enjeu stratégique de puissance instrumentalisé par les États. Aujourd'hui, le maintien de ces infrastructures est considéré comme un enjeu critique, car le développement des technologies numériques donne une place importante aux échanges de données dans la formalisation du marché mondial et les dépendances techniques transcontinentales se sont intensifiées. Ainsi, détenir des câbles sous-marins ou des compétences particulières dans ce domaine, c'est posséder de nouveaux pouvoirs et être en capacité d'instrumentaliser les dépendances à ces infrastructures. Les propriétaires de câbles, et en particulier les *Big Tech* qui ont massivement investi dans ce domaine, détiennent une capacité d'influence non seulement pour l'accès aux données du continent, mais également sur le plan technique, politique et culturel. Pour comprendre ces nouveaux rapports de force, cet article revient d'abord sur les conditions d'interdépendance qui confèrent aujourd'hui aux câbles sous-marins une place importante. Puis il analyse les stratégies de mise en dépendance et d'assujettissement technologique avec l'exemple de l'Afrique qui est aujourd'hui le terrain d'expansion des nouveaux propriétaires de câbles.

Les câbles sous-marins sont trop souvent présentés comme des infrastructures sans lesquelles internet ne fonctionnerait plus. Bien que ceux-ci jouent un rôle crucial dans le transport de données entre les continents, ils ne sont pas seuls à assumer cette tâche, et les chiffres souvent cités selon lesquels 90 à 98 % des données mondiales transitent par les câbles sous-marins sont en réalité difficilement vérifiables et présentent une vision inexacte de la réalité.

Composé de réseaux locaux interconnectés, le principe d'internet ne repose pas sur une infrastructure unique mais plutôt sur une multitude d'objets et de machines : des câbles sous-marins, des répéteurs[1], des câbles terrestres, des routeurs[2], des antennes-relais[3],

[1] Un répéteur est un dispositif utilisé dans les réseaux de communication pour régénérer ou répéter un signal qui pourrait être affaibli ou dégradé lors de son transfert sur de longues distances. Il amplifie le signal reçu avant de le retransmettre.

[2] Un routeur est un dispositif qui assure la connexion entre différents réseaux informatiques. Il gère le trafic de données en déterminant le chemin le plus efficace pour transmettre les informations d'un réseau à un autre.

[3] Une antenne-relais est un dispositif de transmission utilisé principalement dans les réseaux de téléphonie mobile. Elle permet d'établir une communication entre les utilisateurs mobiles et le réseau de l'opérateur.

des commutateurs[4], des serveurs[5], des satellites, etc. L'ensemble forme une diversité de routes qui acheminent les informations entre les appareils de l'utilisateur comme les ordinateurs, les smartphones, les tablettes et autres objets connectés.

Ainsi, en cas de coupure ou d'endommagement de câbles sous-marins, le trafic de données peut d'abord être rerouté *via* d'autres chemins si la densité des infrastructures le permet. La densité des réseaux dans les pays fortement numérisés rend possible le réacheminement des données vers les réseaux terrestres, vers d'autres câbles sous-marins non-endommagés ou vers des connexions par satellite. Par ailleurs, le principe technique de réseau internet s'applique sans problème à différentes échelles territoriales, même en l'absence de connexions intercontinentales. Cela signifie que les réseaux terrestres à l'échelle continentale ont la capacité de relier les pays entre eux et de soutenir un internet à cette échelle. Aussi, il n'y a pas de bouton d'interrupteur général qui permettrait de « couper internet » à l'échelle globale, et si l'endommagement de câbles sous-marins ou la déconnexion volontaire d'un territoire pourrait couper du *web*[6] global une zone géographique particulière, cela ne signifie pas que le principe technique d'internet ne serait plus applicable dans le périmètre restreint d'un pays, d'un groupe de pays ou d'un continent.

Si le principe d'internet ne dépend pas des câbles sous-marins, ceux-ci revêtent néanmoins une puissante dimension symbolique : ils rendent possible le développement d'un mode de vie contemporain fondé sur la mondialisation des échanges. Sans eux, plus de système SWIFT[7] pour gérer les transactions financières massives à l'échelle globale, plus d'accès aux services dont les logiciels ou les données seraient situées sur un autre continent ou à très grande distance[8]. Finalement, les câbles sous-marins de télécommunication sont représentatifs de notre dépendance à des données et des logiciels souvent hébergés sur des territoires extra continentaux. Les questions stratégiques que soulèvent ces infrastructures démontrent en définitive l'omniprésence et le rôle central qu'ont acquis certains services numériques dans le mode de vie de nombreux pays.

À la lumière de ces éléments, nous proposons ici un retour sur la dimension stratégique de ces infrastructures et leur utilisation historique comme levier de pouvoir. Nous verrons également comment ces câbles sont devenus des éléments centraux de la stratégie d'expansion territoriale des géants technologiques, notamment en Europe et en Afrique. Cette mise en lumière de l'utilisation des câbles sous-marins de télécommunication comme outils au service de nouveaux empires nous permettra enfin d'aborder la notion d'« instrumentalisation de l'interdépendance »[9], que nous proposons comme un élargissement de celle de « militarisation de l'interdépendance ».

---

[4] Un commutateur (ou *switch* en anglais) est un équipement qui permet de relier plusieurs appareils sur un réseau informatique pour qu'ils puissent communiquer entre eux.

[5] Un serveur physique est un ordinateur dédié à la gestion et à la distribution de données et de ressources réseau à d'autres ordinateurs connectés à ce même réseau. Il peut héberger divers types de services, comme les sites *web*, les courriels, les bases de données et bien plus encore.

[6] Pour rappel, *web* est l'abréviation de *World Wide Web* (toile d'araignée mondiale), qui est un système d'information qui fonctionne sur le réseau internet.

[7] SWIFT, nommé d'après la Society for Worldwide Interbank Financial Telecommunication, est le système informatique permettant le transport à l'échelle mondiale des messages contenant des instructions de paiement entre les institutions financières.

[8] À l'échelle continentale, il sera plus efficace d'utiliser un câble sous-marin plutôt que de passer par les réseaux terrestres traversant différents pays, qui peuvent être de qualité et de maintenance inégales, notamment dans le cas où la distance entre émetteur et transmetteur est importante.

[9] Cette notion et les enjeux géopolitiques qu'elle recouvre sont approfondis dans un ouvrage dédié : COELHO O. (2023), *Géopolitique du numérique - L'impérialisme à pas de géants*, Les éditions de l'Atelier.

Les câbles sous-marins : un enjeu stratégique ?

Par nature, les câbles sous-marins sont au cœur des relations internationales. D'abord télégraphiques, les premiers câbles posés au XIXe siècle[10] offrent de nouvelles opportunités stratégiques. À cette époque, le réseau télégraphique appartient majoritairement à l'empire britannique, et participe à étendre son influence sur le monde. Les câbles étaient d'abord un moyen sécurisé et rapide de communication entre le gouvernement britannique et ses colonies éloignées. Mais au cours du XXe siècle, les câbles sous-marins sont devenus de véritables leviers de pouvoir. Pendant la Première Guerre mondiale, ils deviennent un outil précieux de communication au service des pays alliés. Plus tard, plusieurs opérations ciblant les câbles sous-marins montrent également la place particulière de cette infrastructure dans les nouvelles stratégies militaires, qu'il s'agisse de couper les communications de l'ennemi ou de l'espionner en recueillant les informations circulant sur son réseau. C'est le cas de l'opération Sabre lancée en 1945 pendant la Seconde Guerre mondiale par la Royal Navy, et qui visait à couper un câble de communication sous-marin japonais reliant Saigon et Singapour afin de perturber les communications entre les différentes unités des forces armées japonaises. Au plus fort de la guerre froide, dans les années 1970, la marine américaine et la National Security Agency (NSA) ont lancé l'opération Ivy Bells pour se brancher secrètement sur un câble sous-marin soviétique dans la mer de Barents et recueillir des renseignements. Cette opération a permis aux États-Unis d'accéder aux communications militaires soviétiques.

Enfin, au début du XXIe siècle, avec le développement des technologies numériques et l'installation progressive de fibre optique qui permet de transporter une très grande quantité de données, la nature de l'instrumentalisation des câbles sous-marins a évolué. Le programme Tempora, révélé par Edward Snowden en 2013, en est un exemple : le GCHQ britannique (Government Communications Headquarters) et la NSA américaine avaient exploité les flux de données des câbles sous-marins pour l'interception massive de données numériques, donnant forme à une nouvelle ère de surveillance numérique à grande échelle.

Un changement historique de paradigme

Jusqu'à récemment, les câbles appartenaient généralement à des consortiums géants composés d'entreprises de télécommunications. Alors que très souvent ces entreprises étaient nationales et gérées par les États, la privatisation du secteur des télécommunications dans les années 1990 redistribue les cartes du pouvoir entre acteurs publics et privés.

Si un État a tout intérêt à conserver une infrastructure stratégique telle que les câbles sous-marins, une entreprise considère d'abord les gains possibles liés à leur exploitation. Or, les câbles coûtent très chers sur tout leur cycle de vie : il faut des milliards d'euros pour les fabriquer, les poser, les surveiller, les réparer, les maintenir en service et les réactualiser en fonction des changements technologiques. Pour une entreprise cotée en bourse, les gains d'exploitation ne couvrent pas une telle charge financière, et ces dernières années il est devenu très difficile pour les télécoms d'investir dans de nouveaux chantiers de câbles.

[10] Le premier câble sous-marin a été posé en 1850, et a relié pendant onze minutes le Royaume-Uni et la France avant d'être endommagé. Cette installation était en effet très rudimentaire, vulnérable aux problèmes de corrosion et de dommages mécaniques.

Dans le même temps, les grands acteurs du numérique comme Google, Meta, Microsoft ou Amazon ont vu augmenter leur besoin en bande passante, et ont décidé d'investir dans leurs propres câbles sous-marins. De cette manière, ils rompent leur dépendance historique aux télécoms. Mais de ce besoin initial en bande passante ressort également une opportunité commerciale stratégique. En investissant massivement dans les câbles sous-marins, ces sociétés ont établi une base solide pour leur expansion mondiale.

Parmi ces nouveaux entrants du marché, Google est la seule entreprise qui finance intégralement certains projets d'envergure, dont elle est seule propriétaire, tels que les câbles transcontinentaux Dunant, qui traverse l'océan Atlantique pour rejoindre les côtes bretonnes, et Equiano, qui relie l'Europe à l'Afrique. Depuis sa première participation à la construction du câble transpacifique Unity/EAC-Pacific en 2010, elle a lancé pas moins de vingt-et-un projets de câbles sous-marins, dont dix-huit sont déjà opérationnels en 2023.

	Nombre de câbles sous-marins	**Nom des câbles**
Google	**21**	Apricot, Blue, Raman, Firmina*, Topaz*, Echo, Grace Hopper*, PLCN, Equiano*, Dunant*, Havfrue, JGA-S, Curie*, INDIGO-Central, INDIGO-West, Junior*, Tannat, Monet, FASTER, SJC, Unity
Meta	**15**	Apricot, Bifrost, 2Africa, Amitié, SJC2, Echo, CAP-1, Havhingsten/CC-2, Havhingsten/NSC, PLCN, Malbec, Havfrue, JUPITER, MAREA, APG
Microsoft	**4**	MAREA, NCP Cable System, Amitié, SeaMeWe-6
Amazon	**2**	CAP-1, JUPITER

Figure 1. Liste des câbles sous-marins de télécommunication dans lesquels Google, Meta, Microsoft et Amazon ont investi (copropriété ou propriété, juin 2023).
* Google est l'unique propriétaire du câble

Lorsqu'une entreprise investit dans un câble sous-marin, elle collabore généralement avec une entreprise de télécommunications locale pour gérer une station d'atterrissement à chaque extrémité du câble, où le signal est transmis au réseau terrestre. Cependant, la Federal Communications Commission (FCC)[11] aux États-Unis a autorisé Google[12] et Microsoft[13] à gérer elles-mêmes certaines stations d'atterrissement.

Ces stratégies de développement des infrastructures numériques annoncent l'émergence d'un nouveau type de pouvoir pour ces multinationales. Non seulement elles acquièrent une indépendance dans des étapes clés de leur activité, mais elles obtiennent également une maîtrise technologique d'un secteur complémentaire, tout en créant une dépendance pour l'écosystème technique environnant. Cette position stratégique leur permet d'exercer une influence considérable sur les États et les entreprises des pays qui ont

[11] La Federal Communications Commission est une agence gouvernementale dite indépendante des États-Unis. Elle est chargée de réglementer les communications au niveau fédéral, notamment les télécommunications, la radio, la télévision, internet et les services mobiles. Elle joue un rôle clé dans l'élaboration des politiques et des règles concernant les télécommunications et les médias aux États-Unis.

[12] C'est le cas pour sept des câbles appartenant à Google, *via* sa filiale GU Holding Inc. : FASTER Cable, Monet Cable System, Curie, Dunant, Japan-Guam-Australia, Grace Hopper, Pacific Light, Cable Network (PLCN), Firmina.

[13] Microsoft gère la station d'atterrissement de sa copropriété New Cross-Pacific Cable *via* sa filiale Microsoft Infrastructure Group, LLC.

actuellement un accès précaire à ces infrastructures. C'est particulièrement le cas sur le continent africain, qui est aujourd'hui au cœur des intérêts des *Big Tech* américaines comme chinoises. Dans cette guerre qui oppose les géants technologiques, les inégalités d'accès aux réseaux de communication sur le continent sont considérées comme une véritable opportunité d'expansion.

Le continent africain, territoire de conquête numérique

Les projets d'envergure en Afrique, notamment les câbles sous-marins de télécommunication récemment construits par les géants américains et chinois du numérique, promettent de transformer les usages numériques sur le continent. Google, parmi ces nouveaux acteurs présents sur le pourtour du continent africain, a investi dans un câble de grande capacité dont il est l'unique propriétaire. Ce dernier s'étend actuellement le long de la côte ouest de l'Afrique. Le projet 2Africa entoure tout le continent avec 45 000 km de câble, regroupant dans un consortium relativement petit les entreprises China Mobile International, Meta, MTN, Orange, Saudi Telecom Company, Telecom Egypt, Vodafone et la West Indian Ocean Cable Company (WIOCC). Quant au câble PEACE, il est la propriété de Peace Cable International Network Co. Ltd, une filiale du groupe chinois Hengtong.

Alors que les capacités des câbles historiques ACE et WACS se limitaient à respectivement 12,8 Tbps et 14,5 Tbps, les câbles PEACE, 2Africa et Equiano surpassent ces chiffres avec des capacités dépassant les 100 Tbps. Ces câbles sous-marins à haute capacité préfigurent l'arrivée de nouveaux services numériques sur le continent africain, soutenus par un mouvement global de transformation numérique. Cette augmentation drastique de la bande passante permet en effet des usages numériques nécessitant une grande capacité de bande passante, tels que les services de *streaming* vidéo et audio pour un usage de masse, l'amélioration de possibilité de télétravail, le transfert de données volumineuses entre des centres de données géants potentiellement situés en Europe, aux États-Unis ou en Chine.

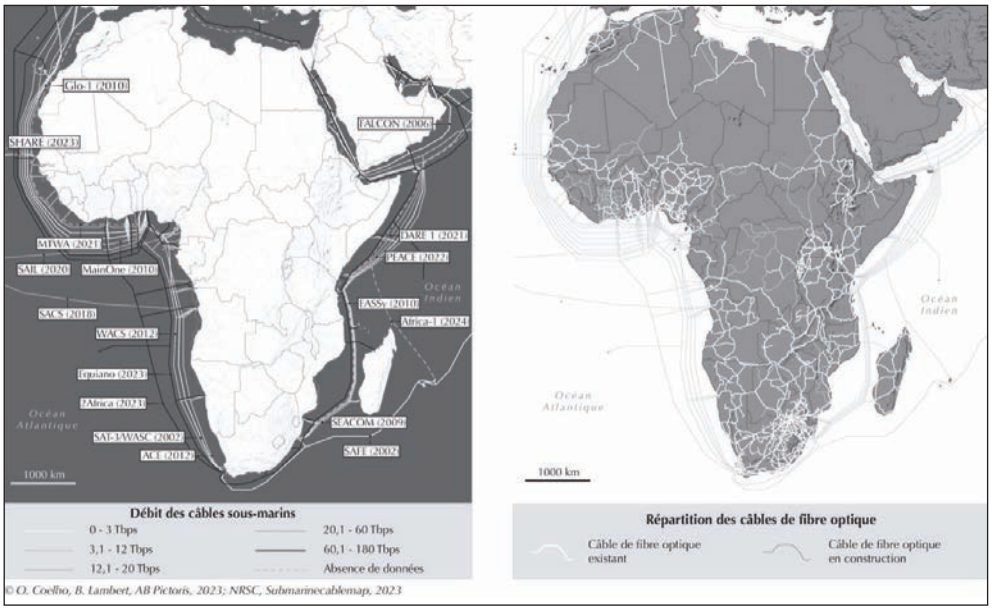


Figure 2. Réseaux de télécommunication sous-marins et terrestres du continent africain.

Cette perspective reste un pari audacieux, compte tenu des usages numériques actuels sur l'ensemble du continent, qui se caractérise par une grande disparité infrastructurelle, et dont l'accès à une bande passante qualitative dépend notamment de la qualité des infrastructures des réseaux terrestres. Or, ceux-ci restent parcellaires dans certaines régions, ce qui favorise des applications numériques requérant moins de bande passante et des principes techniques *low tech* tel que l'USSD[14].

Parallèlement, les *Big Tech* se positionnent comme des partenaires technologiques clés dans une région où l'accès à ces câbles est encore limité, rendant certains pays vulnérables en cas de défaillance de ces infrastructures. C'est notamment le cas de la République du Congo et de la Namibie, qui n'étaient connectés qu'au seul câble de télécommunication WACS, avant l'arrivée des câbles Equiano et 2Africa sur leurs côtes en 2021. Pour ces pays, l'accès à des câbles sous-marins devient stratégique et leur donne un avantage sur leurs voisins enclavés.

Pour réussir leur expansion en Afrique, les *Big Tech* s'associent généralement à des entreprises de télécommunications locales, comme les sud-africaines MTN et Liquid Telecom, ou à des acteurs européens déjà bien implantés sur le territoire, comme Orange et sa filiale sénégalaise Sonatel. Ces acteurs locaux jouent un rôle clé en tant que « passeurs » de technologie[15] et alliés administratifs sur le continent. Ils gèrent le raccordement au réseau et les stations d'atterrissement sur le territoire, facilitant ainsi l'installation et l'exploitation des câbles sous-marins de la *Big Tech*.

L'instrumentalisation de l'interdépendance : un phénomène multidimensionnel

L'instrumentalisation de l'interdépendance se réfère à la stratégie délibérée des acteurs – qu'ils soient étatiques ou privés – pour utiliser les dépendances mutuelles qui se développent dans des écosystèmes socio-économiques interconnectés comme levier d'influence et de pouvoir. Cette notion émane du constat que l'interdépendance dans les réseaux mondiaux, tels que le numérique, n'est pas intrinsèquement équilibrée. Au contraire, les dépendances qui en découlent sont souvent asymétriques et peuvent être exploitées par des acteurs puissants pour imposer leur volonté, contrôler l'accès à des ressources essentielles ou manipuler les comportements. Alors que la notion de « militarisation de l'interdépendance » utilisée par des chercheurs tels que Henry Farrell et Abraham L. Newman[16] se concentre principalement sur l'utilisation des dépendances mutuelles comme des armes dans des situations de conflit entre les États, l'instrumentalisation de l'interdépendance englobe une gamme plus large de tactiques et de scénarios. Cette notion dépasse le contexte étatique et militaire pour englober une stratégie plus large et polyvalente. Celle-ci peut prendre plusieurs formes, y compris la création de dépendances unilatérales ou mutuelles, la monopolisation des ressources clés ou le contrôle de points d'accès essentiels, la manipulation de l'information, tout cela dans le but d'exercer une influence, de gagner en puissance ou de réaliser des bénéfices.

[14] L'USSD (Unstructured Supplementary Service Data) est un protocole de communication utilisé sur les téléphones mobiles pour établir des sessions interactives entre l'utilisateur et les applications basées sur le réseau. Il est utilisé en composant des codes courts sur le clavier du téléphone pour accéder à des services spécifiques, tels que la consultation de solde ou la recharge de crédit.

[15] Cette notion de « passeur » de technologie est développée dans l'ouvrage *Géopolitique du numérique - L'impérialisme à pas de géants*, Les éditions de l'Atelier, 2023.

[16] FARRELL H. & NEWMAN A. L. (2019), "Weaponized Interdependence : How Global Economic Networks Shape State Coercion", *International Security*, vol. 44, issue 1, pp. 42-79.

Ainsi, la notion d'instrumentalisation de l'interdépendance reconnaît le rôle crucial des acteurs privés – en particulier des multinationales – qui, dans le monde moderne interconnecté, ont souvent le pouvoir d'influencer non seulement les marchés, mais aussi les politiques, les sociétés et les individus. Ces acteurs peuvent utiliser leurs positions au sein de réseaux d'interdépendance pour promouvoir leurs propres intérêts, modeler les comportements et les préférences, et façonner les règles du jeu à leur avantage.

De cet état d'inégalité des rapports de force émerge de nouvelles questions : est-il souhaitable que des infrastructures importantes pour notre mode de vie contemporain soient détenues et gérées par des multinationales sur lesquelles nous avons peu de contrôle ? Face aux risques de dépendance qui naissent de la mondialisation des échanges dans un contexte d'inégalité de pouvoirs, comment mieux protéger les sociétés humaines ? Faudra-t-il remettre en question ce mode de vie où le numérique tient une part importante ? Faudra-t-il plutôt travailler à mieux gérer les relations de dépendance et d'indépendance associées à l'activité numérique ? De ces nouvelles questions peut émerger une gestion des risques liés à la mondialisation, qui reposerait notamment sur une analyse des seuils de dépendance[17] et un rééquilibrage des leviers de pouvoirs qui impliquerait une maîtrise des technologies et une réappropriation infrastructurelle.

[17] Dans le cas spécifique des câbles sous-marins, il peut être utile de considérer les niveaux de dépendance d'un pays par rapport aux propriétaires de ces infrastructures. Pour reprendre l'exemple du continent africain, la situation de dépendance varie ainsi nettement d'un pays à un autre selon le nombre de câbles connectés, et la situation géographique du territoire (accès ou non au littoral). Mais à cela s'ajoutent de nombreux critères, tels que la capacité du pays à négocier ses propres atouts, à produire lui-même ses technologies, ou à mettre dans la balance la concurrence pour l'accès à son marché.

Imagerie satellitaire et souveraineté : de la donnée à son exploitation, vers un *continuum* public-privé

Par François BOURRIER-SOIFER
Directeur général adjoint de la société Preligens

La notion de souveraineté a retrouvé récemment une place centrale dans le débat public, sans pour autant que soit réellement renouvelée la dichotomie de l'action de l'État entre une conception patrimoniale (*dominium*) et le contrôle (*imperium*). Or, dans le secteur de l'imagerie satellitaire, compte tenu de l'essor du *New Space*, il semble que l'optimum puisse être de privilégier une forme d'hybridation entre la propriété et l'impact, de la donnée à son exploitation. À cette fin, l'État devrait poursuivre la création d'un écosystème articulé sur une forme de *continuum* public-privé. Il maximiserait ainsi l'effet final recherché : la puissance en actes, dictée par l'impératif d'autonomie stratégique.

La question de la souveraineté a récemment retrouvé une place centrale dans le débat public en France, très certainement en raison de la conjonction de deux événements majeurs : au printemps 2020, l'arrêt brutal de l'économie mondiale et la mise en évidence de dépendances critiques ; et, depuis fin février 2022, le retour de la guerre conventionnelle, aux portes de l'Europe, avec une grande puissance belligérante.

Ces évènements ont mis fin à au moins deux illusions cultivées depuis les années 1990.

