# Newsletter n°42 - 28 octobre 2022

## □□ Édito

**Nos exploits de demain**

Le 20 octobre, le tribunal administratif a sommé le ministère de la Santé de procéder au retrait de l'étrange expression « Health Data Hub » de l'ensemble des « supports de communication destinés au public français ». Great news ! Mais pour prévenir les habituels narquois, posons peut-être ceci : L'anglais est une langue admirable, si agréable à entendre et à parler. Pour autant, elle n'a aucun lieu d'être tenue pour la langue des affaires, de l'excellence technologique, de la modernité ou des relations internationales; pas plus que l'italien n'a lieu d'être tenu pour celle de la poésie ou le français pour celle de la cuisine. La langue est un outil, c'est « un code ». Et nous plier de manière universelle à l'usage d'une seule d'entre elles, ça n'est rien d'autre que livrer le monde au « logiciel » de ses auteurs et nous exposer à l'appauvrissement de notre expression. Beaucoup de succès américains tiennent d'abord à l'étiquette ringarde que nous avons nous mêmes accolée au français, par manque d'estime et de fierté. C'est pourquoi si nous souhaitons recouvrer une forme de souveraineté dans quelque domaine que ce soit, nous devrons avant toute chose dépasser cette inexplicable gêne servile à dire au monde dans notre propre langue nos propres exploits de demain .

**Bertrand Leblanc-Barbedienne**

---

---

**Nous recevons aujourd'hui un ancien de l'Ecole de Guerre Economique (EGE), Franck DeCloquement, qui est expert-praticien en intelligence économique et stratégique (IES), et membre du conseil scientifique de l'Institut d'Études de Géopolitique Appliquée – EGA. Cet entretien a été publié le 28 octobre 2022.**


**La guerre économique est réellement meurtrière.**

---

**🎙️ Le grand entretien**

***1/ Quelle est votre vision de la souveraineté technologique ?***

J'ai coutume de dire avec le sourire que je ne suis pas sujet aux « visions », et me méfie donc grandement de celles d'autrui, tels les « mêmes » chers à Richard Dawkins[1].

Injustement vilipendées par les inconditionnels des bienfaits de la mondialisation heureuse (« globalization » en anglais), **les thématiques de la souveraineté nationale et de l'autonomie stratégique semblent avoir repris ces dernières années du poil de la bête, et une nouvelle forme de vigueur dans notre Landerneau médiatique d'infos-continues. Mais aussi et surtout, un nouveau statut de respectabilité et un nouvel encrage dans les cœurs et les esprits de nos concitoyens.** Si tout ceci demeure en définitive très fragile et parfaitement

conditionnel, le réveil des consciences et leur saisissement semblent pourtant actés. Le contexte actuel de regain des tensions géopolitiques n'y est peut-être pas étranger.

**A mes yeux, et pour répondre à votre première question, « la technique », ce sont avant tout des moyens, des instruments et des outils. Si bien que la « souveraineté technologique » recoupe selon moi tous les moyens de rester maître de ces outils au bénéfice de notre communauté de destin.** Car l'on peut très rapidement ne plus l'être, quand l'outil finit par vous asservir ou vous « piloter », ou quand celui-ci est conçu et/ou commercialisé par des opérateurs étrangers concurrents (« amies ou ennemies ») à des fins subreptices, hostiles ou d'ascendance belliqueuses. La réalité des combats concurrentiels pour la suprématie économique est violente, beaucoup semblent l'avoir hélas totalement oublié. **La guerre économique est réellement meurtrière et pas uniquement symbolique comme beaucoup l'ont trop longtemps cru.** Car elle a quelque chose à voir avec la prédation et la lutte pour la survie dans le règne animal, et a maille à partir avec nos origines anthropologiques sacrificielles et violentes, aux fondements même de notre commune humanité[2]. Des mécanismes mimétiques oubliés ou méconnus, qui régentent pourtant implacablement la vie de nos sociétés et celle de leurs membres depuis la nuit des temps, comme nous les révèlent avec clairvoyance l'académicien français défunt René Girard à travers ses nombreux ouvrages. Et **l'objectif immémorial poursuivi dans ce cas de figure par l'adversité demeure toujours la domination ou la défaite de l'antagoniste – ou de l'ennemi juré – par l'usage immodéré de la ruse et de la tromperie. Très souvent, via l'implémentation, l'adoption et la diffusion – parfois généreuse[3] – de sa technologie dans l'écosystème social ou industriel adverse.**

**Toutes techniques ou technologies humaines véhiculent bien entendu, un substrat idéologique consubstantiel à leur création**, induit en amont de sa conception (« By Design »

pourrions-nous dire métaphoriquement). Les intentions sous-jacentes étant fatalement packagées et incluses avec l'objet lui-même en quelque sorte, dès sa gestation… Le logiciel « Power Point » représente une parfaite illustration en la matière[4] de nos propos. **Dans l'industrie de défense par exemple, la souveraineté est avant tout technologique.** Mais elle porte aussi sur la chaîne d'approvisionnement. Et cela implique aussi de maîtriser les technologies de souveraineté, mais également de contrôler les principales sources et chaines d'approvisionnement pour que l'ensemble demeure opérationnel, sans trop d'anicroches logistiques dans l'interstice. Notamment en matériaux rares et en fournitures de composants électroniques indispensables au bon fonctionnement du produit fini. A la lumière des fortes tensions internationales actuelles, et de l'impact géoéconomique majeur du conflit entre l'Ukraine et la Russie sur le reste du monde, la récente réapparition de la guerre de haute intensité aux portes de l'Europe conduit à porter une attention toute particulière sur ce sujet. D'autant plus quand nos États impécunieux ou désargentés ne disposent plus véritablement du monopole ubiquitaire en matière de souveraineté, ou de garantie des conditions fondamentales de notre sécurité nationale.

**La crise présente, et celles à venir, nous montrent sans ambages combien une économie résiliente repose pour l'essentiel sur un appareil productif et industriel puissant et intégré.** Les États en pointe – et soucieux de leurs prérogatives – l'ont bien compris et d'ailleurs mis en œuvre bien avant le nôtre. Et cela très en amont des derniers bouleversements internationaux en date : les notions « d'indépendance » et de protection de nos intérêts fondamentaux reprennent tout leur sens dans ce contexte durci, lorsque des pénuries se profilent et risquent de se succéder désormais à un rythme soutenu au grand dam de nos concitoyens. La pandémie de la Covid-19 nous l'a d'ailleurs rappelé collectivement et très crûment ces deux dernières années. Message reçu fort et clair, n'en doutons pas !

L’indépendance stratégique revêt toujours au moins deux visages en définitive : économique et technologique. Et cette réalité, pour la première fois, n’est plus réservée aux seuls États. **L’émergence de mastodontes du numérique américains – GAFAM en tête – mais aussi des nouveaux acteurs d’influences délétères non étatiques (entreprises, ONG, groupes d’influence, mouvements de pression divers, etc.) bouleversent la donne ancrée dans nos mœurs depuis le traité de Westphalie.** Car l’indépendance économique et technologique de nos nations concerne désormais toutes les parties prenantes en lice. Entreprises et organisations en tête. S’il fallait s’en convaincre sans conteste, notons que toutes ces structures sont des proies d’égal intérêt pour les cyberattaquants et les intelligences malveillantes à l’œuvre qui officient en coulisses (Etats belligérants, concurrents déloyaux, mafias, criminalité organisée, acteurs commandités, etc.). Et toutes doivent désormais réintégrer très concrètement à leur stratégie globale, cette vérité immuable qu’est la prédation humaine au sens girardien[5]. Dans la course mondiale irrémédiable et violente qui se joue entre belligérants mimétiques, nos organisations (publiques et privées) se doivent d’assimiler que **la maîtrise technologique constitue indéniablement la clef de voute pour qui souhaite véritablement détenir le pouvoir et s’en rendre maitre demain.**

C’est aussi cela la nouvelle donne technologique : une mise à l’horizontale des acteurs qui a abouti à un partage conjoint des responsabilités en matière d’appropriation des nouvelles technologies : **les acteurs publics sont désormais responsables de l’appropriation collective des enjeux technologiques, là où les acteurs privés sont de leur côté condamnés à innover pour survivre. Il est urgent que tous intègrent en leur sein la question de la souveraineté.** On le voit d’ailleurs à l’occasion des multiples attaques informatiques sur nos hôpitaux et leurs données de santé. Plus question de simplement digitaliser son business bien tranquillement comme

le voisin : **toutes les organisations doivent insuffler du sens et du cœur à leur perception générale de la situation délétère actuelle**, pour mieux s'approprier et habiter cette nouvelle réalité plus anxiogène. Et surtout mieux assurer leur développement dans ce contexte fratricide d'ingérences extérieures violentes et pernicieuses. Elles n'ont plus vraiment le choix d'ailleurs de s'aguerrir à la culture du combat. Car force est de constater que la technologie recouvre des réalités mêlées ou hybrides (sociales, éthique, réputationnelles et stratégiques) qui forgent leur identité, et qui se doivent d'être appréhendées sous ce prisme de la souveraineté et des luttes mimétiques violentes entre puissances. A l'heure de la prolifération des logiciels malveillants et des armes cyber telle que « Pegasus », mais également des fuites récurrentes et opportunes d'information en ligne sur les réseaux du Dark Web[6], ou de la recrudescence des cyber-risques hybrides[7], la prise de risques inconsidérés n'est plus de mise. Au risque (c'est le cas de le redire) de la totale perte de contrôle à terme.

