RECUEIL

LA CONFIANCE À L'ÈRE DU NUMÉRIQUE : CINQ PROBLÉMATIQUES, SIX REGARDS

mars 2022

Institut Messine

www.institutmessine.fr

Institut Messine

Présentation

Créé au cours de l'année 2014 avec le soutien de la Compagnie Nationale des Commissaires aux Comptes (CNCC), l'Institut Messine est un *think tank* qui rassemble en son sein des représentants de la société civile et de la profession des commissaires aux comptes qui se sont donné pour mission de réfléchir aux grands enjeux économiques auxquels sont confrontés le pays et ses entreprises. Il ambitionne de formuler puis de soumettre au débat, sous la forme de Rapports et de Notes, des idées et des solutions originales et concrètes susceptibles de nourrir la réflexion et l'action du décideur public. Il s'attache particulièrement aux questions de transparence et de confiance.

L'Institut Messine s'efforce de créer les conditions de travail les plus propices au traitement d'un sujet, notamment par la composition de groupes de travail qui réunissent les meilleures compétences pour chacun des thèmes abordés, la diversité du recrutement garantissant une réelle diversité d'analyses. Dès lors, les opinions exprimées dans les Rapports sont celles de la collectivité du groupe, mais elles ne sauraient engager chacun de ses membres en particulier. *A fortiori,* les Notes, Recueils et Rapports publiés sous l'égide de l'Institut ne l'engagent ni lui-même, ni ses organes de gouvernance, ni la CNCC.

Institut Messine
De l'audit à la société

www.institutmessine.fr

Remerciements

L'Institut Messine remercie particulièrement les personnes suivantes pour leur contribution.

L'Auteur-coordinateur

- **Marianne FOUGÈRE –** Docteur en science politique de l'Institut d'Études Politiques de Paris, spécialiste de la pensée d'Hannah Arendt, Marianne FOUGÈRE a d'abord porté ses travaux de recherche sur la notion de la communauté et sur la question du jugement politique avant d'étendre son expertise aux problématiques liées aux ressources humaines, au futur du travail, à la transformation numérique et aux technologies.

  Plume indépendante, elle accompagne entreprises et particuliers dans leurs différents projets d'écriture (articles, interviews, contenus pédagogiques, livres blancs, scénarios, coaching éditorial, etc.). Diplômée de Sciences Po Paris, Marianne Fougère assure par ailleurs des cours en politique comparée et en humanités politiques au sein de cette institution. Elle a publié plusieurs ouvrages, consacrés à la préparation de concours (fonction publique, IEP) ou à des notions de culture générale comme le secret, les radicalités ou encore le numérique.

Les contributeurs

- **Ferghane AZIHARI** – Essayiste et analyste en politiques publiques, membre de la Société d'économie politique et délégué général de l'Académie libre des sciences humaines.
- **Jean-David BENASSOULI** – Associé, Responsable de l'activité Data Intelligence de PwC France et Maghreb.
- **Yseulys COSTES** – Co-Fondatrice & CEO du groupe Numberly.
- **Frédéric FILLOUX** – Journaliste économique, créateur et éditeur des lettres d'information « Monday Note » et « Episodiqu.es. » sur l'économie des médias numériques.
- **Jean-Louis GERGORIN** – Maître des requêtes honoraire au Conseil d'État, consultant en stratégie aérospatiale, défense et cyber.
- **Nathalie MALICET** – Expert-comptable, Commissaire aux comptes, Associée chez Anexis ; Présidente de la Commission Prospectives et Innovation de la Compagnie Nationale des Commissaires aux Comptes (CNCC).

L'Institut Messine tient également à remercier Vae Solis Communications pour sa participation à l'élaboration de ce Recueil.

Les entretiens et le texte du Recueil *ont été réalisés entre décembre 2021 et début mars 2022.*

Les opinions exprimées dans le présent Recueil *n'engagent ni les personnes citées, ni les institutions qu'elles représentent.*

Sommaire

Introduction

La confiance numérique : panser les vulnérabilités pour mieux la réinventer

« – Vous m'avez recommandé d'avoir confiance, vous m'avez affirmé que la confiance était indispensable, et à présent vous prêchez la méfiance. Ah, j'en aurai le cœur net !

– Je vous ai dit, assurément, que vous deviez avoir confiance, et même une confiance aveugle, mais je parlais de votre confiance dans mon remède bienfaisant et de votre confiance en ma personne sincère.