La première illusion était politique. Elle consistait à penser qu'après la chute du mur de Berlin et la fin de la guerre froide, tous les États convergeraient vers un modèle démocratique. Cette croyance se fondait notamment sur l'idée « d'un sens de l'Histoire », voire de la fin de celle-ci, et s'appliquait aux grandes puissances comme la Russie et la Chine mais aussi aux autres continents et aux pays dits du Sud, la rivalité entre États ne devant alors s'exprimer que de façon pacifiée à travers une forme de concurrence « financiaro-industrielle ».

La seconde illusion était économique, considérant que l'économie de marché et le capitalisme étaient les modèles universels devant permettre à chaque instant la meilleure allocation des ressources pour la satisfaction des besoins de l'humanité. En termes d'accès aux ressources, la mondialisation laissait penser que chaque État pouvait répondre à ses besoins en matières premières essentielles au meilleur tarif.

Aussi, dans un contexte international à nouveau marqué par le triptyque compétition, contestation et confrontation, l'État et l'opinion publique, en France comme ailleurs en Europe et dans le reste du monde, accordent une importance croissante aux enjeux de souveraineté.

Or, le domaine spatial est critique pour la souveraineté d'un État. La capacité à envoyer des charges utiles hors de l'atmosphère et l'exploitation des technologies en orbite (géolocalisation, communication, observation, etc.) sont différenciantes d'un point de vue géopo-

litique. En particulier, l'imagerie satellitaire – de la donnée à son exploitation – confère des avantages aux niveaux stratégique, opératif et tactique, c'est-à-dire, en un sens, une capacité à ne pas faire la guerre ou à la gagner.

Des errements à ce sujet seraient particulièrement dommageables, alors que toutes les grandes puissances accroissent leurs efforts et que de nouveaux entrants apparaissent.

Le pouvoir absolu reste une illusion

La souveraineté, à l'échelle d'un État moderne, dans son acception la plus conceptuelle, la plus parfaite, reste une illusion. Sans reprendre littéralement le constat de Jean Bodin, il va de soi que l'État ne peut s'abstraire des marchés, des ambitions exogènes, des intérêts privés, des aspirations de sa population, etc.

En pratique, il est toujours impossible d'être à la fois autarcique, le plus puissant et le meilleur ; en particulier pour un pays comme la France qui n'est pas la première puissance mondiale ni économique, ni militaire, ni diplomatique, ni académique.

Les États doivent alors choisir leurs alliances et leurs dépendances au risque de se retrouver seuls et faibles car débordés technologiquement, économiquement, militairement. La question est donc de savoir si nous recherchons la pureté conceptuelle de la souveraineté – le mot – avec l'isolement et la potentielle vulnérabilité qu'elle engendre ou si, plus pragmatiquement, nous acceptons des dépendances mesurées en contrepartie d'une puissance – la chose –, relative mais effective.

Construire la puissance, entre *dominium* et *imperium*

L'État seul ne peut pas tout et il n'est que l'un des facteurs de la puissance d'une Nation. Souvent mentionné en pareilles circonstances, Thucydide notait déjà dans *Histoire de la guerre du Péloponnèse* que « La force de la cité ne réside ni dans ses remparts, ni dans ses vaisseaux, mais dans le caractère de ses citoyens »[1].

Certains facteurs de puissance sont indépendants de la volonté de l'État (sauf conquête territoriale) : le territoire ou la présence de ressources naturelles (indépendamment de leur gestion). D'autres relèvent de la volonté de la Nation et de choix politiques :

- un État stratège ;
- une économie innovante (éducation, recherche, investissements, culture du risque) ;
- une société résiliente ;
- des alliances solides.

Pour les États comme la France, parfois qualifiée de « grande puissance moyenne »[2], la limitation des ressources budgétaires et humaines impose de faire des choix, de fixer des priorités. Ces choix portent sur les moyens de la puissance (par exemple : la culture, la recherche, l'industrie, les services, l'espace, les données, etc.) et sur la façon dont l'État exerce son autorité (exemple : monopole étatique, initiative privée, planification, programmation, etc.).

Le pouvoir que l'État peut exercer relève alors soit du droit de propriété, le *dominium*, soit de sa capacité à commander, à imposer sa norme, l'*imperium*. L'État moderne n'est

[1] *Histoire de la guerre du Péloponnèse*, 431-411 avant notre ère, trad. Jacqueline de Romilly, Robert Laffont éditeur, coll. Bouquins, 1990.

[2] Selon les termes du président de la République Valéry Giscard d'Estaing.

pas en mesure de posséder en propre l'ensemble des secteurs stratégiques (*dominium*) mais il peut en revanche exercer son *imperium* sur les acteurs économiques. Ces deux façons pour l'État d'imposer sa volonté ne sont pas contradictoires ; elles sont même complémentaires.

Dans le domaine spatial, l'État a progressivement confié la maîtrise industrielle à des entreprises tout en conservant, notamment à travers le CNES et les budgets des armées, une maîtrise de la politique spatiale. L'État ne reste propriétaire (*dominium*) que des capteurs ou moyens de communication les plus pointus et pour le reste utilise les moyens déployés par des entreprises privées. Il est en revanche important que l'État puisse, à travers sa capacité à édicter les règles (*imperium*), imposer un comportement conforme à sa stratégie de sécurité nationale. Par exemple, en organisant le contrôle de l'exportation de certains composants ou données vers d'autres États ou opérateurs privés. Empêcher de faire, ou faire faire, plutôt que de tout faire soi-même est bien l'un des axes stratégiques pour que l'État préserve sa puissance.

Dit autrement, l'État n'a pas besoin de tout posséder, à rebours d'une conception patrimoniale et d'une logique de stocks. Il peut aussi contrôler, ou maîtriser, dans une logique d'impact et de flux.

La souveraineté à l'épreuve du *New Space*, un partage public-privé des capteurs

Le *New Space*, né aux États-Unis au début des années 2000 est caractérisé par la standardisation et la baisse des coûts, la multiplication des usages civils, la multiplication des acteurs privés avec un mix entre les empires du numérique (Gafam) et une profusion d'entreprises initialement de petite taille.

Quelques chiffres

En 2000, environ 800 satellites étaient en orbite ; ils étaient 8 000 fin 2021. Pour la seule année 2022, 179 lancements orbitaux (États-Unis, Chine, Russie, Union européenne, Inde, Corée du Sud, Nouvelle-Zélande et Iran) sont intervenus et 2 469 satellites ont été déployés (le double de l'année 2020) dont plus de 70 % dans le cadre de la constellation Starlink (1 722 satellites). En termes d'applications, 80 % sont des satellites de télécommunication et 8 % des satellites d'observation de la Terre et de reconnaissance. À elle seule, l'activité de la société d'Elon Musk représente près des deux tiers (64 %) de la masse totale satellisée en 2022, dont 50 % uniquement pour sa constellation Starlink.

Une bascule

L'évolution majeure des dernières années porte non seulement sur le nombre de satellites en orbite mais surtout sur le nouveau partage entre puissance publique et entreprises privées. Alors que jusqu'à la fin des années 2000 les lanceurs et les satellites étaient la propriété de l'État ou de personnes publiques, aujourd'hui ils sont possédés et exploités par des entreprises à des fins principalement commerciales. L'occupation de l'espace n'est plus le monopole de la puissance publique.

L'objectif de souveraineté ou de puissance impose de conserver cette autonomie d'accès à l'espace (un port, des lanceurs, des satellites – partie amont des activités). Mais il faut aussi dès aujourd'hui gagner la bataille des outils d'analyse (partie aval), notamment à l'aide d'intelligence artificielle.

La puissance à l'épreuve de la donnée

Le développement des activités commerciales d'origine spatiale ne doit pas faire oublier l'intérêt stratégique que l'espace représente pour l'acquisition du renseignement d'intérêt militaire. Depuis l'espace, le recueil d'informations peut s'opérer de manière très discrète en s'affranchissant des frontières et du respect de la souveraineté territoriale des États.

Comme le mentionnait le rapport annuel de la Délégation parlementaire au renseignement (DPR)[3] : « En quelques années, les progrès technologiques ont profondément et durablement changé la donne du renseignement d'origine spatiale. Très haute résolution, miniaturisation, mise en orbite de constellations, développement de l'intelligence artificielle : de véritables révolutions sont à l'œuvre qui viennent élargir considérablement le champ des possibles ».

« L'amélioration continue du niveau de résolution des images, associée à l'augmentation du taux de revisite grâce à la mise en orbite de constellations provoque une hausse considérable du nombre de données disponibles ». La question aujourd'hui n'est plus, comme trente années auparavant, d'acquérir la donnée mais d'identifier dans le flot de données celles qui permettront de créer de l'information.

À titre d'exemple, en 2017 le directeur de la National Geospatial-intelligence Agency américaine (NGA) indiquait[4] : "And whether our new persistent view of the world comes from space, air, sea, or ground – in five years, there may be a million times more than the amount of geospatial data that we have today. Yes, a million times more.".

"So just how big is this rising tide? If we were to attempt to manually exploit the commercial satellite imagery we expect to have over the next 20 years, **we would need eight million imagery analysts**. Even now, every day in just one combat theater with a single sensor, we collect the data equivalent of three NFL seasons – every game. In high definition!". Aujourd'hui la NGA peut recevoir, semble-t-il, plus d'un million d'images quotidiennement alors qu'en douze ans entre 1960 et 1972 (première génération de satellite), elle n'avait reçu que 860 000 images de la Terre.

« En quelques années, le flux d'images prises depuis l'espace a été multiplié par cinq, et cette évolution va se poursuivre grâce à des systèmes de plus en plus performants. L'arrivée de constellations de plusieurs dizaines, voire centaines, de satellites, va en effet générer une véritable explosion du volume d'images disponibles qu'aucun opérateur humain ne pourra traiter et analyser en temps réel ». La surabondance a remplacé la pénurie mais il faut maintenant être capable de traiter et d'extraire la valeur ajoutée de ces données. Le seul discernement humain n'est plus suffisant pour traiter ce *big data*.

La couche algorithmique et logicielle de traitement de ces données devient alors à son tour un sujet de souveraineté et de puissance. Cet enjeu déborde la question des seules données d'origine spatiale. Les lois de 2015 relatives au renseignement ont autorisé l'usage d'algorithmes (traitement automatisé des données) pour traiter des masses d'informations dont le volume ne permet pas l'exploitation par des ressources humaines limitées ; « L'intelligence artificielle est la clé de la transformation de la donnée en renseignement, que ce soit à des fins civiles ou militaires »[5]. Dès lors, si l'on considère que l'innovation et les talents nécessaires pour performer sur ce segment se trouvent aussi dans les entreprises privées (prises de risques, attractivité, agilité, etc.) se pose ici la

[3] Rapport de 2020, n°506 Sénat, n°3087 Assemblée nationale, relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020.

[4] https://breakingdefense.com/2017/06/cardillo-1-million-times-more-geoint-data-in-5-years/

[5] Rapport de 2020, n°506 Sénat, n°3087 Assemblée nationale, relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020.

question de l'*imperium*. Comme pour la production de satellites ou l'accès aux lanceurs, les intérêts souverains et commerciaux sont interdépendants.

La préservation de la puissance suppose de garantir un accès indépendant aux systèmes et aux données spatiales autour d'une réelle filière de la donnée, combinant opérateurs publics et privés nationaux sur l'ensemble de la chaîne, de l'amont (collecte) à l'aval (usages) en passant par l'analytique.

L'Espace reste un outil stratégique de puissance

La France doit conserver une maîtrise de l'Espace : une clé de la dissuasion

La dissuasion nucléaire est depuis 1972 la pierre angulaire de la défense française. Le pays dispose, à travers ses industriels, d'une maîtrise de la totalité des technologies qui permettent d'entretenir et de moderniser les deux composantes de la dissuasion. Historiquement, dès les années 1960, le développement des vecteurs civils et militaires (fusée diamant / missile balistique M1) furent intimement liés. La recherche spatiale fut duale dès ses origines.

La France doit conserver une maîtrise des données : une clé du renseignement

Au début des années 1990, lors de la première guerre du Golfe, 98 % des images satellitaires était fourni par les États-Unis. Aujourd'hui, la France dispose d'une panoplie de capteurs qui lui offrent une autonomie d'appréciation des situations. La qualité du renseignement autonome conditionne la liberté de décision politique comme l'a parfaitement démontré le choix du président de la République de ne pas participer à la deuxième guerre du Golfe en 2003. Ce choix a été rendu possible grâce à la capacité de renseignement autonome de la France.

L'élaboration en 2018 d'une nouvelle stratégie spatiale de défense nous semble marquer la reprise de conscience politique des enjeux de sécurité nationale et le réveil industriel indispensable pour y répondre.

« Tout le temps perdu ne se rattrape plus »[6] : des retards inquiétants

Dans la course à l'innovation, les retards s'accumulent. L'Espace qui était un secteur d'excellence française se voit distancé par le *New Space* américain, la conquête chinoise, la constance russe et les efforts accrus des pays en position de challenger (Inde, Allemagne, Italie, Israël, Japon, etc.). Constatant la crise du secteur spatial européen, le président de la République a enjoint aux ministères, aux établissements publics et aux entreprises à capitaux français de combler leur retard et de définir une nouvelle stratégie spatiale.

Les enjeux portent à la fois sur l'amont – les lanceurs, un marché mondial de l'ordre de 15 milliards d'euros par an – et l'aval, un marché dix fois plus grand. Pour les lanceurs, s'agissant des gros porteurs, Ariane 5 a eu une brillante carrière qui vient de s'achever. Ariane 6 est en retard. Pour finir la constellation Galileo, les lanceurs Soyouz pouvaient être appropriés, mais la guerre a mis fin à la coopération entre l'Europe et la Russie en l'espèce. Et pour les petits lanceurs, type Vega, la fiabilité est encore sensiblement plus faible que celle qu'avait atteint Ariane 5, avec plus de 98 % de taux de succès. Il y a donc un *gap* à combler d'abord en réussissant Ariane 6, ensuite en lançant la génération

[6] Barbara, *Dis, quand reviendras-tu ?*

future. Pour ce qui concerne l'aval, il ne faudrait pas que le retard s'accumule aussi, en particulier s'agissant de la capacité d'analyse des données produites par l'ensemble des capteurs mis en orbite. En effet, il pourrait s'avérer inutile d'être souverain sur le segment des capteurs si les acteurs publics et privés nationaux ne sont pas en mesure de traiter de façon autonome les données recueillies.

Selon une étude de l'OCDE (2019), *L'intelligence artificielle dans la société*, (Éditions OCDE, Paris), les entreprises américaines et chinoises évoluant dans le domaine de l'intelligence artificielle ont capté ensemble environ 80 % des investissements mondiaux de capital-risque (États-Unis 56 %, Chine 24 %, Union européenne 4 % – dont 1 % en France). Les trois-quarts des brevets en matière d'IA, déposés entre 2010 et 2022, sont américains (États-Unis 30 %, Canada 1,9 %) et asiatiques (Chine 26 %, Japon 12 %, Corée du Sud 6 %). L'Europe (l'Allemagne 5 %, le Royaume-Uni 2,5 % et la France 2,4 %) est, elle, en net retrait.

En matière de défense, la Chine investit 1,6 milliard de dollars par an sur l'IA *via* un programme baptisé « Chine 2025 » dans lequel Pékin énonce les secteurs dans lesquels le pays ambitionne de devenir numéro un mondial. Pour les États-Unis ce sont 2,5 milliards de dollars par an. Jusqu'à récemment, la France y consacrait 100 millions d'euros par an, soit 25 fois moins.

La France dispose de formidables atouts en termes de recherche fondamentale (INRIA, CNRS, centres 3IA)[7], de recherche appliquée dans les entreprises et un coordonnateur national à l'IA a été désigné dès 2018. Pour autant l'ambition doit être renouvelée si l'objectif est de s'assurer que la France soit demain l'une des grandes Nations de l'IA, à la pointe de l'état de l'art, capable d'analyser toutes les données dont elle a besoin pour comprendre le monde et imposer sa place. Dans une logique de puissance, un souci d'autonomie stratégique, au-delà de la souveraineté.

[7] Rapport de la Cour des comptes d'avril 2023 sur « La stratégie nationale de recherche en intelligence artificielle ».

La commande publique : un accélérateur de la souveraineté numérique

Par Jean-Noël de GALZAIN
Président Hexatrust & Wallix

Et Alain GARNIER
Président EFEL & Jamespot

La commande publique joue un rôle crucial dans la promotion de la souveraineté numérique. L'adoption massive d'outils numériques durant la pandémie a rendu les entreprises plus dépendantes des grandes plateformes étrangères. Pour préserver notre autonomie et notre capacité à exceller dans un monde dominé par l'IA, il est essentiel de recourir davantage à des solutions françaises ou européennes dans les marchés publics, en particulier pour les achats stratégiques et la protection des données sensibles.

En se positionnant dès aujourd'hui sur les solutions numériques souveraines, la France peut reprendre le contrôle de ses données personnelles et industrielles, garantissant ainsi sa liberté, son autonomie et sa capacité d'innovation. L'État peut jouer un rôle plus directif et coercitif pour favoriser l'adoption de solutions souveraines dans les administrations et les entreprises publiques.

L'avenir dépendra des décisions prises au niveau européen, mais la France peut montrer l'exemple en avançant sur la voie de la souveraineté numérique.

En 2020, le monde bascule dans le digital pour maintenir les liens personnels et professionnels en période de confinement. Le travail passe en mode collaboratif. Les outils Office 365, Zoom, Teams, Slack… envahissent nos journées, nos entreprises et nos écrans. Souvent gratuits, facilement disponibles, proposant une expérience utilisateur simple, ils sont rapidement adoptés par le plus grand nombre. En cette période d'urgence, l'heure n'est pas à la réflexion sur les conséquences et les risques. La continuité de l'activité à tout prix efface toute considération sur les risques en matière d'autonomie et de préservation de nos données.

Cette petite révolution nous a rendus encore plus dépendants numériquement des grandes plateformes, alors même que ces solutions ne répondent pas ou partiellement à nos lois européennes en matière de protection des données personnelles et stratégiques. Nous laissons ainsi partir chaque année un peu plus nos data, rendant toujours plus difficile notre capacité à exceller demain, dans un monde dominé par l'IA : sans donnée, pas d'Intelligence Artificielle française ou européenne !

Aujourd'hui, notre pays doit tout mettre en œuvre pour rééquilibrer le jeu, au profit de notre économie, de notre sécurité et de notre avenir. La souveraineté numérique ne peut plus être un sujet secondaire, c'est l'instrument de notre autonomie. Pour l'instaurer, le recours systématique à des solutions françaises ou européennes dans la commande publique doit être encouragé au plus haut niveau, voire imposé dans les achats sur les marchés stratégiques ou la protection des données sensibles !

Le virage collaboratif

Depuis trois ans, dans les entreprises, le standard collaboratif a changé. La pandémie a fait plonger le monde du travail dans l'ère de la *digital workplace* qui est devenue le nouveau bureau, dans une configuration où l'utilisateur se connecte à distance à son organisation. À mesure que les pratiques s'installent et s'intensifient, les entreprises commencent à se poser enfin les bonnes questions, adoptant une vision à plus long terme. La question de la protection des données stratégiques revient au centre des réflexions.

Faut-il encore faire connaître aux dirigeants les solutions alternatives souveraines françaises ou européennes qui existent pour répondre à leurs besoins, et les différenciateurs clés. Face à la domination sans partage des Gafam sur le marché du logiciel collaboratif, seule la commande publique et la régulation paraissent de nature à rééquilibrer le marché sur une approche exemplaire au niveau de la protection des données sensibles.

De la nécessité d'orienter et de favoriser la commande publique

Pour freiner la prolifération de batteries électriques chinoises sur son sol, le gouvernement américain a débloqué 4 milliards sur les 420 milliards de son plan IRA (*Inflation Reduction Act*), pour relancer la commande publique dans ce domaine. Cet investissement est loin d'être un cas isolé du protectionnisme de l'Oncle Sam. Les Américains ont instauré, dès 1953, le *Small Business Act*, qui favorise les petites et moyennes entreprises dans le tissu économique du pays. Aujourd'hui, entre 23 et 40 % de l'achat public est réservé aux PME.

En France, beaucoup d'actions positives ont été menées ces dernières années en matière de formation et d'évolution réglementaire. Pourtant, ce sujet d'un *Small Business Act* à la française reste un serpent de mer, qui revient régulièrement dans les propositions mais se heurte à des freins qui seraient liés à la réglementation européenne en matière de libre concurrence. Certains responsables politiques estiment ainsi qu'il est impossible de favoriser les entreprises françaises ou européennes sans créer une distorsion sur un marché mondialisé.

Des propos plutôt « étonnants » voire « suicidaires » lorsque l'on sait à quel point ce déséquilibre est déjà profond et qu'il se fait au détriment de notre économie et de notre autonomie stratégique. De plus, ceux qui prétendent encore qu'il n'existe pas de solutions alternatives à celles des géants américains ou chinois, ne font que révéler une profonde méconnaissance de notre écosystème numérique et des innovations qu'il fait éclore, écosystème financé partiellement par des financements publics (recherche publique, CIR, JEI, FCPI, France Relance…). Notre pays a réussi aujourd'hui à faire émerger des éditeurs et des acteurs de « La French Tech » dont les solutions sont parfaitement compétitives en termes de performance et de coûts. Elles sont, de plus, nativement adaptées à notre culture, nos contraintes en matière de support local ou de réglementation, ce qui favorise leur intégration dans nos entreprises et nos administrations, ainsi que leur pérennité.

Un rôle modèle à tenir

L'État français a un devoir régalien en matière de culture, d'éducation, de sécurité et de compétitivité de nos entreprises. Il lui revient de préserver les équilibres dans ces domaines stratégiques.

La commande publique apparaît ainsi comme un véritable accélérateur pour notre économie, décisif pour notre industrie, tout en contribuant à la richesse du pays. Sans

la dilapider, elle doit servir la visibilité de notre écosystème numérique et son devenir industriel. Il s'agit, dans un premier temps, de relocaliser notre chaîne de valeur sur nos territoires, ainsi que nos savoir-faire et notre culture. Rien qu'avec l'avènement du collaboratif et du télétravail, le marché est considérable. Nos entreprises doivent prendre part au festin.

Avoir le courage de cette démarche implique des investissements importants, pour faire le poids face à des acteurs monopolistiques et extraterritoriaux. Cependant, ces investissements existent déjà, il s'agit donc de les réallouer pour un retour sur investissement à moyen terme sur notre industrie et notre pays. D'autant qu'en faisant la promotion de nos entreprises en devenir, l'État crée de nouvelles rentrées fiscales, les grosses compagnies étrangères étant peu enclines à payer leurs impôts en France. La commande publique, c'est donc aussi le moyen de promouvoir une approche respectueuse des citoyens que nous sommes, une approche exemplaire en matière fiscale et sociale.

Bâtir des filières numériques stratégiques : le plan France 2030

Les organismes d'État et l'administration française, notamment, doivent être exemplaires en matière de choix d'hébergement de leurs données stratégiques et sensibles. Elles devront pour cela, identifier les solutions souveraines propres à chaque domaine d'application. La France répond aujourd'hui à ce défi avec le lancement d'appels à projets, dans le cadre du plan France 2030. Il s'agit de financer et d'encourager les opérateurs locaux à se regrouper en consortiums, afin d'apporter une réponse globale aux besoins souverains dans l'administration et chez les Opérateurs d'importance vitale (OIV)… Des collaborations naturelles pour construire une autonomie numérique avec un cadre de la confiance numérique dans notre pays.

Ce plan vise à redynamiser et/ou à construire nos filières stratégiques, en nous repositionnant sur les socles techniques et numériques. C'est déjà le cas pour la cybersécurité qui s'organise en filière dans le Comité Stratégique de Filière des Industries de sécurité qui regroupe les industriels du domaine. Et ce sera bientôt le cas, dans le nouveau Comité Stratégique de Filière du numérique de confiance, qui vient là aussi regrouper les industriels (autrement dit les producteurs de technologies) autour d'un contrat de filière commun industriels & DGE (Direction générale des Entreprises).