***2/ On entend relativement peu parler du sujet de la Gouvernance des Identités et des Accès informatiques (GIA), qui semble capital aux yeux de l'un de nos précédents invités, Dimitri Nokovitch*. Le thème est-il selon vous injustement sous-exposé ?***

Il s'agit en effet d'un sujet d'intérêt prioritaire tout à fait sérieux, mettant au jour des vulnérabilités informatiques majeures et jusqu'alors mal comprises, ou très mal prises en considération dans les organisations. Si celles-ci ont depuis pris conscience pour certaines de l'importance de leur gestion des data sensibles, elles n'en mesurent pas forcément toute la valeur intrinsèque, les enjeux ni même les risques opérationnels, cyber et financiers qui leur sont liés. **En l'état, la gouvernance des identités, et des droits d'accès aux données s'impose donc comme une priorité absolue.** Nous nous devons de reconnaître à la donnée toute sa valeur inhérente, en l'abordant comme un véritable actif de

l’entreprise et non plus comme un simple sous-produit de l’activité. Et pour moult organisations, il s’agit là d’un changement radical de paradigme. Dès lors, il s’agit de maintenir la valeur de la donnée en la fiabilisant, en la sécurisant et en l’enrichissant. Pour y parvenir, elles doivent rendre cette data « auditable », au même titre que les autres actifs de l’organisation. Dans ces conditions, la mise en œuvre d’une véritable stratégie de gouvernance des données est plus que jamais une nécessité. Et sans traitement adéquat, les actions délétères et nuisibles sur les données pourraient très rapidement proliférer, compte tenu des visées intrusives de certains opérateurs internationaux indélicats, au prétexte (si l’on se réfère aux discours des commerciaux du segment) de « réduire les coûts opérationnels, de réduire les risques dans l’organisation tout en renforçant sa sécurité, d’améliorer la conformité et les performances d’audit, et d’offrir un accès rapide et efficace aux collaborateurs de l’entreprise ». Le discours marketing de ces firmes est rôdé comme vous le constatez.

***Votre précédent invité est en effet l’un des premiers spécialistes à avoir mis en évidence cette menace fondamentale qui pèse sur la pérennité de nos entreprises.** Il fait justement partie de ces entrepreneurs précurseurs qui, grâce à leur maitrise de l’IA[8], permettent aux entreprises de protéger leurs données vitales ou essentielles (les fichiers clients, les documents stratégiques, les contrats, les brevets, les plans, les clefs de chiffrement, etc.). Suite à son observance attentive des effets funestes de la prédation économique qui ont durement impacté les actifs de la France ces dix dernières années (ainsi que ses grandes entreprises telles que Technip, Alcatel, BNP Paribas ou Alstom), s’est faite jour une nouvelle dimension qu’il nomme aujourd’hui « la gouvernance des accès aux secrets ». Celle-ci est au centre des opérations informatiques, sécurisant les identités numériques pour tous les utilisateurs, applications et données. Très schématiquement, elle permet en outre aux entreprises de

fournir un droit accès automatisé à un nombre toujours croissant d'actifs technologiques à certains personnels qualifiés. Tout en gérant les risques potentiels de sécurité et de conformité. Grâce à son expertise, votre invité est en capacité de répondre en outre à la question fondamentale : « qui doit avoir accès à quoi ? », et propose aux entreprises un dispositif qui leur permet d'identifier rapidement très en amont, ce qui est vraiment au cœur même de leur existence : dissimulé le plus souvent sous des montagnes de données non structurées, qui sont le plus souvent impossibles à traiter efficacement par le truchements d'une simple équipe de collaborateurs dédiés, ou même par la mise en œuvre d'une IA basique.

Dans une logique de prévention, il se propose donc d'identifier et de scanner toutes les personnes-clés de l'organisation, leurs localisations géographiques, leurs relations de travail et leurs accès aux secrets avant même que ne survienne un vol ou un méga-vol de données sensibles, grâce à un outil de recherche automatisée dédié. Pour de très grands opérateurs dont nous tiendront secret l'identité, un vol de données entraine en moyenne 280 jours de localisation et de traitement, ainsi qu'une perte de plus de 4 millions d'euros. « Aujourd'hui, grâce à notre expertise, on a été en mesure d'identifier près de 19 secrets, 375 dépositaires parmi des dizaines de millions de chemins d'accès » indiquait Dimitri Nokovitch dans une récente interview. L'affaire est donc très sérieuse, et même vitale dans de nombreux cas. C'est un fait. En conclusion de votre deuxième question, et dans un monde où les données sont omniprésentes, les entreprises de tout secteur sont appelées à devenir des entreprises de données. Et leurs volumes de data continuent d'exploser avec l'essor ininterrompu des nouvelles technologies. Ces données proviennent notamment des objets connectés, des systèmes d'information, des automates des usines ou encore des capteurs installés dans nos automobiles. Les entreprises sont donc toutes créatrices de data. Pour elles, la difficulté réside

dans le traitement de ces données massives et hétérogènes. Pour exprimer tout son potentiel au service des métiers, la data doit être parfaitement fiable et de qualité. C'est bien là le grand défi actuel : la gouvernance de la donnée[9].

### *3/ Les pouvoirs publics ont récemment haussé le ton sur la question du risque de prédation de nos entreprises stratégiques par des puissances étrangères. Le dispositif actuel vous semble-t-il de nature à nous mettre à l'abri ?*

Rien n'est jamais parfait en la matière et de nombreux trous dans la raquette demeurent, sans doute pour des questions d'idéologies ou de posture héritée dont nos personnels politiques ont définitivement le secret. Nombreux ont décidément du mal à s'en départir. Cette schizophrénie patente interroge pour le moins nos compatriotes et nos élus. Quand certains tirent la couverture à eux dans le sens de nos intérêts stratégiques, d'autres la retiennent « en même temps » dans le sens opposé… Vous noterez l'ironie de mes propos.

A les entendre[10], la France serait donc mieux armée aujourd'hui qu'elle ne l'était il y a quelques années encore ? Pour l'actuel patron du SISSE (créé en 2018 pour mieux armer le ministère de l'économie en matière d'intelligence économique), la politique de sécurité économique « donne des résultats, même s'ils sont souvent confidentiels naturellement, discrets par construction parce que nous ne pouvons pas faire cocorico ». Ces victoires de l'ombre se doivent donc de rester discrètes, même si certaines d'entre elles ont squatté longtemps la une des médias à l'image de celle de « Photonis » arrachée semble-t-il aux forceps à l'adversité. Mais pour combien de joyaux de la couronne happés discrètement en parallèle – dans le même temps – et en toute discrétion ? La question de la loyauté et de la corruption se poserait selon certains parlementaires avisés. **L'ancien ministre de l'économie Arnaud Montebourg ne s'en cache pas, tout comme le député LR Olivier Marleix qui évoque même un**

**pacte de corruption au sommet de l'Etat dans le cadre de l'affaire Alstom.** En 2019, Olivier Marleix avait d'ailleurs saisi le parquet à l'issue de sa commission d'enquête, demandant instamment au procureur de Paris d'enquêter sur l'affaire Alstom-GE et sur le rôle alors joué dans ce dossier par Emmanuel Macron. Le PNF s'est ensuite saisi de l'affaire.

En l'état, le SISSE traite chaque année « plusieurs dizaines de cas de dossiers où la politique de sécurité économique permet de bloquer des menaces ». A ce titre, « des rachats d'entreprises peuvent être effectivement bloqués pour des raisons de souveraineté, ou des rachats d'entreprises peuvent être aussi encadrés de manière stricte lorsqu'il le faut pour assurer le maintien de la propriété intellectuelle en France, même si l'entreprise passe sous capitaux étrangers ». Le SISSE est également « très vigilant sur certains partenariats de recherche dans des écosystèmes de recherche sensibles qui nous conduisent à dire non à un certain nombre de partenariats qui nous semblent problématiques pour la souveraineté ». En outre, la menace peut surgir tous azimuts, y compris dans les organismes de recherche particulièrement ciblés par des concurrents étrangers. Pour reprendre à notre compte une phrase lue dans la presse spécialisée, « **c'est une guerre qui ne fait pas de morts, qui se joue à bas bruit mais qui peut laisser un pays en état de friche sur le plan économique** ». Une guerre très discrète, qui se joue parfois au plus haut niveau de l'État, et bien souvent en dessous du système de détection radar de nos attentions collectives… Joffrey Célestin-Urbain du service de l'information stratégique et de la sécurité économiques, avait fait état fin mai 2021 – lors d'une audition par la délégation sénatoriale aux entreprises – d'une forme de résurgence des rapports de force entre les grandes zones économiques. Une lucidité et une reconnaissance bien tardive pour les plus avertis.