– Mais en votre absence, si je décidais d'acheter des remèdes qui se font passer pour le vôtre, je ne devrais donc pas accorder ma confiance aveuglément.

– Examinez bien tous les flacons ; accordez votre confiance à ceux qui sont authentiques.

– Mais douter, soupçonner, examiner – se livrer constamment à cette tâche épuisante – voilà bien l'opposé de la confiance. Voilà bien de mauvais sentiments !

– Du mal vient le bien. La méfiance est une étape de la confiance. »

Herman Melville, *The Confidence-Man, His Masquerade* (1857)

Écrites dans la seconde moitié du XIXe siècle, ces quelques lignes résonnent étrangement avec notre quotidien. Confiance et méfiance, foi aveugle et soupçon généralisé, économie de la confiance et société de la défiance : comment, en effet, ne pas reconnaître certains traits de notre époque dans le dialogue imaginé par Herman Melville ? Les correspondances entre nos comportements et le **besoin passionné de croire et de faire confiance** décrit, dans son ultime roman, par l'auteur de *Moby Dick*[1] sont frappantes. Mieux, **désormais la confiance est partout.**

Il suffit d'écouter autour de soi. Ou d'entrer le mot « confiance » dans la rubrique « Actualités » du premier moteur de recherche venu. Le dernier *Trust Barometer* nous révèle ainsi qu'**aucun pays occidental n'atteint un *Trust Index* supérieur à 60 points, qui marque l'entrée dans la « zone de confiance**[2] **» accordée par la**

1. Mort dans l'indifférence générale, Herman Melville (1819-1891) est aujourd'hui considéré comme l'un des pionniers de la littérature américaine et ce malgré un passage éclair dans l'histoire de celle-ci. En 1857, *The Confidence-Man, His Masquerade* (*Le Grand Escroc* en français) est si mal reçu par le public et la critique que l'écrivain décide, en effet, de mettre un terme à sa carrière. Mais, il ne cessera pas pour autant d'écrire : ses dernières années seront consacrées à reprendre et à développer *Billy Budd, marin*, un poème devenu roman qui sera publié à titre posthume en 1924.
2. Établi à partir de données récoltées en novembre 2021 auprès de 36 000 répondants à travers 28 pays, le baromètre annuel d'Edelman livre des clés de lecture de la confiance des populations à l'égard de quatre institutions : gouvernement, entreprises, médias et organisations non gouvernementales. On parle de défiance quand la moyenne de la confiance accordée aux différentes institutions est inférieure à 50 ; la confiance est neutre quand la moyenne est entre 50 et 59. En revanche, on entre dans la zone de confiance quand le niveau de confiance atteint les 60 et plus.

population aux institutions. On apprend également en février 2022 que le président du Paris Saint-Germain, Nasser Al-Khelaïfi, réitère toute sa confiance au footballeur argentin Lionel Messi alors que le bilan du septuple Ballon d'Or s'avère bien en deçà des attentes qui avaient été formulées lors de son arrivée en fanfare au cœur de l'été 2021. En revanche, un militaire ukrainien, posté à la frontière biélorusse, déclare se méfier de l'accalmie russe tant il *« ne fait pas du tout confiance »* aux troupes de Vladimir Poutine. Ce texte, quant à lui, n'aurait jamais existé sans la confiance accordée à son auteure.

Dans le langage de tous les jours, la confiance apparaît sous plusieurs visages : confiance en soi, confiance en autrui, confiance dans les institutions. Il arrive aussi que l'on parle de la « confiance en l'avenir ». Celle-ci n'est pas seulement révélatrice d'un certain optimisme ou d'un trait psychologique. **Les économistes voient en elle l'un des ingrédients de la croissance.** D'ailleurs, des « indices de confiance » existent, comme celui du Michigan aux États-Unis[3] ou celui de l'Insee qui indique, pour janvier 2022, une baisse d'un point de la confiance des ménages français. Cet indicateur résume l'opinion que portent les ménages sur l'environnement économique : *« plus sa valeur est élevée, plus le jugement des ménages sur la situation économique est favorable[4] ».* Située en janvier 2022 à 99, c'est-à-dire légèrement au-dessous de sa moyenne de longue période (100), la confiance des ménages français est donc quasiment stable. Ce qui s'avère être plutôt une bonne nouvelle.