Un exemple concret de ce plan est mis en œuvre à travers des panels de manifestations d'intérêt financés par l'État. Notamment sur le besoin d'une solution bureautique souveraine dans le *cloud*. Plus d'une cinquantaine d'entreprises se sont regroupées pour répondre à ces appels à projets. Trois groupements ont été retenus, parmi lesquels, CollabNext. Ce consortium est porté par Jamespot. Il s'inscrit dans le cadre de l'appel à manifestations d'intérêt : « Suites bureautiques collaboratives *cloud* ». Il vise à ériger une offre numérique de confiance en France et, à la passer à l'échelle en conduisant les principaux acteurs français en matière de solutions collaboratives souveraines à s'adosser aux acteurs *leaders* du *Cloud* de confiance et de la cybersécurité, en l'occurrence 3DS Outscale et WALLIX pour le projet CollabNext. Ensemble, ils vont constituer une chaîne de valeur avec des fonctionnalités innovantes, à la fois plus complète et mieux sécurisée, qualifiée SecNumCloud pour la protection des données sensibles par *design*.

Au total, 23 millions d'aides France 2030 seront mobilisées pour financer ces projets. Assez pour donner une impulsion à l'offre française de *digital workplace*. Pour aller au-delà et créer les conditions d'une relance de l'économie numérique, il y aura notamment besoin du levier de la commande publique. En faisant émerger des alternatives crédibles sur les besoins en matière de numérique, avec des différenciateurs clés attendus à l'abri des lois extraterritoriales en matière de confiance numérique, la France s'organise pour créer et

préfigurer un futur contrat de filière numérique de confiance, essentiel pour répondre à nos besoins massifs.

Un cercle vertueux

L'ambition du Gouvernement est de permettre à son administration et aux OIV notamment, de trouver la meilleure offre numérique dans différents segments de niche : *digital workplace*, réalité augmentée, IA, *cloud computing*, *quantum computing*, cybersécurité…

La constitution d'une offre technologique de produits et services souverains va permettre aux entreprises qui en ont besoin de s'équiper tout en se mettant en conformité avec la réglementation européenne en matière de protection des données, conformément à la Directive NIS2 sur les Opérateurs de Services Essentiels.

Aujourd'hui, nous avons les solutions, l'écosystème et les acteurs de la filière. Ce sont souvent des *pure players* technologiques, positionnés dans le logiciel ou le *cloud*, souvent *start-up*, PME de croissance ou ETI comme OVH Cloud, Outscale ou Docapost ; elles sont moins connues que les géants américains ou chinois. Cependant, elles proposent des solutions compétitives en matière de prix comme de fonctionnalités et appliquent les réglementations européennes ou françaises en matière de protection des données.

Dans le milieu hospitalier, particulièrement exposé en matière de données sensibles, la filière Cyber a déjà apporté la preuve qu'il était possible d'organiser un cercle vertueux entre l'offre et la demande. Grâce aux parcours de cybersécurité établis par l'ANSSI (l'Agence nationale de la sécurité des systèmes d'information) sous l'angle des besoins utilisateurs, avec le soutien à la demande du fonds France Relance, et de manière coordonnée avec les industriels, la preuve a été faite que 85 % des besoins exprimés ont trouvé de l'aide avec des solutions made in France, 95 % en y intégrant des solutions *made in Europe*. Et ce sans modifier la régulation.

Il faut donc pérenniser ce cercle vertueux entre l'utilisateur qui a des besoins, l'État qui régule et qui soutient, enfin l'industrie qui répond, en conformité avec les règles françaises et européennes. C'est exactement l'objectif du consortium CollabNext.

Se positionner dès aujourd'hui pour être des leaders demain

L'idée de groupement est d'autant plus importante, qu'en créant des *digital workplaces* souveraines, nous nous donnons les moyens de capter des données qui, demain, alimenteront nos IA et notamment, les IA génératives si prometteuses. Les grandes puissances étrangères ont pris de l'avance dans ce domaine grâce à un facteur essentiel : elles disposent déjà de leurs données et des nôtres ! Nous devons reprendre le contrôle de nos données personnelles mais aussi garder le contrôle de nos données industrielles. Et ce parce qu'elles nous appartiennent, qu'elles sont un marqueur clé de notre liberté, de notre autonomie et de nos innovations à venir. Elles permettront en outre de créer des espaces de recherche plus importants pour notre IA. Cet enjeu ne se limite pas seulement au besoin des utilisateurs. Il s'étend à la façon dont nous voulons nous projeter dans le monde de demain. Un monde qui nous ressemblerait et où nous souhaitons préserver nos chances d'être entrepreneurs et *leaders*.

L'État devra-t-il se montrer plus directif voire coercitif lorsque les règles ne sont pas respectées ? Obliger nos administrations ou nos entreprises publiques à migrer vers des solutions numériques souveraines comme pour l'emblématique Health Data Hub par exemple ? Saurons-nous utiliser la commande publique pour faire grandir notre filière numérique d'excellence ? Que ressortira-t-il du *Digital Act*, du DSA et du DNA sur

lesquels légifère actuellement la Commission européenne ? La France peut-elle montrer l'exemple en avançant comme elle le fit sur les OIV ou la Cnil ?

Rien n'est encore écrit. Cependant, grâce aux aides à l'innovation et au financement d'amorçage, nous avons été capables de faire de la France la *start-up* Nation européenne. Pour passer le plafond de verre et transformer cette *start-up* Nation en génération d'ETI industrielles, nous n'avons pas seulement besoin de licornes surcapitalisées, mais d'accès aux marchés stratégiques des grands donneurs d'ordre publics et privés pour passer à l'échelle supérieure. C'est pourquoi il est aujourd'hui nécessaire d'avancer en France et en Europe, sur un *Small Business Act* et un *European Tech Buy Act* pour transformer l'essai. À ceux qui pensent cela impossible disons le tout de suite, il n'y a pas de combat perdu d'avance ! Nous avons avancé il y a moins de dix ans sur des grands sujets devenus depuis des standards européens en inspirant le RGDP, la Cnil et plus récemment la directive NIS.

C'est dans cet état d'esprit que nous devons continuer à inspirer le monde, en transformant nos besoins en moteur, nos réglementations en tuteurs, notre industrie en instrument d'autonomie, d'innovation et d'emploi.

Alors que l'État veut réindustrialiser la France, le numérique est au cœur de ces enjeux. Comme l'énergie, il est un secteur transverse à tous les autres. Pour notre industrie, le tourisme, le transport, le commerce, l'agriculture et la décarbonisation de notre pays. En cas de nouvelle crise mondiale, nous aurons besoin d'autonomie numérique dans le *cloud*, les services et les applications que nous utilisons.

L'Europe a mis en place des fonds, des initiatives, des réglementations et des moyens. La France doit garder son inspiration et donner l'impulsion comme elle l'a fait jusqu'ici. Soyons donc le moteur d'un numérique de confiance en Europe !

Manque à gagner pour l'Europe de ne pas avoir sa « souveraineté numérique »

➔ 160 milliards d'euros par an, soit 32 milliards d'euros pour la France.

Source : 190 milliards d'euros de dépenses informatiques en Europe (chiffres PAX 2020), 76 % du numérique en Europe est hors Europe (CSF Numérique de confiance).

Gouvernance mondiale d'internet : les leviers

Par Lucien CASTEX
AFNIC

« Faites que le rêve dévore votre vie afin que la vie ne dévore pas votre rêve »,
Le petit prince

La transformation numérique de la société fait d'internet un objet du quotidien entre usages et artefacts techniques. Sa gouvernance est caractérisée par un modèle *ad hoc* empruntant tant au multipartisme qu'au multilatéralisme ou qu'aux usages du réseaux. Celle-ci est aujourd'hui disputée, au cœur d'une lutte de pouvoir autour du réseau des réseaux.

Les venelles de l'information d'antan sont devenues les routes du *cyberspace* désormais très fréquentées. L'entrée dans la galaxie Marconi fait de chacun un voisin de palier, mêlant communauté virtuelle, interactivité, le tout dans une matérialité bien réelle.

Internet se matérialise tant par les câbles, équipements réseaux et constellation de satellites que par les frontières. Ce sont quasi 500 câbles sous-marins en 2023, Marea, Dunant, Amitié, qui permettent au trafic internet de circuler, tissant une toile au fond des mers. Internet est devenu un objet du quotidien, espace de navigation et objet géopolitique où les frontières si elles sont plus difficiles à percevoir n'en sont pas moins présentes. Alors que la conférence des plénipotentiaires de l'Union internationale des télécommunications (UIT) se concluait en octobre 2022[1] en entendant poser des jalons pour l'avenir numérique et en adoptant un plan stratégique ambitieux avec l'objectif de connecter le monde et de favoriser une transformation numérique inclusive[2], les débats autour de l'évolution de la gouvernance de l'Internet sont féconds.

Internet est toujours en construction, tout autant que sa gouvernance, fruit d'une hybridation croisée entre une évolution des usages qui façonne l'internet de demain et une ambition démocratique, faisant du réseau des réseaux un bien commun[3] et une infrastructure essentielle.

[1] La conférence des plénipotentiaires de l'Union international des télécommunications a rassemblé des représentants de 183 pays membres à Bucarest, Roumanie, du 26 septembre au 14 octobre 2022.

[2] UIT, Actes finals de la Conférence de plénipotentiaires, 2022.

[3] Voir par exemple POHLE J. (2018), "The Internet as a global good: Unesco's attempt to negotiate an international framework for universal access to cyberspace", *International Communication Gazette*, vol. 80, issue 4, pp. 354-368.

L'Émergence d'une gouvernance *ad hoc* d'internet

5,3 milliards d'utilisateurs fin 2022[4], soit 66 % de la population mondiale, font d'internet une croisée des chemins géopolitiques et périlleuse[5,6], *summa divisio* entre un modèle *ad hoc* de gouvernance et multilatéralisme. Alors que la pandémie de Covid-19 a accéléré la transformation numérique de la société, faisant état de la nécessité d'accéder à internet, quelques 2,7 milliards de personnes ne sont toujours pas connectées, principalement dans les pays en développement[7].

La gouvernance d'internet, « de l'Internet » dans les textes, passage fort de sens du nom propre au nom commun, s'est développée progressivement face au constat du développement rapide de la société de l'information. Réuni sous les auspices de l'Union internationale des télécommunications, le Sommet mondial sur la société de l'information (SMSI) s'est tenu en deux phases, la première à Genève du 10 au 12 décembre 2003, la seconde à Tunis du 16 au 18 novembre 2005. Il y est fait le constat d'une importance croissante d'internet et de la nécessité de favoriser le développement d'une société de l'information ouverte et inclusive. La déclaration de principes de Genève[8] reconnaissait dès 2003 la nécessité de « nouvelles formes de solidarité, de partenariat et de coopération entre les gouvernements et les autres acteurs, c'est-à-dire le secteur privé, la société civile et les organisations internationales »[9].

Kofi Annan, Secrétaire général des Nations Unies, invitait en novembre 2005 à reconnaître « la nécessité d'une plus grande participation internationale aux débats sur les questions relatives à la gouvernance de l'Internet » tout en soulignant la difficulté à trouver les moyens d'atteindre cet objectif[10]. Préalable et postulat à la fois, une définition de la gouvernance d'Internet est développée par le groupe de travail sur la gouvernance de l'internet (GTGI)[11]. Le GTGI a pour mandat de développer une « définition pratique de la gouvernance de l'Internet » de même que l'identification des « questions d'intérêt général qui se rapportent à la gouvernance de l'Internet » et l'élaboration d'une « conception commune des rôles et des sphères de responsabilité respectives des gouvernements, des organisations intergouvernementales, des organisations internationales et des autres forums existants, ainsi que du secteur privé et de la société civile, tant des pays en développement que des pays développés »[12]. En 2005 à Tunis, le groupe livre une définition pratique de la gouvernance d'internet qui se définit comme « l'élaboration et l'application par les États, le secteur privé et la société civile, dans le cadre de leurs rôles respectifs, de principes, normes, règles, procédures de prise de décisions et programmes communs propres à modeler l'évolution et l'utilisation de l'Internet ». Cette définition reconnaît

[4] International Telecommunication Union, Development Sector, "Measuring digital development: Facts and Figures", 2022.

[5] ROSSI J., MUSIANI F. & CASTEX L. (2022), « La gouvernance d'Internet, entre infrastructures et espaces socio-politiques : apports de la recherche », *Terminal*, pp. 132-133.

[6] BORTZMEYER S. (2018), *Cyberstructure. L'internet est un espace politique*, C&F Éditions.

[7] *Ibid*. p. 1, 2 et 24 (méthodologie).

[8] Sommet mondial sur la société de l'information, *Déclaration de principes*, WSIS-03/GENEVA/DOC/4-E, 12 décembre 2003.

[9] *Ibid*. par. 17.

[10] WSIS, United Nations, Statement by H.E. Mr. K. Annan Secretary General, Tunis, 16 November 2005, as delivered.

[11] Sommet mondial sur la société de l'information, *Geneva Plan of Action*, WSIS-03/GENEVA/DOC/0005, 12 December 2003.

[12] *Ibid*. par. 13.

le rôle spécifique et la pluralité des différentes parties prenantes dans l'élaboration des mécanismes de gouvernance. Si elle recueille un large accord, subsistent des interrogations quant au rôle des États, et aux modalités de souveraineté sur internet, et à la place de la diversité d'entités internationales amenées à se saisir d'internet. Outre l'UIT, créée à l'époque du télégraphe, et plus largement le système des Nations Unies, émergent progressivement des organisations spécialisées, l'ICANN en 1998, qui gère le système des noms de domaine et coordonne l'attribution des adresses IP, les différents registres Internet régionaux, l'*Internet Society* en 1992 ou l'*Internet Engeenering Task Force* (IETF) formée en 1986.

Point d'orgue de ce modèle *ad hoc* de gouvernance d'internet, le SMSI conduit en 2005 à la création d'un espace de dialogue entre les parties prenantes, le Forum sur la gouvernance de l'internet (FGI). Ainsi, l'agenda de Tunis à son paragraphe 72 invite la réunion « selon une approche ouverte et non exclusive » du forum et fixe son mandat, notamment « de traiter les questions de politique publique relatives aux principaux éléments de la gouvernance de l'Internet afin de contribuer à la viabilité, à la robustesse, à la sécurité, à la stabilité et au développement de l'Internet » ; et de faciliter le dialogue, l'échange d'informations et de bonnes pratiques, de renforcer les capacité en matière de gouvernance de l'internet et « de renforcer et d'accroître l'engagement des parties prenantes, en particulier celui des pays en développement ».

Le premier Forum s'est tenu à Athènes en 2006. Le FGI 2023 se tiendra à Kyoto au Japon, héritier de cette approche multipartite, mais aussi confronté à l'évolution d'internet et à l'émergence de nouveaux acteurs et d'un regain de tension – et d'intérêt – pour la chose numérique.

L'Évolution d'Internet à internet, des leviers de gouvernance

À l'approche de la revue à vingt ans du SMSI, le modèle de gouvernance d'internet se trouve confronté à sa propre évolution[13]. Depuis sa création, des initiatives régionales et nationales se sont développées, à l'instar du forum français sur la gouvernance de l'Internet (FGI France), levier d'action au niveau local qui permet de renforcer la diversité des discussions et amène à réfléchir Internet autrement. Objet du quotidien, l'évolution d'internet vers le tout connecté et son immixtion progressive dans toutes les couches de la société accentuent la tension entre un modèle *ad hoc* de gouvernance et le modèle multilatéral, où les frontières de la souveraineté nationale sont plus prégnantes. La volonté de renforcement de la résilience et de la sécurité des technologies numériques emporte, outre les nombreuses initiatives législatives de par le monde, l'émergence de nouveaux processus. De la neutralité d'internet[14], à sa fragmentation[15] ou au développement de nouveaux droits numériques, ce sont autant de sujets de controverse qui questionnent tant l'effectivité que les modalités[16] du modèle multipartite de gouvernance d'internet, parfois perçu comme ne bénéficiant qu'à quelques-uns.

[13] Voir pour référence la revue du SMSI à dix ans, la résolution adoptée le 16 décembre 2015, par l'Assemblée générale des Nations Unies (A/RES/70/125).

[14] CASTEX L. (2020), « La neutralité de l'Internet face au besoin de régulation » *in* Les enjeux contemporains des communications numériques (dir. Hélène de Pooter, Marine They), Éds Pedone.

[15] PERARNAUD C., ROSSI J., CASTEX L. & MUSIANI F. (2022), "'Splinternets': Addressing the renewed debate on internet fragmentation", [Research Report], Panel for the Future of Science and Technology, Parlement européen, Scientific Foresight Unit (STOA).

[16] BELLI L. (2016), *De la gouvernance à la régulation de l'Internet*, Boulogne-Billancourt, Berger-Levrault, 457 pages.

Les routes du cyberespace sont-elles pavées de bonnes intentions ? Choc des souverainetés, la volonté de reprendre la main sur les technologies numériques se fait en miroir d'un changement de narratif d'Internet qui permet du numérique comme activateur d'une mise en exergue – parfois en balance – des risques. Internet s'est construit comme un réseau ouvert et décentralisé où l'interopérabilité permet à des systèmes hétérogènes de parler une langue commune et d'interagir. Sa gouvernance n'en est pas autrement, un ensemble de briques successives, une coopération entre acteurs, aujourd'hui encore en construction.

C'est dans ce contexte que le Secrétaire général de l'ONU a créé le 12 juillet 2018 le groupe de haut niveau sur la coopération numérique avec pour objectif d'identifier les leviers permettant de renforcer cette coopération. Le groupe a remis son rapport intitulé « L'ère de l'interdépendance numérique » le 10 juin 2019. Afin de renforcer la coopération numérique, le rapport pose les bases des futures missions d'un envoyé du Secrétaire général pour les technologies, en particulier, la coordination des activités menées en matière de numériques au sein du système des Nations Unies afin d'assurer une cohérence globale et de faciliter le dialogue avec les parties prenantes. S'en suit le rapport « Notre programme commun », présenté à l'Assemblée générale de l'ONU le 10 septembre 2021, qui propose de mettre sur pied « un système multilatéral plus solide et plus inclusif, travaillant davantage en réseau et dont le socle serait le système des Nations Unies » et de développer un pacte numérique mondial avec pour objectif de « définir des principes partagés pour un avenir numérique ouvert, libre et sécurisé pour tous ». Un tel pacte devrait le cas échéant s'articuler avec l'Agenda 2030, et de ses dix-sept objectifs de développement durable, avec la Charte, de même qu'avec la Déclaration universelle des droits de l'Homme. En mai 2023, dans une note[17], le Secrétaire général des Nations Unies insiste sur la nécessité d'assurer l'implémentation et une évaluation régulière du pacte à l'aune de l'évolution des technologies proposant la création d'un nouveau Forum de coopération numérique. Quelle articulation avec les processus existants en particulier avec le FGI et le réseau des FGI nationaux et régionaux ?

Faut-il en revenir aux processus oubliés, IGF+[18] ou simplement assurer des ressources pérennes pour le FGI afin qu'il remplisse sa fonction première, permettre l'échange ? En somme, est-il besoin d'un nouvel espace multilatéral ou de réconcilier les processus afin de lutter contre les inégalités numériques ? Internet n'est pas achevé, sa gouvernance non plus, gageons que le rêve dévore notre vie.

[17] United Nations, Our Common Agenda Policy Brief 5, A Global Digital Compact - an Open, Free and Secure Digital Future for All, mai 2023.

[18] Le modèle dit « IGF+ », pour Internet Governance Forum Plus, était l'une des recommandations du Plan d'action de coopération numérique du Secrétaire général des Nations Unies (A/74/821) pour renforcer le FGI comme plateforme multipartite dotée d'une approche stratégique et d'un programme de travail pluriannuel.

Les évolutions des postures cyber : comment la Chine, la Russie, les États-Unis et l'Union européenne voient le monde

Par Rayna STAMBOLIYSKA
Fondatrice et directrice générale de RS Strategy

Certaines avancées technologiques sont si importantes qu'elles fracturent notre compréhension du monde. Les experts et les décideurs politiques commencent à disséquer, même si c'est parfois timidement, les conséquences potentielles de l'ajout de nouvelles technologies peu familières, avancées et potentiellement dévastatrices à la boîte à outils des puissances adverses. Dans ce contexte, les postures de cybersécurité présentent un attrait particulier. Ces postures permettent de mieux appréhender les changements stratégiques en cours chez les principaux acteurs de l'échiquier géopolitique. Ainsi, nous examinons la Chine, la Russie, les États-Unis et l'UE par le prisme de leurs postures cyber où se reflètent les visions civilisationnelles qui déterminent les actions à venir de ces acteurs. Ces stratégies reflètent les perspectives à long terme de ces acteurs, offrant ainsi un aperçu de leurs motivations et des éventuels angles morts à prendre en compte.

« Tous les 18 mois, le coefficient de QI nécessaire pour détruire le monde baisse d'un point »[1]. Comment penser sa place dans le monde face à la diversification des menaces et des acteurs capables de les matérialiser ?

Certaines avancées technologiques sont si importantes qu'elles fracturent notre compréhension du monde. Une telle rupture s'est produite avec la bombe nucléaire ; son avènement a transformé la conception de la guerre et de la puissance. Aujourd'hui, les progrès rapides des technologies recèlent le même potentiel, qu'il s'agisse de ciblage publicitaire, de ChatGPT ou encore d'informatique quantique. Les experts et les décideurs politiques commencent à disséquer, même si c'est parfois timidement, les conséquences potentielles de l'ajout de nouvelles technologies peu familières, avancées et potentiellement dévastatrices à la boîte à outils des puissances adverses.

Dans ce contexte, les postures de cybersécurité présentent un attrait particulier. Dans sa compréhension générique, il s'agit d'appréhender quels risques numériques pèsent sur les actifs stratégiques pour les en protéger. Si on adopte la définition la plus stricte, la posture cyber désigne la robustesse des approches de prévention et d'atténuation des cybermenaces, ainsi que la capacité d'agir avant, pendant et après un incident.

[1] Il s'agit de la « loi de Moore pour la science folle » (*Moore law for mad science*), un concept créé et popularisé par l'écrivain américain Eliezer Yudkowsky, http://web.archive.org/web/20071027141829/ ; http://www.acceleratingfuture.com/people-blog/?p=209

La posture cyber repose sur des politiques et procédures organisant les utilisations de logiciels, du matériel, des services, des réseaux et des informations. Il s'agit donc d'un concept dynamique en ce qu'il traduit l'existant ; il permet également une vision longitudinale qui soutient la prise de décision face à l'évolution des menaces et de l'appétence au risque.

Généralement appliquée dans le contexte d'une organisation, la notion de posture cyber peut être utilement mobilisée pour apprécier les principales tendances de gestion des risques. Ainsi, la posture cyber peut aider à comprendre des changements stratégiques le long d'un spectre qui comprend les opérations défensives et offensives, la dissuasion et la résilience. Une telle cartographie est également pertinente lorsqu'on souhaite projeter les lignes de démarcation face à la multiplication d'acteurs pouvant mobiliser des technologies actuelles et émergentes, qu'il s'agisse de leur consommation ou de leur production.

La technologie comme déterminant géopolitique dans un monde incertain

Lorsque le politologue américain Francis Fukuyama annonçait sa grandiloquente « fin de l'histoire », la puissance de créer des tensions et de parer les dangers était l'apanage quasi-exclusif des États. La proclamation aux allures de prophétie se voulait une assurance face à l'incertitude se déployant avec la fin de l'URSS : le modèle civilisationnel occidental de démocratie et de prospérité économique allait submerger le reste de la planète et confirmer l'idée selon laquelle l'essor économique mène inéluctablement à une gouvernance démocratique. La candeur de la vision selon laquelle l'émergence de classes moyennes aisées mènerait à la compétition de valeurs politiques et, de là, au pluralisme politique avait de quoi interpeller.

Quelques trois décennies plus tard, la Chine et la Russie témoignent de l'inanité de cette prédiction. Ni l'une ni l'autre n'a vu se développer un pluralisme politique viable avec son essor économique. Plus encore, chacune a su promouvoir et asseoir sa vision civilisationnelle, qu'il s'agisse de relations extérieures ou de critères pour jauger de la légitimité de ses têtes dirigeantes. Ces trois décennies ont démontré que le modèle occidental a une alternative viable : non seulement un régime autoritaire peut créer de la stabilité, mais il permet également l'innovation et l'émergence de *leaders* technologiques globaux.