**Résultat, la France et l'Europe sont entrées de plain-pied dans une guerre économique portée par des dynamiques de long**

**terme avec le reste du monde, y compris avec ses grands alliés que sont parfois les Etats-Unis d'Amérique.** Un état de fait – qui demeure indéniablement tabou – bien antérieur à ce constat passablement tardif de nos autorités noterait les spécialistes du domaine les plus réprobateurs. Notons au passage que pour l'un des précédents titulaires du poste, Jean-Baptiste Carpentier, premier commissaire à l'information stratégique et à la sécurité économiques en date – et dont l'action ne s'est visiblement jamais inscrite dans le prisme de la guerre économique –, « la guerre économique n'existe pas… seule prévaut la coopétition »[11] (sic). Dans son intervention qui clôturait un colloque organisé en mars 2016 par le SYNFIE, cet inspecteur des finances censé pourtant aider notre République à mieux discerner les enjeux de luttes informationnelles dans les rapports de force économiques fratricides entre puissances – par ailleurs ancien alumni des programmes de visiteurs internationaux IVLP entièrement financés par le Departement d'Etat Américain – « avait fait surtout la démonstration de sa suffisance » (sic) selon les rapporteurs atterrés du portail de l'Ecole de Guerre Economique (EGE).

Que penser de ce changement de cap radical dans la perception de la menace, de nos actuels hauts fonctionnaires en charge ? Et pourquoi maintenant ? La réponse laisse songeur. **Le SISSE n'avait « pas vraiment vu jusqu'à présent » cette deuxième vague** car, « finalement, avec la crise sanitaire, tous les grands pays, tous les grands concurrents économiques avaient été touchés de manière plus ou moins symétrique ». Ce ne serait plus le cas désormais. Mais « avec le décollage peut être plus rapide de certaines zones économiques, la fragilité relative de nos entreprises commence à donner lieu à des tentatives de prédation », nous explique Joffrey Célestin-Urbain à l'occasion d'une interview. « Notre rôle au SISSE est de détecter le plus tôt possible des signaux d'alertes, y compris des signaux faibles de menaces étrangères sur des actifs stratégiques, de les collecter et d'en assurer le traitement systématique pour faire en sorte que chacune soit

traitée efficacement quand les intérêts souverains sont à risques. Ces menaces étrangères doivent être neutralisées ». Mieux vaut tard que jamais.

En 2020 par exemple, les services de Bercy avaient identifié 270 alertes qualifiées concernant des menaces de prédation sur des entreprises stratégiques entre janvier et octobre 2020. La plupart concernaient des PME. La crise sanitaire a encore renforcé ces menaces étrangères sur les entreprises françaises. Le ministère de l'Economie avait constaté une hausse nette du nombre d'alertes reçues rien qu'entre le premier et le deuxième trimestre 2020. En septembre de cette même année, l'Etat avait contrecarré la tentative de rachat de la PME Photonis par l'américain Teledyne. Mais Photonis n'est pas la seule entreprise stratégique surveillée étroitement par l'Etat.

En fragilisant le tissu économique, la crise du Covid a nettement augmenté les risques pour les entreprises françaises. Selon Bercy, le nombre d'alertes reçues avaient doublé entre le premier et le deuxième trimestre 2020. La plupart des cas concernaient des tentatives de rachats par des entreprises extra-européennes. Mais la prédation peut aussi prendre la forme d'accords commerciaux pouvant aboutir à des transferts de technologie à l'étranger – ou des attaques informatiques non crapuleuses – dans le but de soutirer des informations à haute valeur ajoutée. Autre configuration possible dans le registre de la pression : l'ouverture de contentieux visant à affaiblir une entreprise cible pour mieux la ravir. Certaines tentatives de rachats ont été également contrecarrées en trouvant in extrémis un repreneur français ou européen, ou en apportant un financement en capital via notamment la Banque Publique d'Investissement Bpifrance. Le seuil de contrôle des investissements étrangers en France à partir duquel les acquisitions dans les secteurs stratégiques, sont soumises à autorisation de l'Etat. Aussi, celui-ci a été abaissé pendant la crise de 25 % à 10 % du seuil de détention.

Le champ a aussi été étendu aux Biotech, alors que la santé fait partie des secteurs avec l'électronique dans lesquels plusieurs alertes d'importance sont remontées en 2020. En conclusion, le dispositif actuel est une première étape en la matière, mais demeure grandement perfectible sous le prisme de la sécurité nationale, et pas uniquement celui de la défense de nos seuls intérêts économiques. La sécurité Nationale, cette politique publique qui peine encore étrangement à trouver son plein emploi en France… **Rappelons pour mémoire que la « politique de sécurité nationale » ou « stratégie de sécurité nationale » est une politique publique qui consiste en la définition des objectifs à atteindre, des moyens à mettre en œuvre et des ressources à mobiliser par un État pour protéger sa population, son territoire et ses intérêts vitaux.** Elle est transverse aux grandes fonctions ministérielles traditionnelles des États comme la défense, la politique étrangère ou la sécurité intérieure en ce qu'elle appréhende dans une vision d'ensemble les menaces et les risques qui pèsent sur la sécurité nationale et auxquels les réponses, souvent multifonctionnelles, requièrent la mise en œuvre de politiques interministérielles cohérentes et coordonnées.

Pour conclure, et au moment où nous clôturons cette interview, la vente à l'américain Heico de la pépite électronique française Exxelia, qui équipe notamment le Rafale, les sous-marins français, l'A320 et même le F-35, provoque de nombreux remous. La DGA assure refaire le tour des investisseurs français pour tenter de trouver une solution tricolore. Exxelia : vers une nouvelle affaire Photonis titre le magazine Challenge début octobre ? Affaire à suivre très prochainement donc.

### *4/ Que vous inspire le concept de « souveraineté personnelle » promu par les tenants du web3 ?*

Ce concept d'apparence fumeuse – eu égard l'énergie qu'il faudrait dépenser pour que tout cela marche en temps réel, et sans rupture de signal – induit que le Web3 permettrait aux

individus de contrôler leur identité et leurs données biométriques dans les futurs métaverses (mondes virtuels allant au-delà du monde réel). Doux rêve ?

Attaquer l'identité personnelle d'un individu dans le monde réel demeure coûteux en matière de temps, de ressources et de conséquences potentielles. Mais cela est totalement possible. Dans le contexte de l'internet actuel, le ticket d'entrée à l'usurpation d'identité pour les pirates a été considérablement abaissé ces deux dernières années. Et des millions de personnes sont donc victimes de ces attaques chaque année. **L'utilisation d'outils Web3, notamment les NFT et les blockchain[1][2] (technologie qui permet de garder la trace d'un ensemble de transactions, de manière décentralisée, sécurisée et transparente, sous forme d'une chaîne de blocs), pour garantir la souveraineté des données des individus dans le métaverse est d'une importance capitale, car les détails profondément personnels inhérents à ces données créent de nouvelles opportunités pour les acteurs malveillants d'usurper l'identité des individus, afin de les exploiter allègrement.** Ces risques seraient naturellement amplifiés dans le métaverse. Si un pirate peut faire dire ou faire faire n'importe quoi à votre avatar numérique « photo réaliste », et que les autres utilisateurs soient incapables de déterminer s'il s'agit véritablement de vous ou non, il devient beaucoup plus difficile de lutter contre la fraude et l'usurpation d'identité, mais aussi de créer un « écosystème de confiance », essentiels à la bonne marche des communautés. Le métaverse ouvrirait, certes, de nouvelles possibilités de travailler et de jouer dans des espaces virtuels dédiés, mais ceci ne pourrait se faire que si l'on modifie corrélativement la façon dont les données sont échangées et protégées en ligne. Il est essentiel de créer des systèmes qui permettent de garantir aux individus le contrôle de leurs données biométriques. Ce qui n'est déjà pas une mince affaire sur le web 2.0 pourrait devenir dantesque dans les futurs métaverses s'ils venaient à se concrétiser un jour.