Il faut dire que la confiance est la condition préalable à tout échange économique. Qu'il s'agisse de fournir un travail, d'investir ou d'acheter un bien dont la qualité ne serait pas immédiatement vérifiable, aucun de ces échanges ne peut avoir lieu si la méfiance entre les agents économiques est trop forte. Quel intérêt, en effet, pour un acheteur de s'engager dans une transaction s'il redoute de ne pas être livré ? Quel intérêt pour un employé d'effectuer son travail s'il craint de ne pas percevoir de rémunération à la fin ?

Adam Smith (1723-1790), maître à penser de la théorie économique classique, le savait mieux que nul autre, ***« ce n'est pas de la bienveillance du boucher, du marchand de bière ou du boulanger que nous attendons notre dîner, mais bien du soin qu'ils apportent à leurs intérêts[5] »***. L'auteur de *La Théorie des sentiments moraux* insistait d'ailleurs sur le rôle central de la sympathie dans la facilitation des relations marchandes et du fonctionnement des marchés[6]. Quant à son ouvrage *La Richesse des nations*, c'est également à la lumière de la confiance, et non d'un facteur purement économique, qu'elle peut se comprendre selon l'économiste américain Kenneth Arrow (1921-2017). Lorsqu'il reçut en 1972 le prix Nobel d'économie, l'Américain de 51 ans

3. Les données de l'indice de confiance du Michigan, ou *Michigan Consumer Sentiment Index*, sont les résultats de sondages téléphoniques, effectués chaque mois sur un panel d'environ 500 consommateurs par l'*Institute for Social Research* de l'Université du Michigan. Les membres du panel sont interrogés sur ce qu'ils attendent de l'économie, sur leur vision de l'économie pour l'année en cours et les cinq à venir, ainsi que sur leurs finances personnelles. En janvier 2022, l'indice est ressorti à 67,2 contre 70,6 en décembre 2021.

4. Le site de l'Insee précise également que l'indicateur synthétique est *« calculé selon la technique de l'analyse factorielle qui permet de résumer l'évolution concomitante de plusieurs variables dont les mouvements sont très corrélés. L'indicateur décrit ici la composante commune de huit soldes d'opinion : niveau de vie passé et futur en France, situation financière personnelle passée et future, chômage, opportunité de faire des achats importants, capacité d'épargne actuelle et capacité d'épargne future ».*

5. Adam Smith, *La Richesse des nations*, Tome 1, Paris, Flammarion, 1991.

6. Dans le premier chapitre de sa *Théorie des sentiments moraux* (Paris, PUF, coll. Quadrige, 2014), Smith donne de la sympathie la définition suivante : *« Que notre frère soit soumis au supplice du chevalet, aussi longtemps que nous serons à notre aise jamais nos sens ne nous informeront de ce qu'il souffre. Ces derniers n'ont jamais pu et peuvent jamais nous transporter au-delà de notre personne. Ce n'est que par l'imagination que nous pouvons former une conception de ce que sont ses sensations. Et cette faculté ne peut nous y aider d'aucune autre façon qu'en nous représentant ce que pourraient être nos propres sensations si nous étions à sa place. Ce sont les impressions de nos sens seulement, et non celles des siens, que nos imaginations copient. Par l'imagination nous nous plaçons dans sa situation, nous nous concevons comme endurant les mêmes tourments, nous entrons pour ainsi dire à l'intérieur de son corps et devenons, dans une certaine mesure, la même personne ».*

surprit son monde en déclarant : ***« Virtuellement, tout échange commercial contient une part de confiance, comme toute transaction qui s'inscrit dans la durée. On peut vraisemblablement soutenir qu'une grande part du retard de développement économique d'une société est due à l'absence de confiance réciproque entre ses citoyens[7] ».***

Mais n'allez y voir aucune fatalité. Promesses, serments, règles formelles : autant de garde-fous qui permettent de **pallier le déficit de confiance spontanée.** Cependant, chacun d'entre nous sait combien la tentation de ne pas tenir ses promesses est grande. Tandis que la valeur des serments s'estompe à mesure que la crainte d'une possible sanction divine disparaît. Et si la solution du contrat garantit le bon déroulement des échanges, cette option peut s'avérer juridiquement coûteuse en cas de conflit.