Le développement concomitant du numérique a contribué à l'émergence d'innovations et accéléré la mise sur le marché de technologies de rupture. Les ruptures sous-entendues concernent les modifications profondes des comportements individuels et des interactions sociétales, bien plus significatives qu'une prouesse technologique spécifique. Aux côtés des puissances étatiques se sont rangés des acteurs transnationaux, non étatiques et privés, disposant de moyens d'action parfois spectaculaires. Pendant presque aussi longtemps que trois décennies, le numérique était un sujet d'expertise et d'ingénierie, avant de devenir un levier économique. Son rang d'objet politique est récent, la pandémie de Covid-19 ayant significativement accéléré cette reconnaissance. La tech est devenue politique, et, avec ce devenir, le numérique s'est retrouvé mobilisé pour soutenir des visions civilisationnelles distinctes.

La démocratisation de la destruction

Cette « montée en rang » n'est ni facilement acceptable par tous ni facilement gérable. Avec la porosité exceptionnelle des sociétés au numérique est venue une évolution des risques et une fragmentation des acteurs, donc des responsabilités.

Beaucoup plus prégnant aujourd'hui est le constat que l'accès à des technologies puissantes est possible avec un coût d'entrée souvent risible. La diversité des acteurs et des usages combinée à l'absence de débat public sérieux sur l'impact de la technologie sur le tissu sociétal et sur les individus créent ce que Timothy Shoup et August Leo Liljenberg (2023) du Copenhagen Institute for Futures Studies (CIFS) appellent la « démocratisation de la destruction »[2]. En associant ces deux termes, ils soulignent que la prolifération de technologies (notamment émergentes) diverses change la donne ; elle permet à des acteurs non étatiques, à des groupes de plus en plus petits et même à des individus, d'exercer et de projeter leur pouvoir pour faire des choses que seuls les États-nations (souvent de grands États-nations politiquement puissants, économiquement prospères et éduqués) pouvaient faire auparavant.

En effet, la barrière à l'utilisation de nombreux outils technologiques est extrêmement basse. Ce que la notion de « démocratisation de la destruction » projette est l'abaissement des seuils nécessaires à la mobilisation d'un outil complexe et multifonction. Ainsi, le premier seuil est la capacité cognitive de comprendre l'outil et ce qu'il peut faire. Le deuxième est la capacité à accéder à l'information et à comprendre comment l'outil fonctionne. Enfin, le troisième est le seuil de compétence, c'est-à-dire la manière dont la personne transforme son savoir en savoir-faire. Par conséquent, il est possible d'affecter une population significative avec un outil *a priori* anodin et avec un coût de mobilisation faible. Cette situation diffère profondément des dégâts provoqués par une bombe nucléaire : s'il est vrai qu'une population significative en serait affectée, l'outil n'a rien d'anodin et son coût de mobilisation est extrêmement important.

C'est sur cette toile de fond que se joue le déploiement des visions civilisationnelles des principaux pôles de puissance (géo)politique, à savoir l'UE, les États-Unis, la Chine et la Russie. Ce qui interpelle, c'est l'inscription de ces valeurs dans les postures de cybersécurité de ces entités.

La posture cyber : quand la vision civilisationnelle devient réalité opérationnelle

Alors que la Russie et la Chine ont revendiqué assez tôt une vision civilisationnelle dans la gestion du technologique, les États-Unis ont assigné ce volet au militaire et l'UE a privilégié le dénominateur commun économique. Pour la Russie et la Chine, le numérique (et plus largement, le technologique) ont toujours été un moyen de projeter leur puissance et leur vision du monde. En revanche, c'est avec une certaine surprise qu'on découvre, en mars 2023 l'alignement de partenariats avec « des pays qui partagent nos valeurs » annoncé par le Président américain Joe Biden dans la publication de la nouvelle stratégie cyber américaine[3], et en avril 2023 l'annonce d'un *Cyber Solidarity Act* européen par les commissaires Thierry Breton (au marché intérieur) et Margaritis Schinas (à la promotion du mode de vie européen)[4] sur fond d'une recherche d'autonomie

[2] SHOUP T. & LILJENBERG A.L. (2023), "Destruction democratized", in *Farsight: A world pulled apart?*, CIFS, https://cifs.dk/p/a-world-pulled-apart

[3] THE WHITE HOUSE (2023), "Fact sheet: Biden-Harris administration announces national cybersecurity strategy", https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

[4] Adoption of the Cyber Package proposals: Closing statements by Margaritis Schinas and Thierry Breton (2023), https://multimedia.europarl.europa.eu/en/video/adoption-of-the-cyber-package-proposals-closing-statements-by-margaritis-schinas-vice-president-of-the-european-commission-and-by-thierry-breton-european-commissioner-for-internal-market_I239958

stratégique[5]. Alors, que disent les postures cyber de ces quatre grands acteurs de leurs projections dans le monde et possibles interactions futures ?

Les tendances d'évolution des postures cyber des quatre grands acteurs (Chine, États-Unis, Russie, UE) indiquent naturellement des divergences dans la façon d'appréhender les risques. Ainsi, l'UE fait office d'exception dans sa timidité à mobiliser des opérations cyber offensives (ou, comme elles sont souvent appelées en référence aux postures américaine et chinoise, des « actions de défense proactive »). En effet, pour l'instant, l'UE reste partagée sur l'emploi de capacités cyber offensives. La résolution du Parlement européen sur l'état des capacités de cyberdéfense de l'UE, adoptée en octobre 2021, reconnaît que « dans une certaine mesure, la cyberdéfense est plus efficace si elle contient également des moyens et des mesures offensifs »[6]. Bien que cela n'équivaille pas automatiquement à un changement fondamental dans la position défensive européenne, il y a une évolution dans l'approche de cette question. De même, la recherche d'une approche harmonisée de la mise en œuvre de l'autonomie stratégique est un véritable différenciant européen. Enfin, la « troisième voie » européenne[7] – le réglementaire – s'affirme, avec une intensification des textes normatifs affectant des producteurs technologiques non européens (RGPD, *Cyber Resilience Act*, etc.).

Une autre divergence notable, cette fois lorsqu'on met en parallèle la Chine et la Russie, est l'appréhension du contrôle de l'information. Ces deux acteurs ont placé ce qu'on pourrait appeler une souveraineté informationnelle au cœur de leurs postures cyber. En effet, la maîtrise des contenus est érigée en doctrine aussi bien en Russie[8] qu'en Chine[9] ; dans les deux cas, il s'agit de garantir une vision civilisationnelle unifiée et univoque. Cependant, là où la Russie passe de contrôle informationnel à une « guerre des mentalités », la Chine adopte une démarche diplomatique techniciste et une défense proactive holistique. Dans

[5] Apparu officiellement en 2013 (https://data.consilium.europa.eu/doc/document/ST-217-2013-INIT/fr/pdf), le concept d'autonomie stratégique est devenu central dans la vision du monde de l'UE : il est expressément consacré dans la stratégie globale de l'UE en 2016 (https://data.consilium.europa.eu/doc/document/ST-10715-2016-INIT/fr/pdf ; le document de référence sur les orientations européennes de sécurité et de défense). La pandémie de Covid ayant laissé des traces indélébiles dans nos sociétés, l'autonomie stratégique embrasse depuis fin 2020 (https://www.consilium.europa.eu/media/45918/021020-euco-final-conclusions-fr.pdf) l'ensemble du marché unique, de la politique industrielle, de l'espace et du numérique, notamment en ce que ce dernier est aussi la source de nouveaux risques. En raison de l'interdépendance des économies mondiales, le commerce, la santé ou encore l'énergie sont également concernés. Plus généralement, tous les secteurs dont les chaînes d'approvisionnement dépassent les frontières européennes et sont donc vulnérables aux tensions géopolitiques sont dans le giron de l'autonomie stratégique.

[6] European Parliament resolution of 7 October 2021 on the state of EU cyber defence capabilities (2020/2256(INI)).

[7] FRADIN L. (2020), « L'UE post-Covid : une troisième voie face à la Chine et aux États-Unis », *Le Grand Continent*, https://legrandcontinent.eu/fr/2020/06/18/lue-post-covid-une-troisieme-voie-face-a-la-chine-et-aux-etats-unis/

[8] Dans les versions antérieures des documents stratégiques russes, l'approche de sécurité était énoncée comme faisant obstacle aux « menaces contre les droits et libertés constitutionnels de l'homme et du citoyen dans le domaine de la vie spirituelle et des activités d'information, de la conscience individuelle, collective et publique » se matérialisant par « l'utilisation illégale de moyens spéciaux d'influencer la conscience individuelle, collective et publique » (Doctrine pour la sécurité de l'information de la Fédération de Russie, 9 septembre 2000, https://base.garant.ru/182535/). L'hostilité (perçue et réelle) de l'Occident à l'égard de la Russie s'est également manifestée en matière de souveraineté culturelle, conduisant le même document à identifier « l'application des technologies de l'information dans l'intérêt de la préservation des valeurs culturelles, historiques, cultuelles et morales du peuple multinational de la Fédération de Russie » comme un intérêt national à sauvegarder par le truchement de la sécurité de l'information.

[9] RAUD M. (2018), "China and cyber: Attitudes, strategies, organisation", NATO CCD COE, https://ccdcoe.org/library/publications/china-and-cyber-attitudes-strategies-organisation

ce contexte, la posture cyber de la Chine prend davantage les allures d'une image en miroir des postures occidentales. La Russie continue sa trajectoire de modulation informationnelle en codifiant dans ses doctrines depuis 2016 la « guerre des mentalités » qui vise à modifier « la conscience, la vision du monde, les objectifs, les valeurs et les priorités d'une société »[10] adverse, c'est-à-dire les fondements de sa civilisation.

Outre ces divergences, les tendances d'évolution des postures cyber de ces quatre acteurs font aussi état de beaucoup de similitudes. Tel est notamment le cas dans les approches occidentales de contrôle de l'information : tout en dénonçant les approches chinoise et russe, l'UE et les États-Unis ont également tendance à déployer des moyens pour localiser et exploiter le transit d'informations. Même s'il ne s'agit pas tant de façonner les contenus, l'effort pour héberger des données sur les territoires respectifs et à ne pas permettre de main mise sur des informations jugées stratégiques est prééminent depuis quelques années.

Il est notable de constater que la Chine, la Russie et les États-Unis redoublent d'effort pour équilibrer les opérations cyber défensives et offensives dans un processus continu de préparation-détection-atténuation-réponse-résilience. En témoignent les doctrines respectives, notamment américaine et chinoise, articulées autour de concepts tels que « défense active », voire « défense proactive ». La « défense active » côté russe existe de longue date ; elle se retrouve également dans la « guerre des mentalités » : l'effort de transformer et modeler les fondations civiques et culturelles adverses peut se matérialiser par la prise de contrôle de la narration adverse pour en influencer le comportement. La Chine de son côté enrichit sa boîte à outils conceptuelle en développant la « défense proactive » dans une « fusion civil-militaire »[11]. Ainsi, la distinction entre temps de paix et temps de guerre s'efface pour laisser place à un continuum où le processus continu peut se déployer quel que soit le niveau de conflictualité. Enfin, l'approche proactive américaine est articulée autour des notions de « défense en avant » et « engagement persistant »[12] où on retrouve l'aspect longitudinal de la conflictualité. Par ailleurs, les efforts des États-Unis en faveur d'une plus grande intégration entre les secteurs public et privé reflètent certains aspects de la « fusion civil-militaire » chinoise, qui cherche à structurer une approche holistique renforçant les capacités défensives et offensives.

Ce tour d'horizon des tendances suggère que la Chine, les États-Unis et la Russie assument un comportement de plus en plus préventif et conflictuel dans le cyberespace, tout en se considérant mutuellement comme des adversaires potentiels. L'UE devra prestement formuler une position afin de mieux gérer ses réponses, compte tenu notamment de la diversité des positions des États membres et de sa recherche d'une déclinaison réalisable d'autonomie stratégique.

[10] ИЛЬНИЦКИЙ А.М. (2021), МЕНТАЛЬНАЯ ВОЙНА РОССИИ (La guerre russe des mentalités), ministère de la Défense de la Fédération de Russie, https://vm.ric.mil.ru/Stati/item/336904/

[11] US DEPARTMENT OF DEFENSE (2022), "Military and security developments involving the People's Republic of China", Annual report to Congress, https://media.defense.gov/2022/nov/29/2003122279/-1/-1/1/2022-military-and-security-developments-involving-the-peoples-republic-of-china.pdf

[12] US DEPARTMENT OF DEFENSE (2018), "Fact Sheet: 2018 DoD cyber strategy and cyber posture review", https://media.defense.gov/2018/Sep/18/2002041659/-1/-1/1/factsheet_for_strategy_and_cpr_final.pdf

Le numérique, un pouvoir ambivalent : quelle autonomie stratégique pour l'Europe ?

Par Hugues de JOUVENEL et Jean-François SOUPIZET
Futuribles International

Les auteurs rappellent d'abord en quoi l'essor du numérique constitue une véritable révolution qui se diffuse dans tous les domaines et confère aux géants du net un pouvoir sans précédent vis-à-vis des États et des institutions internationales. Ils montrent ensuite en quoi ces technologies sont porteuses d'opportunités mais aussi de risques qui exigent une vigilance permanente, sinon une capacité d'anticipation, inégalement réparties. Enfin, ils soulignent les limites de l'indépendance stratégique de l'Europe et esquissent trois hypothèses sur l'avenir de son « autonomie stratégique ».

L'ascension fulgurante du numérique et le rôle grandissant qu'il joue dans toutes les activités humaines constituent des tendances lourdes qui auront un impact majeur sur toutes nos existences, la vie des entreprises, leur compétitivité et leur marché ainsi que sur l'autonomie stratégique des États. Les avancées en ce domaine sont principalement le fait de multinationales chinoises et américaines qui, grâce à leur dynamisme et à leurs capacités d'innovation disruptive, sont devenues des acteurs incontournables. Leurs capacités à détecter, accumuler et traiter les données de toute nature sur les individus, les entreprises, leurs pérennité et compétitivité et, plus généralement, l'ensemble de nos sociétés, y compris le fonctionnement des services publics et les actions relevant traditionnellement de la sphère publique (préservation des libertés, maintien de l'ordre, défense nationale) leur confèrent un pouvoir immense et sans équivalent.

Le texte qui suit rappelle d'abord en quoi l'essor du numérique constitue une véritable révolution qui se diffuse dans tous les domaines et confère aux géants du net un pouvoir sans précédent vis-à-vis des États et des institutions internationales. Il montre ensuite en quoi ces technologies sont porteuses d'opportunités mais aussi de risques qui exigent une vigilance permanente, sinon une capacité d'anticipation, inégalement réparties. Enfin, il souligne les limites de l'indépendance stratégique de l'Europe.

L'essor du numérique

Le XX^{e} siècle a été marqué par de nombreuses percées technologiques et innovations industrielles qui ont permis l'essor du numérique dont les usages n'ont cessé de s'étendre et qui a ouvert la voie à la convergence de marchés jusqu'ici disjoints. Le XXI^{e} siècle a vu une véritable explosion de l'industrie des services de l'information. La connectivité globale s'est accrue. L'internet est devenu une infrastructure essentielle à nombre d'activités humaines et les plateformes en ligne ont installé une nouvelle économie des échanges de biens et services. De nouvelles formes de communications sont apparues avec les réseaux et les médias sociaux. Les données de masse ont ouvert la voie à une approche probabiliste

de l'appréhension du monde que son caractère opératoire rend incontournable. Enfin, l'Intelligence artificielle[1] (IA) dans ses développements les plus récents avec les systèmes d'IA générative ouvre des perspectives incommensurables. Au-delà, la notion même de frontière devient floue submergée par l'économie des flux sous-tendus par le numérique. Désormais, l'espace numérique, le cyberespace, s'étend déjà partout depuis le fond des mers jusque dans l'espace orbital au travers d'ondes électromagnétiques de câbles et des satellites, plus encore au travers de logiciels et d'applications, des données et des réseaux.

La diffusion du numérique : une révolution

Une telle évolution a eu de multiples conséquences.

D'abord, l'accélération de la mondialisation de l'économie par le jeu du développement de services en ligne, notamment le commerce électronique, les services financiers, les activités logistiques ou encore le fractionnement des chaînes de valeurs industrielles.

Ensuite, l'entrée dans une ère d'innovations de rupture dont les vagues successives n'en finissent pas de remodeler notre environnement. C'est maintenant un élément central de la dynamique économique : le potentiel de transformation d'un projet est la clé de son financement et de la valorisation boursière de son entreprise. Si cette innovation passe le filtre des marchés, elle pénètre tous les domaines où elle apporte l'immédiateté, l'abolition des distances et le pouvoir des données. Alors les cloisonnements entre les secteurs s'évanouissent et la séparation se brouille entre les domaines privés et publics.

Enfin, l'émergence des GAMAM[2] est l'un des phénomènes marquants des premières décennies du XXIe siècle. C'est une poignée d'entreprises qui, en quelques décennies, ont conquis des positions monopolistiques planétaires et dont les services sont aujourd'hui indispensables à des millions de personnes. À leur tour, les BATXH[3], entreprises inspirées du même modèle ont fait irruption grâce à l'appui des autorités chinoises. Ces figures emblématiques de la Tech sont les grands gagnants de la mondialisation. Ils rivalisent désormais avec les institutions étatiques.

Le pouvoir relatif des États vis-à-vis des géants du net

La rivalité entre États et géants du net est de nature systémique parce que leurs pouvoirs sont fondés sur des visions différentes ; l'une, traditionnelle, se réfère à un modèle hiérarchique ; l'autre fait appel à l'horizontalité des réseaux. À ce titre, elle est irréductible. Et la question qui se pose est celle de la forme des relations – conflit ou alliance – que les uns et les autres entretiendront à l'avenir. Dans le contexte des rivalités entre les États, la contribution de ces géants du net est un atout indispensable. Ils détiennent les clés de la suprématie dans l'économie, l'information et la politique, sans omettre le militaire. À l'inverse, ils sont encore dépendants des États pour l'environnement réglementaire, légal et financier dans lequel ils évoluent en dépit des prétentions extraterritoriales américaines.

[1] PORTNOFF A.-Y. & SOUPIZET J.-F. (2018), « Intelligence artificielle : opportunités et risques », *Futuribles*, n°426, septembre-octobre 2018.

[2] GAMAM pour Google, Amazon, Meta (ex-Facebook), Apple et Microsoft, désormais rejoints par Starlink, Tesla et Twitter d'Elon Musk.

[3] BATXH pour Baidu, Alibaba, Tencent, Xiaomi et Huawei.

Pour prospérer, il leur faut un contexte favorable notamment une sécurité juridique couvrant les produits et services qu'ils offrent.

Aux États-Unis, c'est une alliance de raison qui se dessine entre les tenants des dispositions antitrust et un État qui tire une partie de sa puissance des multinationales. En Chine, c'est la primauté de l'appareil d'État qui s'impose et les géants du net paraissent enrôlés par la stratégie de conquête du *leadership* mondial du gouvernement et par ses projets de contrôle social en interne. L'Union européenne (UE) soutient la recherche et encourage les acteurs européens à se fédérer[4]. Elle parie sur l'attractivité de son marché intérieur pour imposer des règles aux acteurs privés qui y opèrent, par exemple avec le RGPD pour les données personnelles ou les règlements sur les services et marchés numériques[5]. Mais l'application de ces règles ne va pas sans difficultés. Par ailleurs le pouvoir des États-Unis donne dans les faits une portée extraterritoriale aux décisions de justice américaines sans parler des dispositions de sécurité nationale qui sont invoquées. Comme on le voit, les marges de manœuvre européenne sont nécessairement limitées[6].

Dans les autres pays, les géants du net ont largement bénéficié des rivalités inter-étatiques et de l'affaiblissement de la gouvernance multilatérale pour imposer leurs conditions.

La dépendance de l'Europe

La pandémie de Covid, l'invasion de l'Ukraine par la Russie et le retour d'un conflit armé aux marges de l'Europe, les tensions entre la Chine et les États-Unis ont suscité un moment l'impression que la mondialisation marquait le pas, sinon que nous allions vers une « démondialisation », voire un retour en force des États qui, prenant conscience de leur dépendance vis-à-vis de l'extérieur, allaient tenter de retrouver une certaine autonomie. Mais les bouleversements en cours de la scène géopolitique ont cependant révélé la dépendance de l'Allemagne, première puissance industrielle d'Europe, pour ses approvisionnements énergétiques et, plus généralement de l'UE dont la dépendance est élevée pour les matières premières si essentielles à la transition écologique et numérique.

La Commission européenne a, néanmoins, en 2020, publié sa nouvelle stratégie industrielle formalisant le concept d'autonomie stratégique et accordant la priorité aux politiques industrielles en lien avec l'innovation. La guerre en Ukraine a évidemment renforcé les préoccupations relatives à la maîtrise des chaînes de valeur jugées essentielles (produits médicaux, batteries, semi-conducteurs, infrastructures énergétiques et technologies bas-carbone (voir le plan de relance Next Generation EU). N'était-ce pas déjà trop tard ? Toutefois, le sursaut semble se poursuivre : ainsi par exemple s'agissant des matières premières stratégiques (tant au regard de la transition numérique qu'énergétique, ces deux transitions étant d'ailleurs liées), la Commission a émis en mars 2023 un plan de travail[7] ambitieux, mais dont la faisabilité reste toutefois à démontrer.

Les pays européens sont très largement équipés en informatique aussi bien en *hardware* qu'en *software* au sein des entreprises et des organismes publics ainsi qu'au sein des ménages. La collecte, le stockage et le traitement des données les plus diverses, y compris en s'appuyant sur les progrès de l'intelligence artificielle, sont déjà des pratiques

[4] Par exemple le projet GAIA X qui vise à créer un *cloud* européen face à l'oligopole américain.

[5] Règlement Général sur la Protection des Données Personnelles, en vigueur. Règlement sur les services numériques (*Digital Service Act*) et règlement sur les marchés numériques (*Digital Market Act*) dont les entrées en vigueur sont respectivement intervenues le 14/09/2022 et le 02/05/2023.

[6] SOUPIZET J.-F. (2021), « Les géants du Net face aux États », *Futuribles*, n°444, septembre-octobre 2021, et, du même auteur, « Les États face aux géants du Net. Vers une alliance de raison », *Futuribles* n°454, mai-juin 2023.

[7] https://ec.europa.eu/commission/presscorner/detail/fr/ip_23_1661

courantes, en général grâce aux géants du net vis-à-vis desquels l'Europe est devenue dépendante. En témoigne de manière saisissante la cartographie des *data centers* et le rôle de plus en plus stratégique des données : celles qui circulent au travers des réseaux sociaux aussi bien que celles des entreprises et des services publics. La population s'est massivement convertie au numérique : plus de 60 millions de Français (93 % de la population) « surfent » chaque jour sur internet et le nombre d'internautes dans le monde dépasserait 5 milliards[8]. Aucune technologie n'a conquis aussi rapidement autant de personnes. On en connaît les vertus, peut-être moins les risques.

La montée des risques

Les risques sont immenses : presque tous les jours, nous découvrons qu'un hôpital public ou une entreprise, recourant tout naturellement à des systèmes informatiques pour stocker et gérer leurs données, ont été piratés. Comme le souligne Henri d'Agrain, « l'espace numérique est composé de nombreux territoires, plus ou moins adhérents d'ailleurs aux territoires physiques, où se déploient de non moins nombreuses rivalités de pouvoir »[9]. Se référant au roman de science-fiction de William Gibson « Neuromancer » publié en 1984, qui décrit un « futur où la technologie, au développement hypertrophique, finit par envahir l'environnement humain », il explique quels sont les attraits et, surtout les dangers, que comporte cette géopolitique de la donnée, sous l'effet des cyberattaques, de nature criminelle ou étatique, dont l'identification exige des stratégies de sécurité de plus en plus complexes à mettre en œuvre.