### *5/ Quels sont les enjeux du développement massif de l'IOT en termes de cybersécurité ?*

La question est très vaste et ne saurait se résoudre en quelques lignes seulement. Car incidemment, ces enjeux sont de taille. **75 milliards d'appareils seront en ligne en 2035, et selon l'une des dernières enquêtes GALLUP datant de 2020, « les utilisateurs mobiles, en moyenne, passent environ 80 % de leur temps en dehors du réseau protégé de l'entreprise, accédant à Internet à partir d'endroits autres que le bureau ou l'entreprise.** » L'Internet des Objets ou « IoT » désigne l'ensemble des objets physiques ayant la capacité de se connecter à Internet. On retrouve dans cette liste, qui ne cesse de s'allonger, les assistants personnels (Google Home par exemple). Les jouets pour enfants connectés. Les caméras de surveillance. Les ampoules, capteurs, volets, stores, portails, interrupteurs et prises connectées faisant partie de la Maison Intelligente. Les balances connectées, les montres connectées, et autres « Smart Watches » et « Smart Bands » pour suivre l'état de santé de son utilisateur. Les lave-vaisselle, fours, et certains réfrigérateurs dits « intelligents » (capables de commander les produits manquants automatiquement en analysant leurs contenus).

Ces nouveaux objets envahissent littéralement nos espaces personnels, notre vie privée et deviennent non seulement une menace pour chacun de nous mais aussi une menace incidente pour nos entreprises. Car les limites entre nos foyers et nos entreprises sont souvent floues et s'amenuisent constamment. Le recours au télétravail n'ayant rien arrangé dans cette affaire. Après tout, qui penserait que sa montre pourrait être une voie d'accès dérobée vers le réseau interne de l'entreprise ? Et pourtant les menaces ciblant les appareils « intelligents » connectés à Internet commencent à se multiplier et demeurent vulnérables. Par ailleurs, cette multiplication du nombre d'objets personnels connectés, et la très forte concurrence entraîne les industries dans une course folle, contre la montre. Et cette course se fait souvent au détriment

des aspects sécuritaires. Globalement, les menaces liées aux IOT deviennent une cible de choix pour les cybercriminels. Ces derniers ont très bien compris que pour accéder à l'ensemble du réseau d'une entreprise, il n'y a qu'à s'introduire sur un de ces appareils non protégés utilisés par un collaborateur. Or, les menaces sont multiples et peuvent impacter aussi bien le grand public que les secteurs professionnels et industriels en lice. Une explosion des menaces aux conséquences potentiellement dévastatrices.

De nombreux fabricants utilisent à ce titre un seul jeu de données de connexion par défaut pour tous leurs appareils. Au lieu de générer un jeu de connexion aléatoire par produit conçu. Ce type de méthode est visiblement favorable à la création massive, et à moindre coût. Mais elle fait aussi l'impasse à peu de frais sur le volet sécurité. Laissant ainsi une porte d'entrée béante aux attaques informatiques de tous poils et surtout, permet une explosion des menaces aux conséquences potentiellement dévastatrices. En 2019, plus de 2,4 millions de données client ont été exposées sur Internet suite à une erreur de configuration. L'entreprise américaine incriminée, Wyze, est spécialisée dans les caméras IP de surveillance et les produits pour la maison intelligente. Selon une étude de SonicWall, expert en solutions de cybersécurité, une augmentation de 30% du nombre d'attaque par malware visant l'IoT a été constatée en 2020 pendant la crise sanitaire de la COVID-19. Par ailleurs, le risque d'indisponibilité des services Cloud devient de plus en plus critique. Il menace la sécurité de ces objets connectés. A mesure que l'IoT évolue, l'utilisation du Cloud comme solution d'hébergement, de traitement, d'échange et de stockage des données se multiplie. Une quelconque indisponibilité de ces plateformes se traduit par un arrêt ou un dysfonctionnement des équipements IoT qui en dépendent. Dans le secteur de la santé par exemple, l'IoT est utilisé massivement pour surveiller l'état des patients et fournir de nombreuses informations. Une défaillance de ces équipements pourrait

avoir des conséquences irréversibles sur la santé du patient. Et **la divulgation de données médicales pourrait être catastrophique, à la fois pour l'institution médicale et le patient lui-même.** Ces équipements, lorsqu'ils sont mal protégés, peuvent donner accès au système informatique d'établissements de santé comme dernièrement l'hôpital de Corbeil en Essonne. Fin 2020, une machine à laver connectée avait aussi été piratée, et avait donné accès au système informatique d'un autre hôpital français bien connu. L'établissement de santé a ensuite subi une attaque de type rançongiciel, bloquant tout l'établissement. Dans l'automobile, une défaillance au niveau des équipements IoT, responsables de l'identification d'obstacles sur la voie publique pour les voitures autonomes pourrait générer des accidents de la route et mettre en péril la vie des passagers et des usagers de la chaussée. De nombreux problèmes de sécurité se cachent derrière l'usage et la présence des objets connectés dans notre environnement quotidien. Des jouets pour enfants piratés, des montres fitness desquelles il est possible de récupérer les mails, les SMS, etc. C'est l'utilisation de ce type de montres connectées qui a en outre permis l'identification d'une base secrète militaire américaine, à partir de traces GPS liées aux parcours sportifs des militaires présents sur la base. Il en fut de même en France avec la reconstitution du parcours de deux joggers, appartenant à une centrale de renseignement. Prenant conscience des menaces et des conséquences que l'IoT peut engendrer, beaucoup s'interrogent désormais sur la nécessité de définir et d'imposer des mesures de sécurité et des normes strictes. Elles permettraient naturellement de mieux encadrer la conception et l'utilisation des objets connectés. Ceci afin de diminuer les scénarios d'attaque tirant profit de la faiblesse des systèmes ces équipements. Les membres de la Commission européenne ont récemment proposés aux membres du Parlement européen de voter un nouveau règlement qui couvre les « objets connectés comportant des éléments numériques, définis comme logiciel ou matériel, ainsi que les solutions de

traitement de données à distance »[13]. L'objectif est clair : renforcer le niveau de sécurité des objectifs connectés. Après son vote, les fabricants de produits IoT devront donc se conformer aux nouvelles exigences européennes en matière de conception, de développement et de production avant le lancement d'un appareil sur le marché, au risque de se voir infliger de lourdes sanctions en cas de manquement. Selon le cadre réglementaire proposé, les objets connectés doivent « garantir la confidentialité des données », notamment en utilisant le chiffrement, en protégeant leur intégrité et en ne traitant que les données strictement nécessaires à leur fonctionnement. La Commission souhaite également établir une liste des produits critiques présentant un risque plus élevé. Ces objets connectés seront divisés en deux classes, avec un processus spécifique d'évaluation de la conformité pour chacune des classes. Les entreprises concernées devront obtenir des certificats obligatoires attestant qu'elles répondent aux nouvelles exigences européennes en matière de cybersécurité. Selon le texte, celles qui ne respecteront pas le règlement seront « passibles d'une amende pouvant atteindre 15 millions d'euros ou 2,5 % du chiffre d'affaires mondial de l'année précédente ».

### *6/ Que pensez-vous de la fin programmée de l'argent liquide ?*

L'argent liquide disparaitra assurément un jour ou l'autre, cela tombe sous le sens, mais cependant pas maintenant. Et si l'on peut envisager sa disparition prochaine (tout comme la création concomitante de nouvelles infrastructures de paiement technologiques privées, identiques en cela à « Libra », cette cryptomonnaie que voulait initialement lancer la multinationale californienne Facebook / Méta), n'oublions pas toutefois que la monnaie demeure avant toute chose une construction sociale. Je n'ai qu'à citer la quatrième de couverture de l'un de mes ouvrages préférés datant de 1982, pour mieux le faire comprendre : « la violence de la monnaie » des économistes français Michel Aglietta, André Orléan. De

quoi retourne-t-il au fond, quand on parle de monnaie selon nos deux auteurs ? La réponse est éclairante : « Prendre au sérieux la monnaie, oblige à un déplacement radical de perspective. Il faut revenir sur les fondements des sociétés marchandes, et reconnaître que la compatibilité des intérêts individuels ne peut résulter du seul jeu du marché. Dans les sociétés dominées par le désir d'accaparer, et fascinées par l'imitation, la cohésion passe par des modes de socialisation spécifiques. Dans cette approche, la monnaie révèle sa réalité ambivalente, indissolublement principe de normalisation des comportements et arme des conflits privés pour l'appropriation des richesses ; à la fois bien social se pliant aux contraintes de la gestion étatique et lieu d'affrontement et de fractionnement entre groupes rivaux. L'ordre monétaire, les crises qui l'ébranlent, les transformations des systèmes monétaires, les compromis noués par la politique monétaire, sont analysés dans le prisme des configurations dessinées par la coexistence de ces forces, qui homogénéisent et morcellent le champ social. » Il s'agit, autrement dit, d'un mode provisoire de pacification des relations violentes entre sujets humains, qui demeurent potentiellement fatales à l'ordre social lui-même… En définitive, la monnaie « contient » en quelque sorte cette humaine violence, dans les deux sens du terme : en cela qu'elle l'empêche (elle lui fait barrage si les transactions monétaires se passent bien), et qu'elle l'inclut en elles, eu égard pour les rivalités humaines toujours engendrées par des velléités violentes de chacun pour s'en rendre maitre… **La monnaie serait en quelque sorte cette réification de la figure du pharmakós (en Grec ancien φαρμακός), très semblable à celle du bouc émissaire : « celui qu'on immole en expiation des fautes d'un autre** ». En d'autres termes, la victime émissaire expiatoire (symbolique dans le cas de la monnaie), dans un rite de purification très largement utilisé dans les sociétés primitives et dans la Grèce antique. Mais si le rite de purification échouait, et ne parvenait pas à purger les velléités envieuses et mimétiques de tous les convives présents, la violence refaisait irruption

dans le social de manière tout à fait concrète cette fois.