Sans même mentionner ici les risques qui pèsent sur nos sociétés d'être soumises à des contrôles incessants, inondées d'informations contradictoires, y compris de *Fake News*, et de messages destinés à les influencer à des fins politique, commerciales et idéologiques, reconnaissons que le numérique est une arme à double tranchant, une technologie ambivalente porteuse du meilleur comme du pire selon les usages qui peuvent en être faits. Or force est de constater que s'il est extrêmement difficile aujourd'hui de s'en passer, l'Europe sur ce plan est très dépendante des multinationales. Au moment du premier choc pétrolier, Valéry Giscard d'Estaing, alors ministre des Finances, avait lancé en France le slogan « on n'a pas de pétrole mais on a des idées ». Nos idées (y compris les découvertes scientifiques, les brevets et autres œuvres, normalement sujettes aux droits d'auteur) sont des données qui, comme tout ce qui est immatériel, s'envolent dans un cyberespace qui est hors de notre contrôle.

Les progrès de l'intelligence artificielle sont tels que, des centaines d'experts et de professionnels, dont Elon Musk, alertent sur les dangers qu'elle fait courir à l'humanité et suggèrent qu'une pause de six mois soit décrétée sur les recherches en la matière. Étrange coïncidence : l'information sort presque en même temps que la déclaration d'Elon Musk lors de la conférence annuelle de Neuralink affirmant avoir obtenu l'accord des autorités sanitaires américaines pour tester ses implants cérébraux connectés sur les humains qui, selon lui, doivent permettre d'arriver à une « symbiose avec l'intelligence artificielle ». Faut-il se réjouir ou s'inquiéter de ces déclarations et écrits, qui semblent pour le moins paradoxales ? Quelle efficacité pourrait donc avoir un moratoire, voire un traité international, sur l'IA alors que l'on sait que ceux-là ne sont, en général, ni respectés ni appliqués de manière équitable à toutes les parties[10] ?

---

[8] Source : BDM, « Digital Report », avril 2023.

[9] AGRAIN H. (d'), « Géopolitique de l'espace numérique. Quelles stratégies de sécurité ? », *Futuribles* n°451, novembre-décembre 2022.

[10] Pensons, par exemple, aux débats suscités dans les années 1940 par le nucléaire considéré par certains comme un « danger pour l'humanité » et faisant plus tard l'objet d'un traité de non-prolifération nucléaire à l'évidence non respecté par tous.

La vocation même de la science et de la technologie est d'aller toujours plus loin mais la puissance sans précédent qu'elles ont acquise et l'ampleur des risques liés à leur usage militent pour que l'on en contrôle le développement. Le problème de la maîtrise sociale des technologies n'est pas nouveau mais il est clair qu'il gagne en acuité. Qui et comment pourrait en assurer un contrôle effectif ?

De la souveraineté et de ses limites

Nous avons vu que le rôle des États, hormis peut-être en Chine, au regard des géants du Net était pour le moins limité et que les instances mondiales, à commencer par les Nations Unies, n'étaient guère prompts à essayer de les réglementer. Elles souffrent du fait que les États membres, au nom de leur souveraineté, entendent très largement en conserver le contrôle même s'ils n'ont pas les moyens de l'assurer. La situation est-elle différente s'agissant des institutions européennes qui bénéficient d'une délégation de pouvoir dans des domaines malgré tout restreints ?

Les compétences de l'UE sont spécifiques ; elles dérivent d'une délégation consentie par les États membres. Dans ce cas l'ambition est celle d'une autonomie stratégique désignant sa « capacité à défendre ses intérêts économiques sur la scène internationale ». Or nous avons vu qu'il n'existe pas d'autonomie sans maîtrise du numérique. Dans ce contexte, quelques hypothèses sur l'avenir du numérique en Europe peuvent être évoquées :

- La première, celle d'une autonomie totale reposant sur les ressources propres de l'UE apparaît comme très naïve. Cette hypothèse n'est guère réaliste ni économiquement ni politiquement.
- La seconde porte sur le renforcement de l'écosystème de la Tech européenne, voire l'émergence d'acteurs majeurs. Cette hypothèse pourrait tirer parti des innovations en cours : les dernières IA bousculent la hiérarchie des moteurs de recherche ; les *datacenters* en orbite celui du *cloud*, etc. Mais les faiblesses européennes restent patentes et notamment la fragmentation de ses marchés.
- Enfin, certains envisagent de miser sur les communs numériques, à l'exemple du logiciel libre. L'UE pourrait abriter des tiers de confiance grâce à ses législations protectrices et accueillir des développements non propriétaires. Mais, est-ce bien à la hauteur des enjeux ?

La souveraineté numérique sans l'État : y a-t-il une souveraineté individuelle pour « l'*homo numericus* » ?

Par Pierre NORO
Enseignant à Sciences Po Paris, au Learning Planet Institute (Université Paris-Cité), chercheur et entrepreneur

La « souveraineté numérique » est un concept habituellement décliné à l'échelle des États et parfois à celle des « géants du numérique » dont ils dépendent pour répondre à leurs besoins. Mais, dans les discours de nombreux pionniers d'Internet et activistes des droits numériques comme dans les pratiques de certaines communautés (logiciel libre, chiffrement, technologies *blockchain*…), les outils numériques permettraient avant tout de revendiquer une souveraineté au niveau individuel.

Cet article a pour but d'esquisser les contours de cette idée, d'en questionner le sens et la légitimité historique. Par-delà une définition limitée d'une souveraineté « de fait », la création d'outils pour positiver des valeurs et des libertés universelles met en lumière une souveraineté numérique individuelle articulée autour des communs numériques et tirant sa légitimité de leur gouvernance, créant une concurrence ou des points de convergence avec celles des États et des entreprises plateformes.

La « souveraineté numérique » est un concept régulièrement invoqué dans les discours des politiques et les feuilles de route stratégiques produites par la puissance publique. Néanmoins, cette notion recouvre souvent des intentions et des réalités différentes et imprécises : la définition de la « souveraineté numérique » est encore, à bien des égards, un chantier en construction (Blandin, 2016 ; Bômont 2018 ; Danet et Desforges, 2020 ; Noro, 2021 ; Glasze *et al.,* 2022). Mais si cette nouvelle forme de souveraineté se décline au niveau des États et qu'elle s'accorde parfois aussi aux entreprises plateformes qui contestent leur pouvoir, est-il possible de la définir à l'échelle individuelle, celle de l'usager numérique, de « l'*homo numericus* » ?

La notion de souveraineté individuelle a une longue histoire derrière elle. Elle est habitée de l'héritage intellectuel de Locke[1] puis notamment de celui des philosophes anarchistes libertaires, reconnaissant aux individus une souveraineté « naturelle » déléguée – et souvent maltraitée – par les gouvernements[2]. Néanmoins, lorsqu'elle s'entrechoque avec celle des États ou des « géants du numérique », la souveraineté numérique individuelle se

[1] "Every man has a Property in his own Person" écrivait-il dans ses *Deux traités de gouvernement* en 1690.

[2] Particulièrement dans le courant anarchiste individualiste, avec l'égoïsme Max Stirner (*L'Unique et sa propriété*, 1844) mais aussi les libertariens et anarcho-capitalistes, notamment américains, de Josiah Warren (*Manifesto*, 1841) jusqu'à Robert Nozick (*Anarchy, state, and utopia*, 1974).

révèle être un amalgame complexe, le résultat de revendications diverses, d'une culture variée et d'enjeux numériques particuliers qui invitent à une cartographie originale de ce concept[3]. Pour ce faire, nous allons explorer les contours de cette souveraineté au travers de prises de positions, de documents et de projets à forte portée symbolique, identifiant une première définition « négative » dont les limites manifestes seront complétées par une appréhension des valeurs défendues par les communautés numériques se réclamant d'une forme de souveraineté et surtout des outils qui les positivent. Au croisement de ces deux notions apparaît une souveraineté individuelle essentiellement collective, fondée sur la défense des libertés numériques et sur la pratique de communs numériques qui méritent d'être valorisés.

La souveraineté individuelle par-delà les États

Avec l'émergence puis la démocratisation de l'informatique personnelle et d'Internet[4], le rapport aux espaces numériques se développe hors des institutions de recherche et militaires à l'origine du réseau ARPAnet et du monde de l'entreprise. De la même façon que l'imprimerie, en facilitant l'accès aux livres et en décloisonnant l'accès à la connaissance, a permis à la fois la naissance d'un nouveau lecteur individuel tout en soutenant l'expansion du mouvement humaniste à l'échelle européenne, les années 1980 et surtout 1990 sont le berceau de nouveaux utilisateurs du numérique qui font l'expérience d'un nouveau « cyberespace ».

Cet espace, plutôt difficile d'accès puisqu'il requiert des compétences et des équipements spécifiques, apparaît comme résolument transnational et hors d'atteinte de la puissance publique. L'information y circule selon de nouvelles règles, de manière relativement ouverte, soumise à des contraintes techniques mais encore libre de normes juridiques, faute non seulement de législation *ad hoc* mais aussi de juridiction claire.

L'espace numérique est à la fois issu et structuré par des idéologies post-hippies, libertaires et libertariennes, où l'individu, hors des juridictions des États peut s'émanciper et exister dans de nouvelles communautés articulées autour de logiques de marché (anarcho-capitalisme), de coopération libre (développement des projets et communautés *open source* et de la philosophie Unix) (Stallman, 2015) et d'initiative individuelle, créative et parfois subversive (la culture *hacker*) (Turner, 2006 ; Cardon, 2019 ; Chen, 2022). Pour compléter le tableau, il faut aussi ajouter l'idéal « connectionniste » des pionniers et des industriels du numérique qui espèrent, avec des motifs variés mais convergents, étendre ce nouvel espace en connectant toujours plus de nouveaux foyers. Ce territoire a donc vocation à s'agrandir, ignorant les frontières nationales, mettant toujours plus d'individus en réseau, les connectant sans recourir à l'État comme intermédiaire.

La première forme de souveraineté numérique individuelle serait donc essentiellement « négative » : le cyberespace apparaît d'abord « a-national », hors des juridictions traditionnelles, au-delà de la souveraineté des États. L'*homo numericus* y serait donc souverain « par défaut », un principe pleinement aligné avec de nombreuses idéologies prévalentes dans les communautés responsables de nombreuses innovations techniques de l'époque, de la Silicon Valley californienne au CERN européen.

John Perry Barlow, artiste militant et cofondateur de l'Electronic Frontier Fondation (EFF), dans sa fameuse *Déclaration d'indépendance du cyberespace* de 1996, présente

[3] Bien que certains auteurs n'hésitent pas à se revendiquer de l'héritage anarcho-libéral, comme par exemple Davidson et Rees-Mogg dans leur *The sovereign individual* (1997).

[4] Avec notamment le déploiement des protocoles TCP/IP en 1982, puis DNS en 1985 et HTTP en 1991.

une revendication claire de cette nouvelle souveraineté numérique individuelle. S'adressant aux « Gouvernements du monde industriel, géants fatigués de chair et d'acier », il proclame : « Vous n'avez aucun droit de souveraineté sur nos lieux de rencontre. […] je m'adresse à vous avec la seule autorité que donne la liberté elle-même lorsqu'elle s'exprime. Je déclare que l'espace social global que nous construisons est indépendant, par nature, de la tyrannie que vous cherchez à nous imposer[5]. ». Si ni le territoire, ni les usagers du cyberespace ne relève des États, il faut bien que l'*homo numericus* y soit souverain.

Cette souveraineté « naïve » n'est toutefois pas appréhendée de manière homogène et présente déjà des paradoxes. L'émergence d'une société inclusive, horizontale et libérée de l'arbitraire des États se heurte déjà aux barrières techniques et à une vision méritocratique et élitiste très affirmée dans certaines communautés. Elle résulte aussi souvent d'une vision déracinée de la réalité matérielle de l'écosystème numérique, dépendant des infrastructures et des technologies (*hardware* et *software*) financées, entretenues et/ou administrées par la puissance publique (Mazzucato, 2013), et bientôt rattrapée par l'extension des juridictions et des intérêts stratégiques.

De l'esquive à l'affrontement : la souveraineté individuelle contre celle des États (et des Gafam)

La souveraineté individuelle face aux États et le capitalisme de surveillance

La déclaration d'indépendance de Barlow relève néanmoins à la fois de l'esquive que de la mise en place d'un conflit de souveraineté. Elle est une réponse à l'adoption du Telecommunications Act de 1996, perçue comme une « invasion » du cyberespace par des autorités publiques incompétentes et illégitimes. L'extension de la juridiction américaine sur le « cyberespace » et le rapport de force qui en résulte vient donc progressivement « positiver » la définition de la souveraineté numérique individuelle.

Cette souveraineté individuelle ne peut donc pas résulter que du constat d'un « ailleurs » hors de portée de l'État. Elle se définit aussi contre l'État parce qu'elle s'enracine dans des valeurs menacées par celui-ci. La « civilisation de l'Esprit » dont Barlow revendique l'indépendance fonde sa légitimité sur sa culture et ses valeurs résolument anarchistes, universalistes, égalitaires, libertaires, rejetant la propriété intellectuelle au profit d'une protection absolue de la liberté d'expression individuelle et de la libre circulation de l'information. Ces valeurs étant irréconciliables avec le droit et donc l'État américain[6], il faut bien que le cyberespace fasse sécession et affirme une souveraineté propre.

La question de la propriété intellectuelle n'est pas le seul point d'achoppement dans ce rapport de force. Mues par une intuition visionnaire des risques que la numérisation, lorsqu'elle est aux mains d'États, surtout illibéraux, ou d'entreprises dominantes et quasi-monopolistiques, puisse normaliser un contrôle sans précédent sur la société, certaines communautés se rallient autour du droit à la vie privée, à la confidentialité des communications, notamment par l'utilisation d'outils de chiffrement. C'est le cas des cypherpunks, dont Eric Hughes écrivit en 1993 le manifeste, affirmant la nécessaire protection de la vie privée comme garante d'une « société ouverte ». Le manifeste des

[5] Traduction issue de *Libres enfants du savoir numérique : Une anthologie du Libre* (2000) de Florent Latrive et Olivier Blondeau.

[6] L'EFF est d'ailleurs née à la suite des premières vagues d'investigations contre le piratage aux États-Unis.

cypherpunks n'est pas qu'un acte de militantisme : en proclamant « les cypherpunks écrivent du code » Hughes affirme que la souveraineté individuelle à l'ère numérique passe par la contribution au développement d'outils partagés qui protègent la souveraineté des individus et le droit universel à une vie privée face aux « gouvernements, entreprises, ou autres grandes organisations sans visage ». La participation à l'élaboration et l'utilisation d'infrastructures logicielles *open source* est donc une autre manière de « positiver » la souveraineté numérique, Hughes reliant déjà le droit individuel à un effort collectif.

L'intuition des cypherpunks se confirme surtout après le tournant que constitue les attentats du 11 septembre 2001, à la suite duquel un mouvement politique transpartisan, mené par les États-Unis entraînant avec eux de nombreux États européens, invoquant la sécurité des citoyens pour surveiller les communications d'une large partie de la population mondiale. Après les premières victoires des activistes numériques durant la décennie 1990[7], ce retour en force de la « Raison d'État » qui prime sur les libertés individuelles a abouti à l'adoption de réglementations remettant en cause le droit au chiffrement, à la vie privée, à la neutralité du Net et à l'accès à l'information, ainsi qu'au déploiement de dispositifs de surveillance numérique de masse, du Patriot Act[8] de 2001 jusqu'au CLOUD Act[9] de 2018, et même à la mise en place de programmes outrepassant ces cadres juridiques, comme ceux révélés par Edward Snowden en 2013 puis de nombreux lanceurs d'alerte par la suite.

Ce basculement est pleinement aligné avec l'émergence d'entreprises plateformes fondant leur activité sur la capture d'un maximum de données des utilisateurs et la publicité ciblée, tout particulièrement les « Gafam ». La souveraineté individuelle numérique est donc amenée à se concrétiser face à une double-menace, celle du retour des États qui étendent leur juridiction au cyberespace, dont la conception de la sécurité collective bat en brèche les libertés revendiquées par les activistes numériques, conjuguée à celle des entreprises qui construisent brique par brique le « capitalisme de surveillance » (Zuboff, 2019).

La souveraineté par le code

L'accélération du conflit entre la souveraineté des États, la souveraineté individuelle et celles des entreprises plateformes présente presqu'une dimension dialectique en ce qu'elle force les communautés numériques à se structurer. Pour « positiver » leurs souverainetés naissantes, « l'*homo numericus* » et les entreprises usent d'un outil qui leur est propre, le code informatique, dont Lawrence Lessig avait déjà identifié le pouvoir normatif puisqu'il définit des « architectures de contrôle social » qui régissent les interactions entre utilisateurs et orchestrent une concurrence avec le droit traditionnel (Lessig, 1999, 2006). En fervent défenseur des modèles coopératifs et de l'*open source*, Lessig affirme aussi la nécessité pour les communautés numériques transnationales d'appréhender le caractère politique de leurs architectures, les valeurs défendues par le code qui leur donne corps et

[7] Par exemple, l'*executive order* 13026 signé le 11 novembre 1996 qui amène au déclassement des logiciels de chiffrement à l'export, considérés jusqu'alors comme matériel militaire, ou la décision *Junger v. Daley* (6th Cir. 2000) qui aboutit à l'extension de la protection fournie par le 1er amendement aux codes sources informatiques.

[8] Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA PATRIOT Act), Acte de 2001 (H.R. 3162, Pub. L. 107-56), repéré à https://www.govinfo.gov/content/pkg/PLAW-107publ56/html/PLAW-107publ56.htm

[9] Clarifying lawful overseas use of data (CLOUD Act), Acte adopté en tant que section V du Consolidated Appropriations Act de 2018 (H.R. 1625, Pub. L. 115-141), repéré à https://www.govinfo.gov/content/pkg/BILLS-115hr1625enr/html/BILLS-115hr1625enr.htm

d'adopter des modèles de gouvernance plus démocratiques afin de légitimer leur souveraineté dans la dialectique qui les oppose aux États[10].

Parmi ces architectures de code, les technologies *blockchain* apparaissent comme des « outils de souveraineté » qui incarnent à la fois l'héritage des cypherpunks et de Lessig. L'ambition du système *Bitcoin*, décrit en 2008 par Satoshi Nakamoto[11], et des autres protocoles qui l'ont suivi, est de déployer des réseaux en pair-à-pair ayant pour but de permettre des transactions entre les membres pseudonymes d'une communauté ouverte. Le code, bien entendu *open source*, prévoit un « protocole de *consensus* » qui permet, sous certaines conditions, aux membres du réseau de s'accorder sur un ensemble d'informations (le registre constitué en chaîne de blocs) sans dépendre d'un tiers de confiance ni craindre la censure, mais aussi des règles de gouvernance décentralisée inspirées par les communautés du logiciel libre pour permettre l'évolution du code source.

Les technologies *blockchain* présentent donc à la fois les particularités des « communs numériques » (gouvernance décentralisée, *open source*, réseau pair-à-pair maintenu par les participants et accessible à tous…) et un ADN profondément anarcho-capitaliste (logique de marché libre, garantie absolue de la propriété privée contre la coercition, collaboration fondée sur l'alignement des incitations économiques et la maximisation des espérances de gains, qui va jusqu'à la marchandisation de la participation à la gouvernance…). Elles remettent radicalement en cause les pouvoirs régaliens, en premier lieu celui du contrôle de la monnaie[12], contournent le système financier traditionnel et ses réglementations, tout en contrecarrant les systèmes de surveillance, puisqu'elles implémentent des technologies de chiffrement par défaut qui redéfinissent la notion d'identité en ligne (Clippinger et Bollier, 2014)[13].

Les technologies *blockchains* sont d'ailleurs plus que des alternatives aux institutions étatiques et aux plateformes centralisatrices des GAFAM. Elles donnent aux utilisateurs des outils pour créer de nouvelles communautés dotées d'un ensemble de règles de gouvernance inscrites dans le code d'un *smart contract*[14] revêtant un caractère normatif, permettant de prendre des décisions collectives et d'administrer un trésor constitué de cryptoactifs, sans entité juridique ni juridiction prédéfinie (Hassan, 2021). Grâce à cette structure technique, les communautés numériques peuvent alors se constituer en « organisations décentralisées et autonomes » (DAO) poursuivant un objectif commun (Buterin, 2014). Puisqu'elles reposent sur une infrastructure ouverte, en pair-à-pair et un modèle de gouvernance décentralisé positivé par un code *open source* capable de s'exécuter de manière autonome, de nombreuses DAO se revendiquent d'une souveraineté de fait (de Filippi, 2018, 2021) et forment un écosystème émergent, bouillonnant d'expérimentations en matière de gouvernance et couvrant des réalités très diverses, de petites communautés

[10] À même de refléter ce qu'il appelle les "citizen-sovereign values" plutôt que les intérêts commerciaux des entreprises qui composent et régulent déjà l'écosystème numérique ("merchant-sovereign").

[11] Satoshi Nakamoto est lui-même un-e auteur-e pseudonyme dont l'identité n'a jamais été révélée.

[12] Pourtant identifié dès le XVI[e] siècle par Jean Bodin comme l'un des fondements de la souveraineté de l'État.

[13] Les transactions sur les principaux réseaux *blockchain*, *Bitcoin* compris, sont pseudonymes et non anonymes. Elles peuvent aujourd'hui être tracées au moyen de technologies d'analyse avancées, mais de nouveaux outils sont régulièrement développés pour renforcer la confidentialité des transactions et contourner ces techniques d'analyse (« mixeurs », nouveaux protocoles comme Monero, Zcash, DarkFi…).

[14] Les *smart contracts* sont des petits programmes informatiques déployés sur un réseau *blockchain*, capables de s'exécuter de manière décentralisée et automatisée.

constituées autour d'enjeux clairs et locaux, jusqu'à des tentatives de constitution de nouvelles entités souveraines alternatives[15].

Si elles constituent des exemples symptomatiques d'une souveraineté numérique ancrée dans une culture alternative et des valeurs structurées autour des droits de l'*homo numericus*, les technologies *blockchain* actuelles présentent de nombreuses limites[16] et sont loin d'être les seuls outils opérés par des communautés numériques, souvent de manière participative et ouverte, afin de garantir leur souveraineté[17]. Cette diversité et le constat évident qu'aucune de ces technologies n'est le fruit du travail d'un seul individu ni qu'elle pourrait opérer sans reposer sur un collectif organisé doit nous amener à questionner la nature « individuelle » de l'élan de souveraineté qui anime tous ces mouvements et projets.

La souveraineté numérique, une affaire de commun

Bien que la préservation de la vie privée prônée par les cypherpunks et par de nombreuses organisations de défense des libertés numériques[18] repose sur l'utilisation par chacun d'outils de chiffrement appropriés, le développement de ces outils est évidemment le résultat d'un long travail collectif[19], tout comme le droit de les utiliser en dépit de velléités politiques appelant à toujours plus de surveillance[20]. Cette protection est d'ailleurs souvent perçue comme une pratique nécessairement collective, un bien commun où l'augmentation du nombre d'utilisateurs contribue à augmenter marginalement la sécurité de tous[21].

De plus, il serait caricatural de limiter la défense des libertés numériques individuelles, notamment en matière de droit à la vie privée, aux seules communautés *open source* se revendiquant d'une souveraineté alternative. Lorsque leurs souverainetés s'entrechoquent, les États comme les entreprises s'appuient presque systématiquement sur la défense des droits individuels de leurs citoyens ou utilisateurs pour contrecarrer la souveraineté d'États rivaux et d'entreprises extraterritoriales (Noro, 2021)[22]. C'est en revendiquant la protection de la vie privée de ses citoyens que les États de l'Union européenne

[15] Là encore, de l'adoption de ces technologies par des micro-nations ou la constitution de villes administrées par des DAOs (decentralized autonomous organization) jusqu'à la promesse de faire naître de nouveaux États transnationaux (Noro, 2022).

[16] Voir notamment Fechtinger *et al.* (2023) et Rozas *et al.* (2021).

[17] Ces outils ne se limitent d'ailleurs pas au logiciel mais comprennent également des infrastructures *hardware* (réseaux Wi-Fi et fournisseurs d'accès internet communautaires, stockage de fichiers décentralisés, mouvement *open hardware*…).

[18] Quelques organisations particulièrement influentes en la matière : EFF, Privacy International, Center for Democracy & Technology, Quadrature du Net…

[19] Il est parfois même financé plus ou moins directement par les États, au travers de la recherche, du développement militaire…

[20] À la suite des attentats ayant frappé la France en janvier 2015, le Premier ministre britannique David Cameron appelait même dans un discours du 12 janvier à l'interdiction de tout service de messagerie chiffrée auquel le gouvernement ne pourrait pas avoir accès, repéré à https://www.bbc.com/news/technology-30794953

[21] Hughes intègre d'ailleurs la protection de la vie privée à une forme de « contrat social » auquel tous les utilisateurs d'outils de communication numérique devraient contribuer.

[22] Comme par exemple avec l'adoption de la loi « Informatique et Libertés » du 6 janvier 1978, qui créée la CNIL en France.

adoptèrent le RGPD, renversant, au moins partiellement[23], le rapport de concurrence avec les États-Unis et leurs entreprises[24]. Apple s'est opposé à l'État américain avec une rhétorique similaire en refusant de fournir au FBI les moyens de briser le chiffrement de l'un des téléphones des assaillants de San Bernardino. Si ces initiatives relèvent d'un mouvement vertical étranger à l'horizontalité qui caractérise les communautés numériques évoquées plus haut[25], leur efficacité est indéniable, d'autant que leur impact ne dépend pas exclusivement de l'adoption par chacun d'outils et de pratiques inégalement accessibles[26].

Que reste-t-il donc de l'idée même de souveraineté individuelle numérique ? D'une part, la définition « négative » d'une souveraineté par défaut s'avère insuffisante, voire naïve puisque déracinée des réalités matérielles, socio-économiques, politiques et juridiques du numérique. D'autre part, la définition « positive », celle qui émerge des faits, de la revendication de droits numériques centrés autour du droit à la vie privée, à la confidentialité des données et la libre circulation de l'information incarnée par le développement et l'adoption de technologies qui protègent ces libertés, est incompatible avec la fiction d'un « solipsisme » numérique, d'un *homo numericus* affirmant par et pour lui seul sa souveraineté, et n'exclut même pas l'exercice de la souveraineté des États et des entreprises lorsque celui-ci converge avec ces objectifs.

C'est à l'intersection de ces deux définitions que se dessinent les contours d'une souveraineté numérique singulière et mobilisable, celle de communautés numériques, transnationales, où les *homo numericus* s'associent librement selon un principe d'autodétermination et se saisissent de droits et libertés numériques qui émergent de l'unicité des dynamiques de l'information et de l'économie du savoir dans le « cyberespace ». Les « communs numériques » tirent alors leur légitimité à la fois des valeurs qu'ils défendent et de leur gouvernance collaborative, horizontale et ouverte (Peugeot, 2012 ; Fuster-Morell, 2014).

Comme les communautés qui les font vivre, les communs numériques forment un ensemble à la fois global et « kaléidoscopique », dont les effets sont cumulatifs et souvent interdépendants. Ils donnent corps à une souveraineté numérique « individuelle », non pas en ce qu'elle se résume à un projet anarchiste individualiste, ni ne recouvre que des pratiques atomisées, celles d'un *homo numericus* fantasmé, « seul souverain contre tous », mais qu'elle vise à protéger l'indépendance, à « encapaciter » les utilisateurs individuels dans un écosystème numérique où se déploient des asymétries de pouvoir et d'information qui provoquent des formes de domination nouvelles.

[23] La mise en conformité par rapport à de nouvelles normes s'avère souvent plus difficile pour les petits acteurs que pour les plateformes qui, pourtant ciblées, jouissent de davantage de ressources techniques et juridiques.

[24] La proclamation de la *Déclaration européenne sur les droits et principes numériques pour la décennie numérique* (2023/C 23/01) par l'Union européenne participe d'un même mouvement.

[25] Ces communautés peuvent néanmoins être indirectement associées à ce genre d'avancées, notamment au travers du travail de militantisme, d'éducation et d'influence des organisations de défense des droits numériques.

[26] Surtout lorsque l'on considère l'éventualité que des normes plus protectives s'étendent au-delà de leur juridiction, comme ce fut le cas avec le RGPD et le "Brussels effect" qui s'en est suivit (Bradford, 2012).

Conclusion

La « souveraineté numérique individuelle », revendiquée par des communautés voulant protéger les libertés numériques individuelles de chaque *homo numericus*, incarnée par des communs numériques accessibles à tous et gouvernés de manière ouverte, présente donc aujourd'hui un caractère « factuel » évident[27]. Elle revêt aussi, comme c'est souvent le cas en matière de souveraineté, une dimension « fictive », celle d'un « mythe idéologique », puisqu'elle s'affirme par la concurrence avec des souverainetés des États et des entreprises du numérique dans lesquelles elle est encastrée (Wallerstein, 1999 ; Krasner, 2001 ; Agnew, 2005). Mais dans ce jeu de souverainetés, les superpositions et convergences sont possibles. Pour les États (ou même les entreprises) soucieux de préserver les libertés numériques individuelles, la reconnaissance de ces biens communs, le soutien à leur développement et la valorisation de leurs modèles de gouvernance, pour eux-mêmes et en tant que source d'inspiration potentielle, doivent devenir une priorité en matière de politiques publiques du numérique, que ce soit pour contrecarrer la domination de certains États ou d'entreprises qui mettent en péril les libertés individuelles, pour protéger le droit à la vie privée de chacun, pour renouer avec une partie de l'utopie libertaire du *web* ou pour concrétiser sa promesse d'une société de l'information plus égalitaire, démocratique et désirable.

Bibliographie

AGNEW J. (2005), "Sovereignty regimes: Territoriality and State authority in contemporary world politics", *Annals of the Association of American Geographers*, n°95, pp. 437-461.

BÔMONT C. (2018), « Maîtriser le cloud computing pour assurer sa souveraineté » *in* Stéphane Taillat éd., *La Cyberdéfense : Politique de l'espace numérique,* pp. 91-97, Paris, Armand Colin.

BLANDIN A. (dir.) (2016), *Droits et souveraineté numérique en Europe*, Bruylant, Coll. « Rencontres européennes ».

BUTERIN V. (2014), "DAOs, DACs, DAs and more: An incomplete terminology guide", Ethereum Foundation Blog.

CARDON D. (2019), *Culture numérique,* Presses de Sciences Po, Coll. « Les petites humanités ».

CHEN C. (2022), *Work pray code: When work becomes religion in Silicon Valley*, Princeton University Press.

CLIPPINGER J. & BOLLIER D. (dir.) (2014), *From Bitcoin to Burning Man and Beyond*, Amherst, ID3 & Off the Common Books.

DANET D. & A. DESFORGES (2020), « Souveraineté numérique et autonomie stratégique en Europe : Du concept à la réalité géopolitique », *Hérodote*, pp. 177-178.

DE FILIPPI P & WRIGHT, A. (2018), *Blockchain and the law. The rule of code*, Harvard University Press, 312 pages.

HASSAN S. & DE FILIPPI, P. (2021), "Decentralized Autonomous Organization", *Internet Policy Review*, ISSN 2197-6775, *Alexander von Humboldt Institute for Internet and Society*, Berlin, vol. 10, issue 2, pp. 1-10, https://doi.org/10.14763/2021.2.1556

[27] Au sens du « positivisme juridique » de Jellinek et de Malberg : la souveraineté existe *de facto*, l'État se constituant de lui-même avant de se doter de règles juridiques.

FEICHTINGER, R., FRITSCH, R., VONLANTHEN, Y., & WATTENHOFER, R. (2023), "The hidden shortcomings of (D) AOs--An empirical study of on-chain governance", pré-publication *arXiv,* arXiv:2302.12125.

FUSTER MORELL M. (2014), "Governance of online creation communities for the building of digital commons: Viewed through the framework of the institutional analysis and development" *in* Frischmann B. *et al.* (dir.) *Governing Knowledge Commons,* Oxford University Press.

GLASZE G., CATTARUZZA A. *et al.* (2022), "Contested spatialities of digital sovereignty" *Geopolitics*, pp. 1-40.

KRASNER S. D. (2001), "Abiding Sovereignty", *International Political Science Review*, vol. 22, issue 3, pp. 229-251.

LESSIG L. (1999), *Code and other laws of cyberspace*, New York, Basic Books.

LESSIG L. (2006), *Code: version 2.0*, New York, Basic Books.

MAZZUCATO M. (2013), *The entrepreneurial State: Debunking Public vs. Private Sector Myths*, Londres, Anthem Press.

NORO P. (2021), « Les enseignements des projets de cloud souverain pour la stratégie numérique de l'État français », Chaire Digital, Gouvernance et Souveraineté de Sciences Po.

NORO P. (2022), « Gouvernement et Démocratie » *in Blockchain et développement durable*, rapport de l'association Blockchain for Good.

PEUGEOT V. (2012), « Biens communs et numérique : l'alliance transformatrice » *in* CALDERAN *et al.* (dir.), *Le document numérique à l'heure du web*, ADBS, pp. 141-154.

ROZAS D., TENORIO-FORNES A., DIAZ-MOLINA S., & HASSAN S. (2021), "When Ostrom meets blockchain: Exploring the potentials of blockchain for commons governance", *Sage Open*, vol. 11, issue 1, pp. 1-14.

STALLMAN R. (2015), *Free Software, Free Society: Selected Essays of Richard M. Stallman*, Boston, GNU Press.

TURNER F. (2006), *From counterculture to Cyberculture*, Chicago, University of Chicago Press.

WALLERSTEIN (1999), "States? Sovereignty? The dilemmas of capitalists in an age of transition" *in* SMITH D., SOLINGER D. & TOPIK S. (dir.), *States and sovereignty in the global economy*, Londres, Routledge.

ZUBOFF S. (2019), *The age of surveillance capitalism: the fight for a human future at the new frontier of power*, Londres, Profile Books.

Le droit au service de la souveraineté numérique de l'UE

Par Brunessen BERTRAND
Professeure à l'Université de Rennes, Responsable de l'Axe intégration européenne, Chaire Jean Monnet sur la gouvernance des données

Il existe une tension interne au sein l'Union européenne sur l'idée de souveraineté numérique, certains États étant plus réticents à s'engager sur une vraie vision politique qu'implique un projet de souveraineté numérique. La régulation européenne du numérique, par son ambivalence, illustre l'équilibre délicat entre l'affirmation politique de l'Union européenne par le droit et la volonté de ne pas trop inhiber, par une régulation trop contraignante, les innovations technologiques dont elle a besoin dans un contexte géopolitique international où elle peine parfois à trouver sa place et assumer sa singularité.

« Notre ambition déclarée est plus pertinente que jamais : il s'agit de mener des politiques numériques qui donnent aux individus et aux entreprises les moyens de s'approprier un avenir numérique qui soit centré sur l'humain, durable et plus prospère »[1]. Cette prémisse conceptuelle que l'on trouve en tête de la « Boussole numérique » présentée par la Commission en mars 2021 illustre toute l'ambiguïté – ou l'ambivalence, c'est selon – de la politique européenne, qui n'a jamais su choisir, ou peut-être assumer, une priorité entre l'économique et le politique, au risque, peut-être, de ne porter correctement ni l'une ni l'autre, surtout dans l'objectif de souveraineté numérique qui a fait son apparition depuis quelques temps dans le discours politique européen.

Cette Boussole numérique reprend les fondamentaux de la politique européenne du numérique telle qu'elle se déploie depuis 2020, en ceci qu'elle s'arrime sur un projet d'autonomie stratégique, parfois qualifié de souveraineté numérique dans le discours politique européen. Dans cette « vision » européenne du numérique, on retrouve, classiquement, un aspect défensif, qui assume l'objectif de « souveraineté numérique », mais on croit aussi déceler une esquisse d'un objectif plus offensif peut être, de l'ordre du géopolitique sans doute, l'Union européenne assumant même une volonté d'atteindre un « leadership numérique » dans le monde. Si l'on retrouve cette diplomatie du numérique dans une pluralité d'aspects de la politique européenne du numérique, la conception européenne se déploie souvent à travers la technicité, ce qui est une façon de dépolitiser un débat sur la souveraineté numérique qui ne fait pas l'unanimité au sein des États membres de l'Union européenne, de sorte que la question de la connectivité semble être le cœur de cet enjeu[2].

Si l'ambition politique reste modeste, au fond il s'agit surtout de combler un retard européen en anticipant de façon plus stratégique les évolutions à venir, il faut aussi reconnaître, au titre du bilan, que la stratégie « Façonner l'avenir numérique de l'Europe » a porté quelques fruits. La perspective, on l'a dit, était assez défensive : il s'agissait surtout

[1] Communication de la Commission, 9 mars 2021, « Une boussole numérique pour 2030 : l'Europe balise la décennie numérique », COM/2021/118 final.

[2] Dans les Conclusions du Conseil du 12 juillet 2021, Une Europe connectée à l'échelle mondiale, le Conseil a par exemple souligné que l'UE devait inscrire la connectivité dans une approche géostratégique et mondiale.

de défendre la position européenne en ouvrant des écosystèmes numériques dominés par les grandes plateformes (acte sur la gouvernance des données, législation sur les services numériques, législation sur les marchés numériques, cybersécurité), en donnant une crédibilité à l'industrie européenne par un financement public (en particulier, les 20 % de la facilité pour la reprise et la résilience consacrés à la transition numérique).

Cette stratégie européenne défensive face à l'extérieur est maintenue mais elle se double d'un enjeu interne plus marqué de convergence entre les États membres en matière de transformation numérique, faisant apparaître l'hétérogénéité des situations nationales. Surtout, elle ne s'accompagne plus d'un discours sur l'autonomie européenne qui semble avoir changé de centre de gravité : à travers l'idée que « l'Europe parviendra à la souveraineté numérique dans un monde interconnecté », on trouve une forme de réalisme politique qui ne cherche plus à faire de l'Europe un acteur à part dans le cyberespace, mais plutôt un acteur à part entière.

La « vision européenne » de la politique du numérique se déploie désormais en quatre points qui portent sur les « capacités numériques » de la société européenne (infrastructures et compétences) et la culture numérique de la société européenne (numérisation accrue des entreprises et des services publics).

Le droit au service de la souveraineté numérique s'inscrit dans une forme d'ambivalence. En un sens, les institutions européennes légifèrent en mettant en œuvre une stratégie de dépolitisation afin d'éviter les dissensions internes que suscite la notion de souveraineté numérique au sein de l'Union. Dans l'autre sens, ces législations européennes en matière de numérique tentent de défendre une certaine vision européenne de la régulation du numérique, assumant là une façon d'être au monde propre à l'Union européenne.

La régulation européenne du numérique : l'ambivalence d'une vision politique européenne de la souveraineté numérique

La régulation européenne du numérique entretient un rapport ambigu avec la souveraineté numérique européenne. D'un côté les institutions assument le projet politique sous-jacent à ces régulations. D'un autre côté, les régulations européennes du numérique n'assument pas pleinement cet objectif politique.

De la société numérique à la citoyenneté numérique européenne

L'« approche européenne de la société numérique » devrait ainsi « étayer et soutenir les initiatives ouvertes en faveur de la démocratie en contribuant à l'élaboration de politiques inclusives ». En un mot, dans l'Union européenne, « l'environnement numérique » est « centré sur l'humain », mais aussi « sûr et ouvert », « conforme à la loi » et doit « permettre aux individus de faire valoir leurs droits, tels que le droit à la vie privée et à la protection des données, la liberté d'expression, les droits de l'enfant et les droits des consommateurs »[3].

La politique européenne du numérique se veut ainsi politique, car elle défendrait une certaine vision de l'individu : ainsi apprend-t-on que « les technologies et services numériques utilisés doivent être conformes au cadre juridique applicable et respecter les droits et les valeurs inhérents au mode de vie européen ». On pourrait y voir un certain nombre de contradictions tant il est vrai que la prévalence recherchée de l'économique ne s'accom-

[3] Communication de la Commission, 9 mars 2021, « Une boussole numérique pour 2030 : l'Europe balise la décennie numérique », COM/2021/118 final.

mode pas toujours d'une approche politique volontaire centrée sur les droits et les valeurs. On peut aussi y voir une permanence, une force peut être aussi au fond, du discours européen qui n'assume jamais d'élever l'économie au-dessus de l'individu et d'un projet de société. De cette dialectique européenne compliquée entre intégration économique et intégration politique, on ne sortira sans doute jamais. Appelons là ambivalence alors, plutôt qu'ambiguïté. Il n'en demeure pas moins que la lecture de cette *Digital Compass* ne nous éclaire guère sur le projet d'intégration politique et social de l'individu dans cette nouvelle société que l'on nous annonce, si ce n'est qu'il doit maîtriser les rudiments d'internet.

Cette « approche européenne de la société numérique » repose sur le plein respect des droits fondamentaux de l'UE. Cette approche européenne s'apparente parfois à une application des droits fondamentaux au cyberespace, parfois à une promotion des grandes lois européennes porte-drapeau de la politique du numérique. On trouve ainsi : la liberté d'expression, y compris l'accès à des informations diversifiées, fiables et transparentes ; la liberté de mettre en place et de gérer une activité économique en ligne ; la protection de la vie privée et des données à caractère personnel, ainsi que le droit à l'oubli ; la protection de la création intellectuelle des individus dans l'espace en ligne.

À cela s'ajoute un « ensemble complet de principes numériques » tels que l'accès universel aux services internet, un environnement en ligne sécurisé et fiable, une éducation et des compétences numériques universelles permettant aux citoyens de participer activement à la société et aux processus démocratiques, un accès à des systèmes et dispositifs numériques respectueux de l'environnement, une administration et des services publics numériques accessibles et centrés sur l'humain, des principes éthiques applicables aux algorithmes centrés sur l'humain, la protection et l'autonomisation des enfants dans l'espace en ligne et l'accès aux services de santé numériques.

Penser l'individu dans la société numérique

Penser, au-delà des droits fondamentaux, la place du citoyen dans un projet d'intégration politique et social serait une vraie rupture avec les méthodes et raisonnements du droit de l'Union européenne. C'est l'une des perspectives que l'on aurait aimé percevoir plus nettement derrière la « boussole numérique » et du projet de « décennie numérique de l'Europe » présenté en mars 2021. Au lieu d'un projet politique d'intégration, la Commission propose un « cadre » de principes numériques supposé définir une véritable « citoyenneté numérique européenne ».

Cette citoyenneté numérique passerait, reprenant une distinction opérée par la Charte, par la définition de droits et principes numériques pour les citoyens européens après la mise en place d'un débat public et d'une réflexion ouverte dans l'espace public. Ce cadre de principes numériques doit contribuer à promouvoir et à défendre les valeurs de l'Union dans l'espace numérique. Dans le prolongement de cette esquisse, la Commission a proposé en janvier 2022 une déclaration sur les droits et principes numériques dans l'Union qui « vise à expliquer les intentions politiques communes ». Son objectif est de rappeler les droits les plus importants dans le contexte de la transformation numérique, mais aussi « servir de référence aux entreprises et aux autres acteurs concernés qui élaborent et déploient de nouvelles technologies ». À lire cette déclaration, la conception européenne de la transition numérique serait ainsi centrée sur les citoyens, la solidarité et l'inclusion, et revendique l'importance de la liberté de choix, de la participation à l'espace public numérique, de la sûreté, de la sécurité et de l'autonomisation, et de la durabilité.

Politiquement, la déclaration affirme la nécessité d'accroître le contrôle démocratique de la société et de l'économie numériques. Juridiquement, la portée de cette déclaration est si modeste que l'on peine à y voir autre chose qu'un résumé, peu synthétique, sans réelle cohérence et même assez mal rédigé, de l'objet des différentes législations européennes.

La multiplication des boussoles, plans, communications, déclarations et autres stratégies masque de plus en plus mal une vision politique au fond assez faible de la politique numérique européenne. Le paradoxe est le suivant : à mesure que la politique européenne du numérique s'étoffe et se densifie, on perçoit en creux la faiblesse du projet politique qui la sous-tend. Il n'y a pas réellement d'amour, mais en revanche il y a désormais beaucoup de preuves d'amour. L'importance matérielle de cette politique se révèle inversement proportionnelle à la conception politique dont elle serait porteuse. Il y a incontestablement un volontarisme politique, une efficacité législative, une densité juridique et, ainsi une véritable politique européenne du numérique. Pourtant, on peine à être convaincu par l'existence d'un projet politique sous-jacent qui chercherait à penser la place de l'individu dans cette transition, dans ce changement de société ainsi annoncé.

La régulation européenne du numérique : la défense implicite d'une vision politique européenne de la souveraineté numérique

La fondamentalité et l'ubiquité des bouleversements induits par l'irruption des enjeux numériques ont fait prendre à l'Europe la mesure de son impuissance, si elle se limite à ne penser son action qu'à travers son marché intérieur. Même si ce marché intérieur reste au cœur de sa stratégie de reconquête numérique, par la création d'un espace européen des données ou la conditionnalité de l'accès aux données des citoyens au respect des règles européennes, l'aveu d'impuissance est là, et suscite un mouvement d'européanisation convergent.

Une régulation inédite

Les États acceptent l'européanisation de la régulation du numérique, même si celle-ci évolue sans fondement juridique propre dans les traités européens. La défense de la souveraineté numérique européenne passe ainsi par une gradation de la régulation. Une régulation douce, proche de la *soft law* pour les compétences auxquelles les États restent attachés. Les États membres acceptent ainsi, de fait, d'exercer en commun des compétences nationales, que la Commission coordonne avec des « boîtes à outils » (pour la 5G, pour l'*e*-santé, pour la numérisation de la justice) ou des « cadres » (pour le filtrage des investissements directs étrangers).

Une régulation plus assumée et contraignante apparaît aussi, en parallèle, dans les domaines stratégiques : régulation des plateformes numériques, de l'intelligence artificielle, de la cybersécurité. L'adoption de régulations générales, que ce soit pour les plateformes numériques ou pour l'intelligence artificielle, dans l'Union européenne porte un objectif fondamentalement politique. L'objectif politique, largement atteint si l'on en juge par l'attention portée à cette régulation dans le monde entier avant même son adoption, est d'afficher une législation européenne identifiable : un Artificial Intelligence Act[4], un Digital Services Act[5], un Digital Markets Act[6] que l'Union peut brandir sur la scène internationale comme autant d'emblèmes d'une politique forte en matière de régulation du numérique.

[4] Proposition de Règlement établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle), COM/2021/206 final.

[5] Règlement (UE) 2022/2065 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques), JOUE L 277, 27/10/2022, p. 1.

[6] Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique (règlement sur les marchés numériques), JOUE L 265, 12/10/2022, p. 1.

La politique européenne du numérique, par les enjeux extraterritoriaux qu'elle assume et les conditions à l'entrée sur le marché intérieur européen qu'elle impose, cherche même à atteindre un « *leadership* numérique » dans la Boussole numérique proposée en 2021 : c'est l'affirmation, classique mais appliquée ici à un domaine qui se veut disruptif, du primat du droit et de la régulation juridique sur un développement perçu comme anarchique de l'innovation technologique, de la défense des valeurs et des droits fondamentaux, de l'approche multilatéralisée sur le plan international. Là où beaucoup d'États dans le monde se contentent de proclamations éthiques, de dispositions ponctuelles, ou d'incitations, l'Europe légifère de façon ostensible, avec un unilatéralisme assumé. Si les déclarations éthiques ne manquent pas en matière de numérique, l'Union européenne est la première à assumer cette approche juridique classique, que l'on pensait dépassée, désuète même, avec l'avènement de la *compliance* et de la corégulation, qui va au-delà de l'autorégulation, des codes de conduite et autres formes de *soft law* dont l'efficacité, sans être nulle, ne peut être que limitée.