Concernant l'euro, le nombre de billets en circulation a doublé depuis son lancement en 2002 et s'élèverait aujourd'hui à 10 % de la masse monétaire. Cela s'expliquerait notamment par le fait que les dollars et les euros en billets sont utilisés dans beaucoup de pays en développement dont ce n'est évidemment pas la monnaie officielle. Cité dans un article du Monde par la professeure d'économie Olena Havrylchyk, « The Curse of Cash »[14], l'économiste américain Kenneth Rogoff déploie un plaidoyer contre l'argent liquide cash qui favoriserai selon lui l'évasion fiscale et la criminalité grâce à l'anonymat généré. Les sondages montrent par exemple qu'en Suède, la baisse de l'argent liquide y est très négativement perçue par l'ensemble des personnes âgées du pays, mais également par les populations rurales. A cet effet, les autorités du pays ont rapidement réagi, obligeant la banque centrale de Suède ainsi que les banques privées, à fournir une infrastructure adéquat pour permettre aux habitants d'accéder à de l'argent liquide. En parallèle de la baisse de l'argent liquide sont apparues les cryptomonnaies. Le bitcoin avait été créé en 2009, mais il en existe naturellement plusieurs dizaines d'autres à travers le monde. Sont-elles pour autant l'avenir de la monnaie, ou plus simplement d'étranges objets sujets aux bulles spéculatives ? De même que la monnaie, comme nous l'évoquions déjà plus haut, les cryptomonnaies sont également des constructions sociales elles aussi. La domination du bitcoin sur ce marché n'est pas due à sa technologie plus avancée, bien au contraire, mais exclusivement à sa force narrative et à sa communauté. Le bitcoin a permis la création d'une infrastructure de paiement sans « tiers de confiance ». Le rôle qui est traditionnellement dévolu aux banques, ou à des opérateurs comme PayPal ou Visa. Intellectuellement, la solution proposée est fascinante mais, en pratique, l'absence d'un tiers de confiance impose bien entendu des limites techniques au dispositif : une transaction sur la blockchain est extrêmement

énergivore et consomme autant d'électricité que le chauffage d'un seul appartement pendant un mois d'hiver. En période de restrictions électriques drastiques, cela pourrait interroger le pecus vulgum sur le bienfondé de l'affaire… Dans le cadre de ses expérimentations de monnaie numérique, la banque centrale européenne a récemment désigné cinq entreprises pour réaliser des prototypes d'interface utilisateur, afin de simuler des transactions. Parmi elles, le français Worldline mais aussi plus surprenant, la multinationale Amazon, seul acteur non européen de la liste… La Banque centrale européenne (BCE) demeure un petit peu plus avancée que les Etats-Unis en matière de création d'euro numérique, grâce à son projet pilote de deux ans lancé à l'été 2021. L'effort, comparable à celui de la Chine et son e-yuan, vise à répondre aux besoins des Européens tout en s'imposant comme un acteur plus fiable que les marchands décentralisés. Les freins au développement d'une monnaie commune numérique restent nombreux. Demeurent des problèmes de conception et de distribution afin de protéger le secret des transactions. C'est dans cette optique que la BCE s'est récemment rapprochée de ces cinq entreprises afin d'effectuer des simulations de transaction. Les compagnies ont été choisies parmi un groupe de 54 fournisseurs « front-end » : la banque CaixaBank fera office de prototype pour les paiements en ligne peer-to-peer ; la multinationale française Worldline servira sur les peer-to-peer hors ligne ; le consortium European Payment Initiative, qui regroupe 31 institutions bancaires et financières travaillant sur une solution de paiement paneuropéenne, et qui sera en charge des paiements en point de vente initiés par le payeur. Et enfin, l'entreprise italienne spécialisée dans les paiements électroniques Nexi, spécialiste des paiements électroniques, fera la même chose mais pour les paiements initiés par le commerçant. Ces travaux de prototypage s'intègrent au projet pilote et dont les conclusions seront rendues au premier trimestre 2023.

### *7/ La NSA a récemment juré qu'il n'y aurait pas de « backdoor » dans la prochaine génération des standards cryptographiques : que doit-on en penser ?*

Cela retournerait presque de la boutade entre spécialistes. Une question se pose cependant : faut-il toujours croire ce que jure la NSA au regard de sa mission prioritaire : la préservation absolue des conditions de la sécurité nationale des Etats-Unis ? Blague à part, il est bien entendu impossible de vérifier l'exactitude de cette affirmation. Outre les centrales spécialisées, il n'existe aucun moyen concret de savoir si l'agence américaine mettra en œuvre des actions particulières pour contourner ces protections. Sauf à attendre peut-être un jour l'improbable défection d'un nouvel objecteur de conscience au sein même de ces dispositifs couverts par le secret. Gageons que la « dénégation plausible » serait alors mise en œuvre dans ce cas par les autorités, et un pare-feu sémantique efficace déployé corrélativement si des divulgations intempestives intervenaient à ce titre dans les prochaines années. N'en doutons pas un instant.

Depuis les révélations de 2013, les capacités de la NSA ont nécessairement évolué dans des proportions faramineuses eu égard son budget de fonctionnent annuel, mais sous le sceau du secret. Ses moyens n'ont sans doute plus rien à voir avec ce qui était connu ou décrit dans les documents extraits frauduleusement par le traitre Snowden. Dans ce domaine, le paramètre essentiel est donc la « vérifiabilité » des propos tenus. Il s'avère que **le futur algorithme qui sera retenu par le NIST (*National Institute of Standards and Technology)* sera ouvert à un examen international, afin de permettre à tout le monde de déceler de possibles faiblesses ou défauts. Cela sera-t-il suffisant pour dissiper les craintes légitimes en la matière ? Rendez-vous en 2024, date à laquelle l'algorithme devrait être opérationnel…**

Pour mémoire, rappelons que l'affaire dite « Snowden » avait exposé les machinations de cette centrale américaine,

notamment en matière de chiffrement. Le soupçon plane toujours en l'état, et sans doute pour très longtemps encore. Y compris sur la nature des contributions de la NSA dans le domaine de la cryptographie. Une déclaration du directeur en personne de la cybersécurité au sein de l'agence, à Bloomberg le 13 mai dernier n'est pas forcément de nature à lever les doutes. Si la mission première de la NSA est d'assurer la sécurité nationale des Etats-Unis contre toutes formes de menaces informatiques et d'ingérences, elle a aussi tout un volet d'actions spéciales parfaitement secrètes en matière de renseignement dans le spectre électromagnétique, ainsi que la faculté de mener des actions offensives ou subversives en matière cyber, en vertu de la législation spéciale sur la sécurité Nationale. Nous savons justement (entre autre chose, grâce aux documents secrets divulgués par Snowden) que la NSA a été mise en cause pour avoir cherché à mettre en place des stratagèmes afin d'amoindrir un standard cryptographique solide. L'altération ciblait le générateur de nombres pseudo-aléatoires « Dual Elliptic Curve Deterministic Random Bit Generator ».

Dès lors, il apparaissait clairement à tous que l'objectif de la NSA en la matière (qui s'est penchée sur ce générateur dès le milieu des années 2000), était en réalité de pouvoir prédire les nombres générés aléatoirement, et ainsi avoir une capacité secrète, le moment venu, de déchiffrement. En bout de course, il s'est avéré que la NSA a été seule aux commandes pour fixer le fonctionnement de Dual_EC_DRBG. Outre-Atlantique, l'affaire avait fait très grand bruit à l'époque et avait, de plus, indéniablement éclaboussé la réputation de l'institut national des normes et de la technologie (NIST). L'organisme en charge de valider justement de nouvelles normes cryptographiques… S'était même posé la question de mise à l'écart de la NSA, concernant la conception des normes de chiffrement. La robustesse de la prochaine norme est donc un enjeu stratégique majeur et hautement critique pour les Etats-Unis. C'est sur elle en définitive que va reposer pour la

prochaine décennie, une large part de l'écosystème informatique, mais aussi la sûreté des communications des gouvernements. Celui des États-Unis en tête – bien entendu – qui a aussi besoin de ces outils pour sécuriser ses propres liaisons, mais également pour tout connaitre des liaisons d'autrui… La pérennité du Grand Jeu en somme.