L'avènement de régulations asymétriques fondées sur les risques

Le Digital Services Act, le Digital Markets Act et l'Artificial Intelligence Act sont des actes d'autorité, de revendication du volontarisme politique européen. Si les critiques sur les effets néfastes sur l'innovation, notamment pour les industries européennes, n'ont pas manqué, l'Europe mise peut-être sur le fameux *Brussels Effect*, conceptualisé par Anu Bradford[7], pour compenser les freins potentiels au développement économique que cette législation pourrait engendrer. Pour porter cet objectif politique d'une régulation du numérique des « Act », de grandes lois sont nécessaires, même si ses dispositions peuvent se révéler en pratique plus nuancées qu'il n'y paraît.

Ces grandes lois européennes constituent ainsi des étendards de la volonté politique européenne. On retrouve d'ailleurs tous les fondamentaux du droit de l'Union européenne : tropisme juridique, instrumentalisation politique du marché intérieur, défense des valeurs européennes et des droits fondamentaux qui forment le cœur de l'identité européenne. Cette politique, arrimée à l'ambition d'une souveraineté européenne[8], ou, à tout le moins d'une autonomie stratégique, est fondamentale car la transition numérique est l'un des deux grands objectifs politiques de la Commission Von der Leyen, avec le *green deal*.

Construire une politique générale, globale, cohérente, passe par l'adoption de grandes lois à même d'identifier et de rassembler le consensus politique nécessaire au sein des États membres pour l'élaboration d'une politique sans base juridique. Il est d'ailleurs, par nature, difficile de conduire une politique européenne globale au regard de la structuration des compétences de l'Union, envisagées de façon sectorielle malgré quelques exigences de cohérence et de clauses de de transversalité. De ce point de vue, la base juridique du marché intérieur fait, à nouveau, la preuve de son efficacité.

Ce détour par l'objectif politique de ces réglementations est nécessaire pour comprendre les grands équilibres proposés par ces textes : certes le choix est de réglementer les marchés et services numériques, et l'IA mais en gardant une très grande souplesse pour ne pas trop inhiber les innovations. Pour parvenir à cet équilibre délicat, l'Union innove juridiquement en proposant des régulations asymétriques fondées sur les risques.

[7] BRADFORD A. (2020), *The Brussels effect: How the European Union rules the world*, OUP USA, 424 pages.

[8] BERTRAND B. (2021), « La souveraineté numérique européenne : une pensée en acte" *?* », *Revue trimestrielle de droit européen*, Dalloz, pp. 249-278.

Cryptocurrencies and the passion for secrecy

By François VALÉRIAN
Member of the International Board of Transparency International,
Professor of Finance, Regulation and Supervision at Mines ParisTech and
Associate Professor of Finance at Conservatoire National des Arts et Métiers

Cryptocurrencies have developed over the past 15 years, benefiting from a passion for secrecy and a desire to abolish government control. This has created vast opportunities for the financial crimes that opacity allows, among which money laundering. More government is needed, more of a state whose financial regulation serves the needs of citizens, not the "less government" claimed by the first promoters of cryptocurrencies. More government, and more global regulation, since the financial world is global whereas the political world is fragmented.

This article owes much to the very clever and attentive reading of my friend and Transparency International founding member Laurence Cockcroft, as well as to other friends from Transparency International: Ilia Shumanov and his colleagues from Transparency International Russia, Ke Rafitoson from Transparency International Madagascar. The reader interested in this topic may also read with great profit "Cryptocurrencies, corruption and organised crime (u4.no)" at https://www.u4.no/publications/cryptocurrencies-corruption-and-organised-crime.

Since the article signed under the pseudonym of Satoshi Nakamoto and now celebrated as the founding myth of Bitcoin, cryptocurrencies have only grown in importance in the financial economy, reaching in 2021 a total transaction volume of sixteen trillion dollars. This amount, which grew by 567% from 2020[1], is of the same magnitude as the total US banking assets of twenty-four trillion dollars.

We can talk about cryptocurrencies in different ways and easily get lost in the numerical complexities of the codes and algorithms implemented to ensure the proper mechanics of these tools.

We can also try to say what these cryptocurrencies reveal about the diseases of our time and more particularly about two of them, the passion for secrecy and the rejection of any form of government. Cryptocurrencies are a symptom of cryptomania and what we could call statophobia, or rejection of any statal control.

At the very origin of cryptocurrencies, there is the secrecy surrounding the person behind the pseudonym Nakamoto, a secrecy that strangely seems to have given confidence to the first investors in Bitcoin, a secrecy as a guarantee that public institutions could not get their hands on this new currency. The very name cryptocurrency is ambiguous, in that it covers two meanings. Cryptocurrency is a currency that uses encryption algorithms to operate, but it is also a secret currency that satisfies the dream of completely hidden wealth, a treasure island that can be enjoyed by lucky or smart investors, hiding their good fortune from those around them.

[1] Chainanalysis, "The 2022 Crypto Crime Report".

Cryptocurrency indeed is like a far-away island, very comparable to the offshore center whose model it carries to near perfection. This is not lost on cryptocurrency practitioners, who often use real offshore centers in addition to cryptocurrency. Sam Bankman-Fried, the founder of FTX, the much-celebrated cryptocurrency player whose bankruptcy in November 2023 cost several billion dollars, was arrested the following month in the Bahamas, where FTX was otherwise registered, and regulated with the lightness that we know characterizes regulation in offshore centers. Several other cryptocurrency players are registered in offshore centers, such as Ideg Asset Management Limited in the British Virgin Islands.

The proximity between the cryptocurrency and the offshore center does not end however with the cryptocurrency actors' taste for the offshore centers. Cryptocurrencies themselves are offshore centers, far simpler and more efficient in their secrecy than any of the jurisdictions specializing in that sort of business. Laundering through traditional and physical offshore centers required, and still requires, an intermediary who opens an offshore account, a transfer from a third institution and a number of people aware of the transaction. On the contrary, hiding money in cryptocurrencies whose owners cannot be unmasked only requires the digital ability to use electronic marketplaces that sell to their investors the anonymity of transactions in currencies whose owners will not be known.

A cryptocurrency is an offshore center transformed and simplified into a series of codes

The passion for secrecy, or cryptomania, that characterizes cryptocurrencies also amplifies a justifying narrative that we already heard about offshore centers. Cryptocurrencies would allow investors, and human beings in general, to free themselves from a supposedly tyrannical state constraint. The creation of money, since the ancient times, has always been the privilege of a power established at the head of a territory. The ideology of cryptocurrency is to question this privilege of the powerful in order to put money at the service of the greatest number, outside of any central regulation.

The tool that allows this challenge is decentralized control, distributed among the users, a control which can take various technical forms depending on the cryptocurrency, but always amounts to entrusting control to a moving set of human beings, who owe their role in the system only to their digital skills. The technical innovation allowing such decentralized control is the blockchain, and the individuals, or now companies, who replace the central banks and spend days and nights validating transactions, are called the miners. The combination between blockchain innovation and the work of tech-savvy miners would lead to the end of state monetary privilege and to a currency accessible to the greatest number of people, close to all needs, particularly in regions of the world with limited banking services or without strong state structures. Conversely, where the state is oppressive, cryptocurrency would allow to escape its grip.

An anarchist utopia has thus developed in support of cryptocurrencies, an anarchist utopia of our time, therefore more widespread among the affluent than among those deprived of everything, but an anarchy all the same, which hopes for a lasting weakening of all governments or at least of their central banks and financial regulators, and this for the supposed benefit of the greatest number.

The benefit for the many has not been realized

What about the realization of this utopia? Benefit for the many has obviously not been realized. What has happened is what happens in any place where there is wealth, and where the lights are turned off and all control is removed: unscrupulous ingenuity unfortunately prevails over virtue.

Bandits of all kinds roam the world of cryptocurrencies to seize ill-protected sums of money, North Korea has made a specialty of these raids that would finance its nuclear missiles. Other criminals who do not have cryptocurrencies at their disposal ask for them as ransom when they have succeeded in hacking an organization's IT system. This allows them to hide their loot immediately: this is a far cry from the banknote numbers that used to help police track down criminals!

The possibility of money creation, when supported by the confidence of the crypto asset markets, also allows the created money to be used later as collateral for excessive loans that endanger the lending banks, their customers and the taxpayer if these banks need to be rescued. FTX, the second largest crypto asset marketplace, went bankrupt late last year because it had used billions of dollars entrusted to it to invest in its own cryptocurrency, which was thus supported in price, and used as a collateral to get the loans in central bank currencies.

This unregulated possibility of money creation is much more problematic than the abuse committed for centuries by princes or states when they created too much money compared to the wealth generated by the economies they controlled. Indeed, in the case of cryptocurrencies, there is no underlying economy and therefore absolutely no wealth creation beyond the work of the crypto-miners who replace the central banks and allow cryptocurrencies to circulate. The investor who buys dollars today can bet on the growth of the US economy, the one who buys Euros bets on the growth of the Eurozone. The one who buys bitcoins only bets on her or his ability to sell them to more naive people than her or him.

The cryptocurrency market is only speculative, and as it is otherwise very opaque it is also a market considerably exposed to insider trading. Contrary to the promises of the cryptocurrencies' promoters, these currencies remain dominated by intermediaries who create or trade them in large quantities. When Luna, the Terra cryptocurrency, collapsed in the spring of last year causing tens of billions of dollars in losses, the powerful intermediaries who had invested in the currency were able to dispose of it in time and the victims were found in the crowd of small investors who had dreamed of getting rich.

The dream of easy enrichment is at the heart of the cryptocurrency world, nurtured as it often is by high-profile influencers with a financial stake in the success of the cryptocurrency, through a mechanism quite comparable to the one used by some more or less scrupulous start-ups when they attract celebrity support in their search for funds.

Cryptocurrencies: secrecy, corruption and money laundering

Finally, the secrecy of cryptocurrencies and their platforms obviously encourages corruption and money laundering.

Cryptocurrencies have transformed bribe-paying, up to a certain amount, into an extremely easy and safe game. The bribe payer goes to a coffee shop with a used laptop and creates a cryptocurrency wallet. Regular cash deposits are then made to the wallet via a bitcoin ATM. Codes which are the keys to the wallet are then given to the bribe taker who can obtain cash in central bank currencies from a bitcoin ATM anywhere in the world, for example in a holiday resort.

Money laundering with cryptocurrencies is faster than through an offshore center and the hiding techniques are more powerful because they largely circumvent the banking system. To some extent and in spite of all their technological sophistication, the cryptocurrencies constitute a new informal sector, but not an informal sector allowing the poor to survive, rather an informal sector allowing the affluent to play, bet or hide. Money earned illegally can already exist in the form of cryptocurrencies, and for example a bribe can be paid in

this form. In this case everything is already secret. If the money exists in the form of central bank money and if the amount goes beyond bitcoin ATM capacities, it can be used under a false identity to purchase cryptocurrencies, a process also called "cryptocurrency on-ramp", on a platform that does not verify the identity of the actors. Several successive transactions, using various cryptocurrencies and platforms, allow for further concealment of identities through so-called "layering". Adding such successive layers of opacity is obviously more effective than using more regulated markets. The final stage of laundering, using illicit money in the real economy, involves converting cryptocurrencies held in a secret account into usable currency in the open, a process which reverts the initial "on-ramp" and is therefore called "cryptocurrency off-ramp". Even if they are not very numerous, companies accepting payment in cryptocurrencies for services that are more or less easy to identify, or start-ups that can be sold for payment in cryptocurrencies, now form a sufficiently established model that can be used to justify a positive flow of cryptocurrencies.

The ease of concealing identities through trades in cryptocurrencies demonstrates how misguiding a certain narrative about cryptocurrencies is. Decentralized control among the users has always been presented by the promoters of the cryptocurrencies as the guarantee that every transaction is being recorded by the system in a more certain manner than by a centralized authority. This may be true, but if the main information is missing, which is the identity of the players, there is little value in being certain that a transaction happened at an exact day and time between two machines. Such knowledge may help investigative authorities at some point, but not until the identities of the individuals involved are known through other means.

An argument often heard about the limitations of cryptocurrencies for money laundering purposes is that they would be associated to the high valuation risks due to their volatility. The argument does not apply, however, to the so-called "stable coins" linked to strong central bank currencies, and even for more volatile cryptocurrencies the speed of the processes may be such that volatility risks remain modest. A recent investigation by Transparency International has proven that stable coins brought to cryptocurrency dealers in Moscow could be delivered the same or next day in London and in pounds[2].

Total cryptocurrency laundering would have reached $9 billion by 2021, still a small portion of total global laundering (less than 1%[3]), but two observations can be made. Firstly, we are only at the beginning of the expansion of cryptocurrencies, so it is likely that their importance in money laundering will increase rapidly. Secondly, a significant advantage of money laundering through cryptocurrencies is the extreme speed of the operations required. One can have created the company that will receive the payments in cryptocurrencies even before realizing the illicit gain, and once this gain is realized the money can go through all the stages of opacification in a few hours and then return to the system after having erased all its origin. This largely offsets the risk associated with the high volatility of cryptocurrency prices, volatility that would be a significant obstacle if transactions required a longer time.

Fines against crypto companies, largely for non-prevention of money laundering, nearly doubled in 2022, reaching nearly $200 million worldwide, with the largest fines being $30 million against the three founders of BitMex, a U.S. platform.

Remarkably, cryptocurrencies now seem to be considered by money laundering actors as one of the standard tools of their operations. In February 2023, Australian police broke

[2] Transparency International Russia, *From Moscow-City with crypto: A step-by-step guide to receiving cash from Russia anonymously in London*, 2023.

[3] Frank Vogl (*The Enablers*, 2022) evaluates the total annual volume of cross-border illicit financial flows above $2 trillion, Global Financial Integrity's estimates of illicit financial flows related to trade only is $1 trillion (GFI, *Trade Related Illicit Financial Flows*, 2020).

up a laundering ring in Sydney that operated primarily in real estate and luxury goods, but also held cryptocurrencies.

What to do about it? The simplest answer to this question would be to ban cryptocurrencies worldwide. They are described as innovations but the term "innovation" is misleading because it induces an idea of progress. They are more a novelty whose economic impact is quite clearly negative, which favors crime by opacity and also costs a lot of energy, therefore often carbon, spent in the functioning of the decentralized network.

Experience has taught us, however, that such novelties are not easy to get rid of, and their power of attraction will continue to be exerted on various people for more or less legitimate reasons. This is the case with cryptocurrencies as well as with Credit Default Swaps, which largely contributed to the crisis of 2008, or with a number of other financial novelties with high risk and almost no economic utility. They unfortunately remain in the system, mainly because their speculative nature attracts individuals or organizations that are more gambling than investing.

The financial world is global whereas the political world is fragmented. Hence the need for global regulation of cryptocurrencies

Regulation of cryptocurrencies, as on almost every topic, is uneven across the globe. Within the European Union, the 5th Anti-Money Laundering Directive requires cryptocurrency exchanges and cryptocurrency wallet providers to identify their customers. Some countries ban cryptocurrencies, others however do not even regulate them.

The financial world is global whereas the political world is fragmented. This was already a lesson from the 2008 financial crisis and the cryptocurrencies further demonstrate how the regulatory loopholes across the globe can be easily exploited. Since the essential transactions are done digitally without being impeded by physical borders, a few countries with some international connections are enough for platforms and dealers to register there and offer worldwide services. International coordination is crucial and should be prominent on the agenda of the G20 and the international financial institutions such as the IMF. We now have to address a system that not only circumvents the governments, but also largely circumvents the banks and traditional exchanges. What matters is to target the individuals involved everywhere in the world and to target them through transnational cooperation.

Regulating cryptocurrencies is not enough, however. Cryptocurrencies are falsely presented as an answer to the shortcomings of the current financial system, the governance flaws of banks or the limits of financial inclusion. In the North as well as in the South, cryptocurrencies are often marketed to people who are refused loans by banks for their projects, and then end up losing their last savings in vain attempts to get their funding through cryptocurrency speculation. The more the financial system will be perceived as fair, economically and socially useful, the less cryptocurrencies will benefit from the ideological justification that allows their promoters to obtain favorable regulations in many countries. This requires more government, and more of a state whose financial regulation serves the needs of citizens, not the "less government" claimed by the first promoters of cryptocurrencies.

Lastly, the risks associated to cryptocurrencies have to be more vastly communicated by governments and regulating bodies. Young or less young would-be investors consider cryptocurrencies as a "cool" investment where part of our future would take shape. They often ignore the high risks associated to the volatility of the assets they invest in and they strengthen market players and places which offer secrecy to criminals. The battle to be fought is, as often, a battle of ideas. Investing in secrecy is not cool, it should belong to the past, not to the future.

Digital sovereignty: ten years of debate, and afterwards?

The debate on digital sovereignty, a topic that divides digital and institutional actors, coincides with the arrival of the commercial Internet in the early 1990s. The combination of the deindustrialisation of our telecom industries, the de-digitalization of our state computing and a growth model based on the use of services from major US platforms has put us in a highly dependent position. With the war in Ukraine, France must now ensure that it still has some form of digital resilience by relying on its local ecosystem.

A critical discourse unfolds on the orientations taken by France and the European Union in the field of digital sovereignty. It focuses partly on the place of law. It would confine the Union to a subordinate role when others (the United States in the first place) master the foundations of digital. To shed light on this issue, the article presents digital sovereignty as a fact and by law. The fact situation is that large platforms are propelling themselves into the field of sovereignty. To catch up, the European Union relies on competitive regulation while at the same time working to lay the foundations of an ethics through sovereignty.

The Covid pandemic has reinforced pre-existing trends: technological interdependencies that are still real, but thwarted by competition between the United States and China, and the problem of diversifying value chains. The war in Ukraine, which began in February 2022, has only accelerated a global movement towards the consideration of sovereign logics in the digital field. States are naturally acting in different ways depending on their political regime, giving rise to responses and counter-responses combining legal, financial and technological tools. Used for (geo) political ends, digital sovereignty is therefore more than just an industrial ambition – a trend that is likely to be reinforced by the superposition of international crises.

organise competition, security and the use of soft power. France's industrial sovereignty has been undermined by globalisation, with digital European sovereignty short after the dynamics of global oligopolies GAMAM and BAIDU.

The IMT is at the nodal point of sovereignty, it trains the design, engineering and management frameworks to carry the digital transformation of the economy and society and produces knowledge on technologies, architectures, security, uses and transformation of companies. IMT is a source of innovation through the support of companies and the incubation of start-ups.

61 Europe: digital sovereignty and the challenge of technological autonomy
Henri d'AGRAIN

The concept of sovereignty, particularly in the digital field, is being used more and more in the public space. However, it is often misused, and in a way that does little to enlighten the debate on the risks that our loss of technological autonomy poses for the European continent and its economy. In the first part of this article, we attempt to shed some light on the concept of digital sovereignty. In the second part, we present the main risks that Europe faces as a result of its technological dependence.

66 Regaining the levers of sovereignty in cyberspace through a better organisation of missions in the field of cyber security
Hugo ZYLBERBERG

In a cyber environment that is now characterised by digital instability, it is essential to find ways of taking better account of cyber risk at all levels of organisations. To this end, the way the State is organised seems to be a useful way of identifying priority functions and strategic objectives that provide a practical response to these major cyber security challenges.

70 Can we move towards quantum sovereignty?
Alice PANNIER

Quantum information science and technology is a vast field that includes computing, telecommunications, detection and sensors, with a wide range of applications. Taken together, these technologies promise to revolutionise our information systems. The significant advances in quantum technologies in recent years, and their implications for security and the economy in particular, have created a real momentum of interest among governments, including in Europe.

Despite the impressive advances made by the two giants, China and the United States, and unlike most other digital technologies, Europe (in the geographical sense) is well placed in the global race for quantum technologies. On this promising basis, can Europe hope to achieve technological sovereignty in quantum technology? There are two main challenges: firstly, reconciling the objective of sovereignty with international cooperation, and secondly, ensuring that any quantum strategy is rooted in a holistic, long-term perspective.

75 Sovereignty and digital resilience: impossible mission?
Olivier BEAUREPAIRE, Thomas BOLLE, Sophie LAFON & Stanislas SMIEJAN

This article summarises the thoughts of the mission carried out for the *Fondation Nationale Entreprise et Performance* on the general theme of digital sovereignty.

The authors have focused on two specific subjects, quantum computing and the ethics of artificial intelligence, two areas in which the members of the mission believe that France and Europe can maintain their sovereignty, and show, in their recommendations, how this can be achieved and the pitfalls to be avoided.

The first submarine telegraph cables in the 19th century were already a strategic power issue exploited by states. Today, maintaining these infrastructures is seen as a critical issue, because the development of digital technologies has given data exchanges an important place in the formalisation of the global market, and transcontinental technical dependencies have intensified. So owning submarine cables or having specific skills in this area means having new powers and being able to exploit dependencies on these infrastructures. The owners of cables, and in particular the Big Tech companies that have invested massively in this field, have the capacity to influence not only access to the continent's resources, but also the technical, political and cultural aspects. To understand these new balances of power, this article first looks at the conditions of interdependence that give submarine cables their important place today. It then goes on to analyse the strategies of dependence and technological subjugation, using the example of Africa, which is now the expansion ground for the new cable owners.

The notion of sovereignty has recently regained a central place in public debate, without however really renewing the dichotomy of State action between a patrimonial conception (dominium) and control (imperium). However, in the satellite imagery sector, given the rise of New Space, it seems that the optimum approach might be to favour a form of hybridisation between ownership and impact, from the data to its exploitation. To this end, the State should pursue the creation of an ecosystem based on a form of public-private continuum. This would maximise the desired end effect: power in action, dictated by the imperative of strategic autonomy.

Courses of action and levers

Public procurement plays a crucial role in promoting digital sovereignty. The massive adoption of digital tools during the pandemic has made companies more dependent on large foreign platforms. To preserve our autonomy and our ability to excel in a world dominated by AI, it is essential to make greater use of French or European solutions in public procurement, particularly for strategic purchases and the protection of sensitive data.

By positioning itself today on sovereign digital solutions, France can regain control of its personal and industrial data, thereby guaranteeing its freedom, autonomy and capacity for innovation. The State can play a more directive and coercive role in encouraging the adoption of sovereign solutions in public administrations and companies.

The future will depend on decisions taken at European level, but France can set an example by moving forward on the road to digital sovereignty.

99 Global Internet governance: the levers
Lucien CASTEX

The digital transformation of society has turned the Internet into an everyday object, a combination of uses and technical artefacts. Its governance is characterised by an ad hoc model borrowing from multipartism, multilateralism and the uses of the network. Today, this governance is disputed, at the heart of a power struggle over the network of networks.

103 Changing cyber postures: how China, Russia, the USA and the EU see the world
Rayna STAMBOLIYSKA

Some technological advances are so significant that they fracture our understanding of the world. Experts and policy-makers are beginning to dissect, albeit sometimes timidly, the potential consequences of adding unfamiliar, advanced and potentially devastating new technologies to the toolbox of opposing powers. In this context, cybersecurity postures are particularly attractive. These postures provide a better understanding of the strategic changes underway among the main players on the geopolitical chessboard. We examine China, Russia, the United States and the EU through the prism of their cyber postures, which reflect the civilisational visions that determine the future actions of these players. These strategies reflect the long-term perspectives of these actors, offering insight into their motivations and possible blind spots that need to be taken into account.

108 Digital, an ambivalent power: what strategic autonomy for Europe?
Hugues de JOUVENEL & Jean-François SOUPIZET

The authors begin by pointing out how the rise of digital technology is a veritable revolution that is spreading to all areas and giving the Internet giants unprecedented power over governments and international institutions. They then show how these technologies bring opportunities but also risks that require constant vigilance, if not a capacity for anticipation, which is unevenly distributed. Finally, they highlight the limits of Europe's strategic independence and outline three hypotheses for the future of its "strategic autonomy".

113 Digital sovereignty without the State: is there individual sovereignty for "homo numericus"?
Pierre NORO

The concept of "digital sovereignty" usually refer to nation-states, their ability to provide for their digital needs, and occasionally to "Big Tech" companies they often depend on. However, considering the ideological roots of the Internet, the advocacy work of digital rights activists, and the practices of various communities revolving around FOSS, encryption or blockchain technologies, digital tools might primarily be technological foundations for users to claim a new form of sovereignty for themselves.

This article aims to outline this concept, probing its meaning and historical legitimacy. Beyond a limited initial definition of a de facto self-sovereignty, the

Issue editor
Julien NOCETTI

Ont contribué à ce numéro

Henri d'AGRAIN est diplômé de l'École Navale, et breveté de l'École des officiers transmetteurs et de l'École de Guerre. Il est auditeur de la 47e session nationale « armement et économie de défense » de l'Institut des Hautes Études de la Défense Nationale (IHEDN).
Officier de marine pendant 27 ans, il a alterné, au cours de sa carrière, des fonctions opérationnelles embarquées, des commandements à la mer et des postes de direction dans le domaine des systèmes d'information et de communication des armées. Il fut, dans ses dernières fonctions au sein de l'état-major de la Marine, directeur des systèmes d'information et autorité de cyberdéfense de la Marine nationale avec le grade de capitaine de vaisseau. Il a quitté la Marine le 31 août 2013.
De 2013 à 2016, Henri d'Agrain était Directeur général du Centre des Hautes Études du Cyberespace (CHECy).
En octobre 2016, Henri d'Agrain rejoint le Cigref, dont il est Délégué général depuis le 1er janvier 2017.
Par ailleurs, depuis 2015, Henri d'Agrain est membre, en tant que personnalité qualifiée auprès du Parlement, de la Commission Supérieure du Numérique et des Postes.
Marié et père de cinq enfants, Henri d'Agrain est chevalier de la Légion d'honneur et officier de l'ordre national du mérite.
→ ***Europe : la souveraineté numérique au défi de l'autonomie technologique***

Olivier BEAUREPAIRE est Directeur Data de l'activité TER – SNCF Voyageurs. Titulaire du Master MIAGE Finances & Informatique délivré par l'université Paris Dauphine, il a précédemment exercé des fonctions de Directeur de la Digitalisation et de l'Innovation, DSI, RSSI et directeur de programmes de transformation, pour différentes activités au sein du secteur Transport et Tourisme (SNCF Mobilités, Rail Solutions, Gares & Connexions, SNCF Voyages).
→ ***Souveraineté et résilience numérique : mission impossible ?***

Brunessen BERTRAND est Professeure agrégée de droit public à l'Université de Rennes 1, spécialiste des questions numériques : intelligence artificielle, souveraineté numérique, cybersécurité, régulation des plateformes (marchés et services numériques), lutte contre la désinformation, identité numérique, *blockchain*, services publics numériques, gouvernance des données de santé, impact environnemental du numérique, etc.
Elle est directrice du Centre de recherches en droit européen de l'Université de Rennes 1.
Brunessen Bertrand est titulaire d'une chaire Jean Monnet, dans le cadre de laquelle elle dirige plusieurs projets de recherche collectifs : souveraineté numérique, données de santé, données environnementales, *blockchain*, intelligence artificielle, régulation des plateformes, métavers, etc.
Elle dirige plusieurs thèses actuellement sur des sujets tels que *Blockchain* & *Privacy*, le droit européen de la cybersécurité, l'utilisation de l'IA dans l'action publique.
Elle a rédigé une pluralité d'articles sur le droit européen du numérique et dirigé plusieurs ouvrages collectifs sur *La politique européenne du numérique* (Larcier, 2022) ou le *Règlement général pour la protection des données personnelles, aspects institutionnels et matériels* (Mare & Martin, 2020).
→ ***Le droit au service de la souveraineté numérique de l'UE***

Annie BLANDIN est Professeur à l'IMT Atlantique, au sein du département Systèmes réseaux, cybersécurité et droit du numérique. Annie Blandin est co-responsable de la voie d'approfondissement « Plateformes numériques : infrastructures et marchés ». Outre ses enseignements en droit du numérique, elle effectue des travaux de recherche sur un

ensemble de sujets qui vont de la régulation des télécommunications et des plateformes au droit des données, avec un accent sur les questions environnementales. La souveraineté numérique constitue le fil rouge de sa réflexion. Elle est enfin investie dans des activités d'aide à la décision publique et a notamment été membre du Conseil national du numérique lors de la mandature 2018/2020. Elle préside actuellement le pôle Innovation et prospective du Conseil national de l'information géolocalisée.
Publications : https://cv.archives-ouvertes.fr/annie-blandin
→ ***Numérique et marché : souveraineté de fait, souveraineté par le droit***

Thomas BOLLE est officier de gendarmerie (lieutenant-colonel). Titulaire d'un DEA sécurité internationale et défense et d'un *executive* mastère d'HEC Paris, il est actuellement professeur au centre de formation des dirigeants de la gendarmerie. Il a exercé auparavant des responsabilités en métropole en gendarmerie mobile et départementale et à l'étranger (Europol).
→ ***Souveraineté et résilience numérique : mission impossible ?***

François BOURRIER-SOIFER a effectué une première partie de carrière en qualité d'avocat au barreau de Paris puis a rejoint en 2020 la société Preligens en tant que Directeur général adjoint, dont il était précédemment investisseur et membre du conseil d'administration. Il y assure désormais des fonctions en lien avec les opérations, le commerce et la coordination de programmes gouvernementaux, dans le domaine de l'intelligence artificielle appliquée à la défense et au renseignement.
→ ***Imagerie satellitaire et souveraineté : de la donnée à son exploitation, vers un continuum public-privé***

Lucien CASTEX est le représentant de l'AFNIC pour les affaires publiques et les partenariats. Il représente l'Afnic en France et à l'International dans le champ des politiques publiques liées au développement de l'internet et du numérique. À ce titre, il coordonne le Forum français sur la gouvernance de l'Internet (FGI France) et participe à l'organisation du Forum mondial organisé sous l'égide des Nations Unies (UN IGF). Depuis 2022, il est le point focal de l'Afnic au sein de l'Union internationale des télécommunications (UIT) et au sein des groupes de travail interministériels dédiés.
Il siège également au sein de l'Observatoire de la haine en ligne de l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom) et est membre du Conseil d'administration du *think tank* Renaissance numérique.
Il est par ailleurs chercheur associé au sein de l'Université Sorbonne Nouvelle – Paris 3 et a été nommé au sein de la CNCDH.
Dernières publications :
CASTEX L. (2023), « La gouvernance de l'internet et la construction d'un nouveau multilatéralisme », La souveraineté numérique (dir. Bertrand B.), Larcier, à paraître 2023.
CASTEX L. (2023), « Le chiffrement des communications électroniques, du droit au code. La construction d'un droit français du chiffrement en tension », Gouverner par les données ? (dir. Theviot A.), ENS Éditions.
CASTEX L. (2023), « La transition écologique face à la transition technologique », Le droit public économique du monde d'après, Mare & Martin.
ROSSI J., MUSIANI F. & CASTEX L. (2022), « La gouvernance d'Internet, entre infrastructures et espaces socio-politiques : apports de la recherche », Terminal, pp. 132-133.
CASTEX L. (2022), « Allers et retours de la neutralité d'internet », Droits fondamentaux et crise du pluralisme (dir. Bottini F.), Mare & Martin.
PERARNAUD C., ROSSI J., CASTEX L. & MUSIANI F. (2022), "'Splinternets,: Addressing the renewed debate on internet fragmentation [Research Report] Parlement Européen" ; Panel for the Future of Science and Technology (STOA).

CASTEX L., FAVRO K. & ZOLYNSKI C. (2021), « Lutter contre la haine en ligne : de l'appel du 18 juin au discours de la méthode », Recueil Dalloz 2021, pp. 246-25.
→ ***Gouvernance mondiale d'internet : les leviers***

Ophélie COELHO est une chercheuse indépendante, spécialiste en géopolitique du numérique. Elle est membre du Conseil scientifique de l'Institut Rousseau et de l'Observatoire de l'éthique publique. Ses travaux abordent les enjeux géopolitiques relatifs aux infrastructures et aux technologies numériques. À ce titre, elle étudie également les phénomènes de dépendances techniques et industrielles, leurs conséquences sur la formation du droit du numérique et leurs externalités négatives sur l'environnement. En parallèle, elle travaille depuis 2009 dans le secteur du numérique en tant que développeuse *front-end*, cheffe de produit et chargée de recherche utilisateur.
→ ***Notre vie numérique dépend-elle des câbles sous-marins ?***

Florence G'SELL est professeure de droit privé à l'Université de Lorraine et titulaire de la Chaire Digital, Gouvernance et Souveraineté de Sciences Po. Agrégée de droit privé et sciences criminelles, elle a commencé sa carrière académique en travaillant principalement sur le droit de la responsabilité civile, les systèmes judiciaires et le droit comparé. Elle se consacre depuis plusieurs années au droit du numérique et notamment aux problématiques liées à la régulation des plateformes, à la manière dont le droit peut appréhender des technologies et des environnements inédits (*Blockchain*, *Metaverse*), à la notion de souveraineté numérique et plus généralement aux politiques publiques relatives au numérique. Au cours de l'année universitaire 2023-2024, Florence G'sell est professeure invitée au Cyber Policy Center de l'Université de Stanford.
→ ***L'avenir incertain des flux de données transatlantiques***

Jean-Noël de GALZAIN est PDG et fondateur de WALLIX Group, *leader* européen de la cybersécurité des accès et des identités. La société a été créée en 2003 et est aujourd'hui cotée sur Euronext Growth depuis juin 2015 (ALLIX).
Impliqué dans l'écosystème de l'innovation, du numérique et investisseur, il est fondateur et président du groupement HEXATRUST, créé en 2014 qui regroupe aujourd'hui 80 entreprises championnes françaises et européennes de la cybersécurité et du *cloud* de confiance.
Il est directeur du projet « Cybersécurité & Sécurité de l'IOT » du comité stratégique de filière « Industrie de sécurité » à l'origine de la stratégie nationale de cybersécurité, et fondateur en 2021 du fonds d'investissement « Cyber Impact Ventures » dédié aux *start-up* de la cybersécurité.
→ ***La commande publique : un accélérateur de la souveraineté numérique***

Alain GARNIER, innovateur en série et entrepreneur dans l'âme, fonde sa première société, Arisem, à seulement 26 ans. La société est revendue 10 ans plus tard, en 2003, à Thalès, permettant à Alain Garnier de se lancer dans de nouvelles aventures entrepreneuriales.
Il cofonde alors Evalimage en 2004, puis Jamespot en 2005. Il est depuis cette date président-fondateur de cette entreprise éditrice de logiciels collaboratrices en pleine croissance (+ 20 % en 2022) qui compte aujourd'hui une quarantaine de collaborateurs et dont la solution éponyme est utilisée par plus de 400 000 utilisateurs à travers le monde.
Convaincu que la réussite passe avant tout par le collectif et la collaboration, Alain Garnier est impliqué depuis des années dans l'écosystème numérique français : président de l'association EFEL Power (Entreprendre en France pour l'Édition Logicielle) qui œuvre pour la reconnaissance du savoir-faire des éditeurs de logiciels français, Alain Garnier est également membre des associations Numeum, Cap Digital et d'Hexatrust, et co-pilote du groupe de travail collaboratif du comité stratégique de Filière Numérique. Enfin, il

accompagne, coache et partage ses conseils aux professionnels souhaitant se lancer dans l'entrepreneuriat.

→ ***La commande publique : un accélérateur de la souveraineté numérique***

Paul JOLIE est ingénieur général des Mines, diplômé de l'École polytechnique et de l'École nationale supérieure des télécommunications. Il est également titulaire du MBA Edhec.

Après une carrière passée au centre de recherche de France Télécom et dans différents services opérationnels de l'opérateur, il rejoint l'administration en 2008 pour occuper un poste de DSI adjoint au ministère des Affaires étrangères. Après un passage à l'INRIA, il occupe le poste de sous-directeur de l'informatique centrale au ministère de l'Économie et des Finances. Après deux ans en tant que conseiller pour le numérique auprès du ministre d'État de Monaco, il revient à Bercy pour occuper un poste de conseiller au SISSE. Il rejoint le Conseil général de l'Économie en 2020, en tant que référent Intelligence artificielle.

→ ***Politique chinoise de l'IA : comment la Chine joue au go***

Hugues de JOUVENEL a été pendant 40 ans délégué général de Futuribles International dont il est aujourd'hui président d'honneur. Fondateur et rédacteur en chef de la revue *Futuribles*. Il est expert en prospective et stratégie, notamment sur les relations science, technologie et société.

→ ***Le numérique, un pouvoir ambivalent : quelle autonomie stratégique pour l'Europe ?***

Francis JUTAND a été enseignant, chercheur, chef du département électronique et fondateur du laboratoire sur les VLSI à Télécom Paris de 1975 à 1992. Il a dirigé l'école Télécom Bretagne de 1992 à 1996 puis il a été nommé Directeur scientifique du CNET, le centre de R&D d'Orange. En 2000, il est nommé Directeur scientifique du département STIC du CNRS à sa création. Il a été le concepteur du pôle Cap Digital créé en 2004, dont il a été le vice-président académique jusqu'en 2012. En 2005, il rejoint l'Institut Télécom pour prendre la direction scientifique, il obtient le label Carnot Télécom et Société Numérique en 2006, fait entrer l'Institut Télécom dans l'Alliance nationale Allistene. En 2012, il prend la direction scientifique de l'Institut Mines-Télécom. L'IMT devient membre fondateur de l'Alliance pour l'industrie du futur et créateur de l'Académie franco-allemande pour l'industrie du futur avec la TUM. Il devient le Directeur Général Adjoint de l'IMT en 2015 jusqu'à son départ en 2023. Il a travaillé à la création de la chaire « Valeur et politique des informations personnelles » en 2013 et de la chaire « Économie des Communs de Données » en 2023.

Il a été membre créateur du RNRT, a présidé le CCSSTIC de l'ANR, membre du Conseil National du Numérique de 2013 à 2016 et auteur en 2014 du rapport sur la neutralité des plateformes numériques. Il a présidé le comité national du débat sur l'ouverture des données de transport en 2015 qui a introduit la notion de donnée d'intérêt général. Il a été nommé en 2022 au conseil scientifique de One Point. À son départ à la retraite le 1er avril il est nommé membre associé du CGE.

Prospectiviste, il travaille sur l'impact du numérique sur l'économie et la société. Il a édité un ouvrage collectif en 2013 « La métamorphose numérique, pour une société de la connaissance et de la coopération », et participé à de nombreux ouvrages de prospective. Il est membre de l'Association française de prospective.

→ ***L'IMT au cœur de la stratégie nationale de souveraineté numérique***

Tariq KRIM est un entrepreneur et pionnier de l'Internet. Il a été l'un des principaux défenseurs d'une souveraineté numérique de la France. Il est également l'initiateur du mouvement Slow Web, qui prône un usage apaisé du numérique et de l'intelligence artificielle.

Il a fondé plusieurs *start-up*, dont Netvibes et Jolicloud. Il a été conseiller du gouvernement français (eG8 et vice-président du Conseil national du numérique). Il vient de lancer Cybernetica.fr, une maison d'édition, et un *think tank* qui étudie les interdépendances entre le numérique, l'intelligence artificielle, la géopolitique, la culture et le monde de la défense.
En 2007, il a été le premier Français à recevoir le prix TR35 du MIT pour le numérique. Il a également été nommé Young Global Leader du Forum économique de Davos.
Il est diplômé de l'Université Paris 7, de l'ENST et de la Harvard Kennedy School. En 2019 il est promu officier des Arts et des Lettres.
→ ***Souveraineté numérique, une occasion manquée***

Sophie LAFON est Directrice adjoint à la Direction Statistiques et Valorisation des Données au RTE (Réseau de Transport d'Électricité). Elle est titulaire d'un Master 2 professionnel en Gestion / Export et d'un Master 1 en Langues étrangères appliquées. Elle a exercé auparavant des fonctions de contrôle de gestion, de pilotage de projet d'infrastructure et d'accompagnement de la transformation digitale des fonctions *corporate*.
→ ***Souveraineté et résilience numérique : mission impossible ?***

Julien NOCETTI est chercheur, spécialiste des questions numériques et cyber internationales. Il est actuellement chercheur associé à l'IFRI et au centre GEODE (Géopolitique de la datasphère – Université Paris 8), ainsi que responsable de la chaire Gouvernance du risque cyber à Rennes School of Business. Entre 2019 et 2023, il a été enseignant-chercheur en relations internationales et études stratégiques à l'Académie militaire de Saint-Cyr Coëtquidan. Docteur en sciences politiques, il a été chercheur à l'IFRI entre 2009 et 2019. Il est par ailleurs membre du conseil d'orientation stratégique du CIGREF et membre du comité de rédaction de la revue *Études françaises de renseignement et de cyber*. Ses recherches portent sur la conflictualité et la gouvernance internationale du numérique, la diplomatie de l'intelligence artificielle et des données, ainsi que sur les stratégies cyber et informationnelles de la Russie. Il publiera prochainement *Géopolitique du numérique* aux Éditions La Découverte (coll. Repères).
→ ***Introduction - Souveraineté numérique : dix ans de débats, et après ?***
→ ***La souveraineté numérique, un instrument de politique étrangère***

Pierre NORO est enseignant à Sciences Po Paris, au Learning Planet Institute (Université Paris-Cité), chercheur et entrepreneur. Ses travaux sont consacrés aux politiques de l'innovation, aux technologies *blockchains*, à la souveraineté numérique, à la gouvernance décentralisée, l'innovation sociale et aux problématiques éthiques dans le numérique. Après plusieurs années au sein des Programmes *Blockchain* et Cryptoactifs de la Caisse des Dépôts et Consignations, Pierre Noro a coordonné la Chaire Digital, Gouvernance et Souveraineté de l'École d'Affaires Publiques de Sciences Po. Il collabore désormais à plusieurs projets d'entrepreneuriat social, ainsi qu'à l'élaboration de Pebble.vote, la première plateforme de vote en ligne décentralisée, transparente et sécurisée, avec une équipe de chercheurs internationale.
→ ***La souveraineté numérique sans l'État : y a-t-il une souveraineté individuelle pour « l'homo numericus » ?***

Alice PANNIER est responsable du programme Géopolitique des technologies à l'Institut français des relations internationales (Ifri). Ses recherches portent sur la dimension géopolitique des nouvelles technologies, les politiques technologiques européennes, et les relations extérieures de l'Europe. Elle a également longtemps travaillé sur la sécurité européenne et les politiques de défense des pays européens, notamment la France et le Royaume-Uni.

De 2017 à 2020, elle était professeure assistante en relations internationales et études européennes à la Paul H. Nitze School of Advanced International Studies (SAIS) de l'Université Johns Hopkins à Washington. Elle a également travaillé comme chercheuse postdoctorante à l'Institut de recherche stratégique de l'École militaire (IRSEM). Elle est diplômée du King's College de Londres et de l'Université Panthéon-Sorbonne et titulaire d'un doctorat en science politique de l'IEP de Paris, en co-direction avec le King's College.
→ ***Pourra-t-on tendre vers une souveraineté quantique ?***

Jean-Paul SMETS, fondateur de l'éditeur de logiciels libres Nexedi, puis de l'équipementier 5G et fournisseur de *cloud* libre Rapid.Space, est ingénieur des mines et diplômé de l'École normale supérieure avec un doctorat en informatique. Il a acquis une expérience industrielle dans l'industrie de l'habillement, l'industrie pétrolière, les associations à but non lucratif et à la préfecture de région Lorraine. Il est l'auteur en 1999 avec Benoît Faucon du premier ouvrage sur les logiciels libres – *Logiciels libres : Liberté, Égalité, Business*. Après avoir créé en 2000 le progiciel de gestion intégré "ERP5" autour d'un modèle unifié minimaliste pour la gestion des entreprises, il est l'un des inventeurs en 2008 du *edge computing* et le concepteur du logiciel d'exploitation de *cloud* "SlapOS". Il est un membre actif d'associations de logiciels libres, a joué un rôle clé dans la campagne Eurolinux pour protéger l'innovation des effets néfastes des brevets logiciels, et a créé en 2021 l'alliance européenne des industriels du *cloud* (EUCLIDIA) dont les membres commercialisent et exportent plusieurs solutions technologiques européennes pour un *cloud* indépendant.
→ ***Confiance numérique ou autonomie, il faut choisir***

Stanislas SMIEJAN est Directeur marketing chez ADISSEO, après avoir occupé la fonction de Chef de Cabinet du CEO, en charge notamment de la transformation digitale. Il est diplômé d'HEC Paris et du King's College de Londres. Il a également obtenu un double diplôme à l'Université de Tsinghua (Pékin) lors de sa dernière année à HEC. Par le passé il a exercé les fonctions de Senior Analyst en Transaction Services chez Ernst & Young, de Manager en Développement International chez Kompass, et de Consultant Senior en Stratégie chez Roland Berger.
→ ***Souveraineté et résilience numérique : mission impossible ?***

Jean-François SOUPIZET est conseiller scientifique auprès de Futuribles International. Ancien élève de l'ENSAE, titulaire d'un doctorat de sciences économiques de l'Université Libre de Bruxelles. Il a consacré sa carrière aux technologies de l'information et aux relations internationales. Son parcours l'a conduit du ministère des Affaires étrangères (Abidjan, Québec), au Bureau Intergouvernemental pour l'Informatique (Rome) et à la Commission européenne (Bruxelles). Auteur de « La fracture numérique Nord Sud » (Economica, 2005) et de nombreux articles sur le numérique, il est également professeur invité à l'Externado de Colombie et membre du Club des Vigilants.
→ ***Le numérique, un pouvoir ambivalent : quelle autonomie stratégique pour l'Europe ?***

Rayna STAMBOLIYSKA est la fondatrice et la directrice générale de RS Strategy, une société de conseil qui fournit aux entrepreneurs et aux PME une expertise utile pour les aider à faire face à l'incertitude. Rayna Stamboliyska se concentre sur la diplomatie numérique et la résilience de l'UE par le biais de la cybersécurité, des menaces hybrides, de l'autonomie stratégique et de la protection des données. Elle est également Digital EU Ambassador pour la Commission européenne, enseigne à Sciences Po Paris et est membre du conseil d'administration de la Fondation européenne Women4Cyber. Elle est experte indépendante et rapporteur du groupe de travail *ad hoc* de l'ENISA sur les menaces émergentes et futures et experte externe du Centre d'innovation d'Interpol.

Rayna Stamboliyska copilote la commission de recherche « Gouvernance et géopolitique du numérique » au sein du *think tank* Renaissance numérique.
Auteur primée pour son dernier livre *La face cachée d'Internet* (Larousse-Hachette, 2017), elle a étudié en profondeur l'impact des données et de la technologie dans les zones de conflit et de post-conflit dans la région MENA, en Europe de l'Est et en Asie centrale. Multilingue, elle a été consultante pour des organisations internationales (Banque mondiale, OCDE, PNUD, Unesco, entre autres), des entreprises privées, des gouvernements et des organisations à but non lucratif. Énergique et passionnée, Rayna Stamboliyska est une conférencière reconnue dans le domaine de la sécurité de l'information, engagée à informer les personnes extérieures au secteur sur les menaces et les meilleures pratiques en matière de sécurité.
→ ***Les évolutions des postures cyber : comment la Chine, la Russie, les États-Unis et l'Union européenne voient le monde***

François VALÉRIAN est ingénieur général des Mines honoraire, polytechnicien et docteur en histoire. Il a exercé différentes responsabilités à la fois dans le secteur public et le secteur privé, et il a été rédacteur en chef des *Annales des Mines*. Il enseigne désormais la régulation financière et la finance à l'École des Mines de Paris et au Cnam, et il est membre du conseil d'administration international de Transparency International. Il est l'auteur de plusieurs ouvrages et articles d'économie ou d'histoire.
→ ***Cryptocurrencies and the passion for secrecy***

Hugo ZYLBERBERG est Chef d'État-Major de la sous-direction Stratégie de l'Agence nationale de la Sécurité des systèmes d'information (ANSSI) où il travaille notamment sur l'anticipation stratégique ainsi que sur l'organisation de l'État en matière de cybersécurité. Auparavant, il a travaillé au sein de l'équipe Cybersécurité de PwC et pour l'École d'Affaires publiques et internationales de Columbia University à New York. Il est diplômé de l'École polytechnique et de la Harvard Kennedy School.
→ ***Retrouver des leviers de souveraineté dans le cyberespace grâce à une meilleure organisation des missions dans le champ de la cybersécurité***