### *8/ Quel conseil donneriez-vous aux entreprises françaises qui souhaitent s'implanter en Chine ou aux Etats-Unis ?*

La question recoupe naturellement des espaces textuels très vastes de réponses possibles, dont nous ne disposons pas ici, au risque de perdre nos lecteurs dans le méandre des options.

Je vais donc me limiter aux conseils d'usage et de bons sens en la matière. Ils seront forcements très incomplets et quelque peu caricaturaux. Exporter son activité ou sa production aux Etats-Unis ou en Chine pour se lancer est une idée que de très nombreux entrepreneurs français ont eu un jour ou l'autre. Tous attirés par un marché potentiel de plus de 300 millions de consommateurs d'un côté, et de plus de 1,4 milliard de l'autre. Pour se lancer, il faut impérativement avoir des idées claires, s'y préparer très longtemps à l'avance. Mais surtout, savoir ce qui change véritablement de l'autre côté de l'océan pour un dirigeant d'entreprise ou un entrepreneur qui ose s'y risquer. Mais est-ce le moment véritablement idéal pour s'implanter aux États-Unis ou en Chine ? Et cela, compte tenu de la chape d'incertitudes actuelles en matière de commerce international et de stabilité géopolitique ? La question se pose. Par exemple, aux Etats-Unis, les décisions se prennent bien plus rapidement qu'en France, les salariés sont bien moins fidèles, les impôts personnels et sur les sociétés ne sont pas nécessairement moins élevés et l'installation au Delaware ne vous épargnera pas forcément d'en payer…

Enfin, si les charges sociales sont souvent plus basses, pour

être attractif un employeur devra le plus souvent offrir à ses salariés des avantages ayant un coût certain comme la mutuelle ou le plan de retraite notamment. Une implantation aux Etats-Unis demande un minimum de deux années de préparation pour optimiser ses chances. Tout d'abord, il va falloir déterminer l'endroit où l'on souhaite s'implanter et qui variera en fonction de l'activité envisagée. Ce choix sera déterminant car il va conditionner à la fois la proximité avec les clients et avec les sources de financement. Technologies ? Historiquement, la Californie et plus spécifiquement San-Francisco. La finance ? Principalement New-York. Les biotech ? Il y a Boston par exemple. Le Luxe ? La Floride, très proche des marchés Sud-Américains. Le choix de l'implantation ne doit pas se faire en visant le plus économique, mais en ciblant bien au contraire les opportunités de développement. Ensuite, la préparation passe par la constitution d'emblée d'une très solide assise financière d'au moins une année de cash-flow d'avance. Celle-ci devant permettre d'absorber sereinement la première année sur le sol américain. Qu'il s'agisse de prendre un bail, de faire une acquisition ou de s'associer, les fonds devront être disponibles sans attendre. Les aides apportées par Business France ou la BPI, mais aussi les chambres de commerce franco-américaines locales peuvent aider l'entrepreneur – candidat à l'implantation. Enfin, la clef sera de constituer une équipe de direction biculturelle, franco-américaine, et donc de recruter au demeurant la ou les bonnes personnes. Sans cela, le risque est élevé de ne pas parvenir à s'interfacer parfaitement et dès le départ avec ses interlocuteurs locaux, qu'ils soient fournisseurs, salariés ou partenaires. Au Etats-Unis, le droit est omniprésent et sa maitrise indispensable. La différence culturelle s'applique également à l'environnement business, en commençant par le droit. Aux Etats-Unis, dans la plupart des cas, l'organisation des affaires ne repose pas sur des lois avant tout, mais bien sur des contrats. Il faut donc recourir aux services d'un avocat très régulièrement. Pour les baux quand on loue, pour les contrats de travail de ses employés clefs, pour les

contrats commerciaux avec ses partenaires, pour les questions d'immigration afin d'avoir le droit d'y travailler. Le budget juridique moyen pour une entreprise ayant ces différents besoins sera au moins trois fois supérieur à celui nécessaire pour la même activité en France.

En matière fiscale, jusqu'à trois niveaux d'imposition existent aux Etats-Unis pour l'impôt sur les sociétés. Au taux fédéral de 21%, il faut ajouter celui de l'Etat où l'entreprise est implantée ou active : par exemple 5,5% en Floride, 6,5% dans l'Etat de New-York et 8,84% en Californie. Mais il peut aussi arriver que la ville d'implantation impose également, comme à New-York, pour un taux supérieur à 8%. En matière de fiscalité personnelle, l'imposition sera fédérale et, souvent, par l'Etat de résidence, même si certains pratiquent la non-imposition comme en Floride. Par ailleurs, les rapports avec le fisc américain sont très différents de ceux que l'on peut entretenir avec l'administration fiscale française. En la matière, le droit à l'erreur n'existe pas… La plus grande prudence et la plus grande transparence s'imposent donc car toute omission sera interprétée comme un mensonge et sanctionnée en conséquence très lourdement. Il faudra par ailleurs avoir une vigilance particulière si jamais le dirigeant devenait résident américain… Et ceci, compte tenu des très lourdes obligations fiscales qui en découleraient. Dans tous les cas, il est nécessaire de recourir à un comptable, en vérifiant qu'il s'agit bien d'un CPA (certified public accountant), car l'accès à la profession est totalement libre.

Enfin, le financement de son activité est un sujet capital aux Etats-Unis. **Les banques américaines prêtent très difficilement aux entrepreneurs étrangers et leurs taux sont dès lors très élevés : entre 6 et 7% actuellement.** De leur côté, les banques françaises dont les taux sont bien plus avantageux, sont le plus souvent très frileuses et peu enclines à financer le développement de leurs clients aux Etats-Unis, qu'elles jugent

particulièrement risqué. Dès lors, la solution est de lever des fonds, en trouvant des associés américains, des personnes physiques, des entreprises ou des fonds d'investissement. Là encore, avoir une équipe biculturelle, capable de prendre des décisions rapidement sera pour le moins indispensable.

Quels sont les défis d'une implantation en Chine ? Que ce soit pour y créer une société pour y implanter un siège social, ou pour y installer un bureau de représentation ou un site de production, il est très important de suivre quelques étapes clés pour entreprendre sur place. Malgré les nombreux avantages d'une délocalisation en Chine ou d'une expansion de son activité sur le sol chinois, un tel projet présente un certain nombre de défis pour les entreprises étrangères. Il existe en effet de très nombreuses réglementations concernant l'implantation d'une société en Chine. Les conditions d'accès au marché chinois peuvent notamment varier en fonction des secteurs d'activité et des provinces considérées. D'autre part, de nombreux médias sociaux sont censurés, comme Twitter, Facebook, et YouTube, ce qui peut compliquer grandement la stratégie de communication, et nécessite de s'adapter aux outils et tendances locales en la matière… Il faut également savoir que la propriété intellectuelle fait très souvent l'objet de transgressions notables en Chine, d'où l'importance de protéger juridiquement son projet d'entreprise. En outre, la barrière linguistique et les différences culturelles peuvent constituer un très grand défi pour les étrangers. Les codes sociaux sont très ancrés, même dans le monde des affaires. Quelle que soit l'étape de votre implantation, il sera primordial de bien connaître et de respecter les codes culturels et les coutumes non écrites en vigueur dans le pays, et notamment dans la province et dans la ville concernée. La Chine regroupe en effet 7 langues différentes, de très nombreux dialectes et 56 nationalités. D'une région à l'autre, il existe de très fortes disparités entre les langues, les cultures, ainsi que les habitudes de consommation, besoins et attentes des consommateurs.

Le marché chinois est très complexe et extrêmement vaste. Une phase préalable essentielle dans un projet d'implantation est donc une étude de marché particulièrement détaillée. Celle-ci doit permettre d'analyser en profondeur l'offre, la demande, les opportunités, les forces et les faiblesses, les menaces, la concurrence, les besoins des consommateurs. Il faudra ensuite adapter son offre, son positionnement et sa stratégie de croissance en fonction de ces différents facteurs. Par ailleurs, il faut savoir que la Chine est très compétitive dans certains secteurs spécifiques, tels que : le secteur manufacturier, l'agriculture, le secteur minier, le secteur tertiaire, la Tech, la Fintech. C'est notamment un leader dans le e-commerce. Avec une superficie de 9,597 millions de km2, la Chine offre des opportunités d'implantation très diverses et variées. De nombreuses grandes villes, dynamiques, attractives et ouvertes sur le monde représentent des destinations privilégiées. C'est notamment le cas de Beijing, qui compte 20 millions d'habitants, de Shanghai, qui regroupe plus de 26 millions d'habitants, mais aussi de Shenzhen, Canton, Hong Kong, Wuhan… Le choix de la ville devra notamment se faire en fonction de votre domaine d'activité, et dépendra de l'offre et de la demande dans ce secteur au niveau local.

Bien que la Chine soit ouverte aux sociétés internationales, certains investissements sont particulièrement encouragés par le gouvernement, tandis que d'autres sont plus restreints. D'autres encore sont strictement interdits. Il faut pour cela consulter le catalogue des investissements étrangers, qui classe les secteurs en trois catégories distinctes : les secteurs d'investissements encouragés sont la santé, la culture, le travail social, les services techniques, le secteur financier, les transports. Les secteurs d'investissements restreints demeurent la création d'établissements d'enseignement supérieur, d'établissements hospitaliers, l'agriculture. Quant aux secteurs d'investissements interdits, ceux-ci recoupent la production et la diffusion de programmes télévisés, la vente de tabac, le

conseil légal sur les lois chinoises. Il est donc nécessaire de s'informer sur les obligations légales en vigueur pour les investisseurs étrangers et des démarches administratives propres à votre secteur d'activité, à la municipalité concernée, et au type de société créée.

Par ailleurs, les procédures pour enregistrer une entreprise en Chine sont assez fastidieuses et nécessitent de bien connaître les rouages de l'administration chinoise elle-même. Pour cela, il s'avère impératif de faire appel à un organisme spécialisé ou de trouver un partenaire local fiable pour se faire accompagner dans toutes ces démarches. Dans le cas de l'implantation d'une entreprise française en Chine, il est par exemple possible de s'adresser à Business France, ou à la CCI Franco-chinoise (Chambre de commerce et d'industrie, ou CCIFC), qui soutiennent les entrepreneurs dans leur projet d'implantation en Chine. Cela sera aussi très utile pour mieux comprendre la culture locale, de même que les spécificités et les exigences du marché chinois. Pour une implantation en Chine, plusieurs options sont possibles. Vous avez notamment le choix entre plusieurs structures juridiques. La première est un bureau de représentation : c'est l'option la plus simple, mais elle ne permet pas de réaliser une activité de vente ou d'achat en Chine. La deuxième recoupe les entreprises mixtes de capitaux (Equity joint venture, ou EJV), ou sa forme simplifiée, une entreprise mixte coopérative (Cooperative joint venture, ou CJV) : elles nécessitent de s'associer avec un partenaire local. C'est une structure naturellement très encouragée par le gouvernement, pour des raisons sous-jacentes que l'on comprendra aisément. L'entreprise à capitaux exclusivement étrangers (Wholly Foreign owned enterprise ou WFOE) permet, elle, de s'implanter en Chine sans avoir à passer par un investisseur local. Elle offre en outre beaucoup d'autonomie et de flexibilité au dirigeant. Au demeurant, chaque forme juridique fait l'objet d'un certain nombre de réglementations légales, de démarches administratives et de modalités de financement qui lui sont propres. Par ailleurs,

les activités autorisées peuvent varier en fonction du type de société créée. Il ne faudra donc pas négliger cette étape très importante, et veiller, là encore, à demander l'avis d'un professionnel aguerri. Comme nous le mentionnions plus haut, la Chine compte une grande diversité de langues. Le mandarin figure d'ailleurs parmi les langues les plus difficiles du monde. La barrière linguistique peut représenter un obstacle de taille lors d'une implantation en Chine. Pour simplifier les échanges avec les partenaires locaux, il sera donc impératif de faire appel aux services d'un traducteur, que ce soit pour réaliser des traductions assermentées pour des documents officiels et légaux lors de des démarches d'implantation, traduire les éléments de langage d'un site internet, et les documents marketing, commerciaux et institutionnels en chinois.

On le réalise aisément après ce très rapide descriptif, tout ceci pose naturellement de nombreuses questions de sécurité et de sureté spécifiques qui ne pourrons qu'avoir un impact notable sur la réussite du projet lui-même, et sur la réalité de la vie sur place du dirigeant et de ses équipes d'expatriés. La pérennité du projet entrepreneurial et de la sécurité de ses opérateurs est à ce prix.

### *9/ Nous avons désormais un ministre de la souveraineté numérique, qu'est-ce que cela change selon vous ?*

Que dire… La politisation des questions liées au numérique via le truchement de la souveraineté ne date pas d'hier. Ministère du numérique ou simple secrétariat d'Etat ? La question avait beaucoup agité l'écosystème de la Tech français, donnant lieu pendant le mandat précédent à d'intenses discussions parmi les spécialistes et les proches du pouvoir. Et parfois même, générant de franches oppositions à la création d'un tel ministère[15]. Cela avait aussi mobilisé, dans les colonnes de La Tribune ou des Echos, ceux qui estiment que **les enjeux de la révolution numérique sont trop importants pour être uniquement pilotés par un modeste secrétariat d'Etat, sans**

**véritable pouvoir.** J'en fus assurément.

Du côté de l'écosystème Tech et des défenseurs de la souveraineté numérique, la déception de n'avoir finalement pas obtenu satisfaction est toutefois partiellement atténuée par la prise en compte apparente de cet enjeu crucial par l'exécutif. Mais au vu des insuffisances patentes du premier quinquennat en la matière, la méfiance reste plus que jamais de mise dans le Landerneau des spécialistes et des sachants. Finalement, Emmanuel Macron a encore une fois tranché dans le « ni-ni » comme à son habitude : ce sera ni l'un, ni l'autre. Ou plutôt, ce sera les deux, « en même temps ». Le règne de l'oxymore présidentiel, toujours et encore…

**Déception notable donc : il n'y aura finalement pas réellement de ministère du numérique de plein exercice**, malgré les apparences. Le ministère de l'économie et des Finances se voit doter d'une dimension numérique par décret du 4 juillet 2022 relatif à la composition du gouvernement, et Bruno Le Maire s'est vu nommer ministre de l'Économie, des Finances et de la Souveraineté industrielle et numérique. Bon présage pour la suite ? Simple habillage de circonstance pour noyer le poisson ? Les avis sont tranchés.

Il ne faut, malgré tout, pas totalement sous-estimer l'importance symbolique de cette promotion du numérique à Bercy via cet appendice. En plaçant l'enjeu de la souveraineté numérique dans les prérogatives du ministre de l'Economie et des Finances, le gouvernement Borne reconnait à mi-mot pour la première fois que la thématique est éminemment politique, et que les choix de l'Etat sur ces sujets cruciaux s'inscrivent dans le cadre d'une politique économique globale plus vaste. C'est une prise en compte inédite, même si elle demeure ad-minima et très incomplète car réduite aux acquêts. En d'autres termes, aux seuls enjeux économiques de souveraineté, de la transversalité du numérique. Pour le co-rapporteur du rapport de référence sur la souveraineté numérique, l'excellent et très actif député Modem, Philippe Latombe : « le verre (est) à

moitié vide, est j'aurais préféré un vrai ministère du Numérique englobant la souveraineté, la cybersécurité, l'écosystème Tech et la réforme de l'Etat. Mais chaque chose en son temps ce qui se passe est déjà très positif », avait-il indiqué à La Tribune. De son côté, l'écosystème Tech – forcément déçu – préfère lui voir le verre à moitié plein, business oblige : « Le message envoyé est fort, va dans le bon sens et pourrait dynamiser les solutions françaises portées par les startups », analyse Maya Noël, la directrice de France Digitale.

Le scepticisme sur les hauts fonctionnaires décisionnaires de Bercy, et sur la stratégie de souveraineté proférée par Bruno Le Maire demeure donc prégnant en coulisses. Reste désormais le plus important : quelle sera véritablement la politique de la France en matière de souveraineté numérique, et cela bien au-delà des discours et des déclarations d'apparat ? Le maintien en poste du ministre en charge inquiète plus qu'il ne rassure forcément. « Le fait est que le terme souveraineté numérique soit entré dans le gouvernement est une victoire pour nos idées. Sur l'implémentation, je reste extrêmement prudent car Bruno Le Maire n'a pas montré sa capacité à écouter les acteurs de cet écosystème », estimait l'entrepreneur et proactif Tariq Krim. Si Bruno Le Maire est le choix de la continuité, dans les faits, le premier quinquennat d'Emmanuel Macron a été très nettement insuffisant, voire même très ambiguë dans ce domaine. Et notamment concernant le Cloud, qui est très schématiquement cette couche d'infrastructures logicielles sur laquelle repose toute l'économie numérique : et donc la mère de toutes des batailles autour de la souveraineté et de l'autonomie de nos dispositifs techniques. Or, la stratégie euphémique et parfois risible du « Cloud de confiance », pilotée par Bruno Le Maire et feu Cédric O, a tôt fait de faire la quasi-unanimité contre elle. Y compris au sein même de l'Etat, car elle ouvre toute grande – mais à bas bruit – la porte aux mastodontes américains du Cloud… Ce qui leur permet d'ores et déjà de

gagner de nouveaux marchés au sein des administrations publiques et des opérateurs d'importance vitale (OIV). Mais aussi des services essentiels (OSE) sans que cela ne semble gêner personne… Le ministre et ces conseillers ne sont pas les plus critiques vis-à-vis des GAFAM, et notamment vis-à-vis de l'Europe qui a très clairement reculé sur sa souveraineté numérique comme l'a démontré sans ambages le très récent et subreptice accord sur les transferts transatlantiques de nos données aux Etats-Unis. La politique qui sera réellement menée sera donc à déduire des hommes et des femmes choisies aux postes stratégiques de la Direction interministérielle du numérique – Dinum – et des secrétaires d'Etat qui incarneront ces sujets à Bercy. En l'état, je vous laisse juge… Une bonne due diligence a toujours l'avantage de pouvoir en connaitre sur les acteurs en présence et les parties prenantes en lice, bien au-delà des postures affichées. Et même quand on cherche à noyer le poisson par ailleurs, sous un tombereau de mièvreries sémantiques d'apparence flatteuse. Vous l'aurez compris, je ne suis pas du tout optimiste pour l'avenir tant il existe de trous dans notre raquette à très grosses mailles, et d'accointances à peine voilées de nos décideurs publics devenus éminemment réceptifs et poreux aux sirènes américaines. Et je ne parle même pas des actions de lobbying intensif des GAFAM et des centrales américaines au niveau des pouvoirs publics européens, pour que soient adoptées leurs technologies, et accueillis leurs champions nationaux à bras ouverts par les instances de Bruxelles. Selon moi et en l'état, la messe est dite. La situation internationale et le conflit ukrainien ne faisant qu'accélérer un peu plus ce processus inéluctable d'accaparement engagé.

### *10/ Pouvez-vous nous confier le nom de trois logiciels dont vous faites un usage quotidien, et pour quelles raisons ?*

**J'utilise naturellement OLVID**, une messagerie de chiffrement française qui n'est pas à proprement parler un « logiciel » mais une application de communication sécurisée. **ZBrush**, qui

est un logiciel de modélisation digitale pour la création de forme, et la réalisation d'impression 3D. J'utilise également quelques applications pour des investigations OSINT, mais je me repose pour l'essentiel sur ma perspicacité, et mes capacités de recherche et d'analyse, car je ne suis pas sujet au fétichisme technologique. Pour le reste, je garderai naturellement sans grande surprise mes usages personnels sous le sceau de la confidentialité.

**[1]** Le mème est « un élément de langage reconnaissable et transmis par répétition d'un individu à d'autres ». La définition que donne Richard Dawkins correspond à une « unité d'information contenue dans un cerveau, échangeable au sein d'une société ». Elle résulte d'une hypothèse selon laquelle les cultures évolueraient comme les êtres vivants, par variations et sélection naturelle.

**[2]** « Des choses cachées depuis la fondation du monde » Grasset, 1978, dialogue avec René Girard.

**[3]** Of ice 360 : en aout 2022, le député Philippe Latombe alerte M. le ministre de l'éducation nationale et de lajeunesse sur la gratuité d'Of ice 365 pour les élèves et les enseignants. Lien web : https://www2.assemblee-.fr/deputes/fiche/OMC_PA721984

**[4]** Lire à ce propos, l'édifiant le livre de Franck Frommer : « La pensée PowerPoint. Enquête sur ce logiciel qui rend stupide »

**[5]** Apports et limites de l'approche girardienne des rivalités mimétiques à l'analyse des conflits => https://www.afri-ct.org/wp-content/uploads/2018/06/Article-Berger.pdf

**[6]** https://fr.wikipedia.org/wiki/Dark_web

**[7]** Voir également des lois encadrant l'utilisation strictes des technologies (RGPD, en outre).

**[8]** L'intelligence artificielle désigne communément l'ensemble des théories et techniques ayant pour finalité la création de machines capables d'exécuter des tâches traditionnellement réservées à l'intelligence humaine.

**[9]** Data Governance Strategy en anglais.

**[10]**
https://www.latribune.fr/economie/france/entreprises-francaises-alerte-maximale-sur-des-menaces-de-predation-etrangeres-885247.html

**[11]**
https://www.ege.fr/infoguerre/2016/03/la-lutte-anti-corruption-outil-d%25e2%2580%2599influence-des-etats-unis

**[12]**
https://www.economie.gouv.fr/entreprises/blockchain-definition-avantage-utilisation-application

**[13]**
https://siecledigital.fr/2021/06/16/deputes-europeens-renforcement-dispositifs-connectes/

**[14]** « La malédiction de l'argent liquide », non traduit (« The Curse of Cash »), paru aux éditions Princeton – University Press, 2016).

**[15]**
https://www.lopinion.fr/politique/il-ne-faut-surtout-pas-de-ministre-du-numerique-la-tribune-de-giuseppe-de-martino

## Mezze de tweets

> *Nous avons lu « Dé-coder, une contre-histoire du numérique » de @catchthewhistle et notre verdict est sans appel : Recommandation HAUTE !?Découvrez-en ici notre recension.https://t.co/MXjjeKAc7l pic.twitter.com/IFUA5Px6uA*
>
> *— souveraine tech (@SouveraineTech) October 24, 2022*

> *Excellente nouvelle ! On va parler français en France. Prochaine étape, l'hébergement des données ? #HealthDataHub https://t.co/IV5A4MMX9Y*
>
> *— souveraine tech (@SouveraineTech) October 24, 2022*

> *Une étudiante en chimie de l'université de Surrey (Angleterre) a inventé une sorte de poisson-robot capable de dépolluer les rivières en capturant les microplastiques. Une innovation qui lui a valu un prix dans un concours de robots biomimétiques.https://t.co/OrcfF2fHmf*
>
> *— souveraine tech (@SouveraineTech) October 24, 2022*

> *L'objectif de #Microsoft est "d'aider la #France à retrouver sa #souveraineté économique et industrielle."#MasterTrolls ????https://t.co/nvqo05y5ZJ*
>
> *— souveraine tech (@SouveraineTech) October 24, 2022*

> *Le gouvernement surveille le risque d'écoutes depuis des toits de Paris après le rachat de 600 sites de télécommunications par un fonds d'origine américaine.https://t.co/sBrt4AuHi6*
>
> *— souveraine tech (@SouveraineTech) October 24, 2022*

*L'influence du parti communiste chinois dans le monde https://t.co/jHSqAa6RZX*

*— souveraine tech (@SouveraineTech) October 25, 2022*

*Nous venons de mettre à jour notre petite éphéméride de la démission, avec le passage de l'entreprise #TRAD?? sous pavillon ??. Diffusez largement cette soixantaine de dates qui disent toutes le contraire du discours ambiant. https://t.co/99h6WPdKLT*

*— souveraine tech (@SouveraineTech) October 25, 2022*

*Pensez à remplir vos frigos.https://t.co/5vVn2EriAw*

*— souveraine tech (@SouveraineTech) October 25, 2022*

*"De plus en plus de nos chercheurs se risquent à défier les géants de la tech. @jlmoullet, en charge de l'#innovation au @CNRS, veut les y encourager."https://t.co/lDBWTBYlvj*

*— souveraine tech (@SouveraineTech) October 25, 2022*

*Top 10 des fournisseurs cloud chinois et les leçons à en tirerhttps://t.co/QPuIvgiqqK*

*— souveraine tech (@SouveraineTech) October 25, 2022*

*« Devenir une 'nation licorne' est une erreur de politique publique. Les licornes sont considérées à tort comme une panacée pour la croissance et la souveraineté numérique par le gouvernement de Macron » selon @cyrine https://t.co/X1PuobZDin*

> — souveraine tech (@SouveraineTech) October 25, 2022

> L’Allemagne multiplie les affronts envers la France sur les projets d’armementhttps://t.co/tryGlR4IbD
>
> — souveraine tech (@SouveraineTech) October 25, 2022

---

---

## □□ Hors spectre

**Anse du chaudron retrouvé à Lavau représentant le dieu grec Acheloos.**

*Les lâches qui me calomnient oseraient-ils m’affronter en face ? Georges Jacques DANTON*