C'est pourquoi l'économiste américain, spécialiste de la théorie du jeu, David Kreps estime, dès les années 1990, que **la réputation peut suffire à assurer la confiance.** Un mécanisme réputationnel repris depuis par l'économie des plateformes Internet[8]. Leurs systèmes de notation ou d'avis certifiés se basent, en effet, sur les comportements adoptés par les utilisateurs lors des échanges précédents. Malgré tout, on pourrait douter de l'importance de la réputation quand les agents économiques avec lesquels nous entrons en relation se cachent désormais sous des pseudonymes aussi poétiques que « galou63 » ou « toons_petitefleur » …

Sans surprise donc, galou63 nous inspire de prime abord de la méfiance. Mais celle-ci s'envole vite une fois que les cinq euros, reçus en échange de ce tee-shirt, sont bien déposés sur notre compte bancaire. Nous acceptons le paiement de galou63 car nous avons confiance en la valeur de l'euro.

De la même manière, **nous accordons notre confiance à la monnaie et, plus généralement, aux institutions** sur lesquelles repose notre système économique non seulement **parce qu'elles font partie de nos vies quotidiennes** mais surtout **parce qu'elles sont soutenues par des organisations comme les tribunaux, les banques ou encore les commissaires aux comptes.** La présence d'un auditeur légal permet, en effet, de sécuriser à la fois l'entreprise et toute autre entité, l'entrepreneur et son environnement. **Du fait d'un travail minutieux et rigoureux de certification et de transparence des comptes, les commissaires aux comptes créent un environnement de confiance** pour les financeurs, les investisseurs, les fournisseurs, mais aussi pour les salariés et les clients[9]. **En jouant leur rôle de garants de la relation de confiance entre les entreprises et leurs parties prenantes, les commissaires aux comptes témoignent du caractère composite de la confiance.**

Cette dernière, en effet, peut être décomposée en trois moments clés : *« quand la confiance s'installe, quand elle fonctionne, et quand elle entre en crise (ce qui finit toujours par arriver)[10] »*. Ne dit-on pas d'ailleurs que nous sommes entrés dans **« l'âge de la défiance »** ? Le constat, dès 2007, d'une crise de la confiance en France est en tout cas l'une des prémisses du livre des économistes français Yann Algan et Pierre Cahuc. *« En France,*

7. Kenneth Arrow, "Gift and exchanges", *Philosophy and Public Affairs*, 1972, vol. 1, p. 343-362.
8. Selon Kreps, quelqu'un a bonne réputation si les autres croient qu'il ou elle est, ou peut être, une *« âme coopérative ».* Voir notamment *Game Theory and Economic Modelling. Clarendon Lectures in Economics,* Oxford, Clarendon Press, 1990.
9. Dans son article 4, le Plan d'action sur l'accompagnement des entreprises en sortie de crise confie aux commissaires aux comptes une nouvelle mission *« prévention et relation de confiance »*. Dans le cadre de celle-ci, les commissaires aux comptes sont désormais chargés de sensibiliser les dirigeants sur l'opportunité de se tourner vers le tribunal de commerce ou le tribunal judiciaire, lorsque la situation de l'entreprise le justifie.
10. Achille Weinberg, « Qu'est-ce que la confiance ? », *Sciences Humaines*, 2015/6, n° 271, p. 22.

la défiance règne », soulignent les auteurs de *La Société de défiance. Comment le modèle social français s'autodétruit*[11]. Une affirmation confirmée par la douzième vague du *Baromètre de la confiance politique* conduite en février 2021 en France, en Allemagne, en Italie et au Royaume-Uni par le CEVIPOF. **Dans notre pays, en effet, la confiance sociale reste faible :** 62 % des Français interrogés déclarent ainsi que *« l'on n'est jamais assez prudent quand on a affaire aux autres »*. Seuls 35 % d'entre eux estiment que *« l'on peut faire confiance à la plupart des gens »*, contre 42 % pour les Allemands et 45 % pour les Britanniques[12].

Pourtant, même chez nous, la confiance s'améliore. Celle que l'on porte à sa famille reste très élevée[13]. Et que dire de notre capacité à faire confiance à des personnes qui habitent à l'autre bout du pays, voire à l'autre bout du monde ? **L'économie numérique**, et la numérisation de nos sociétés en général, **illustrent en effet parfaitement que, aujourd'hui comme hier, rien ne s'entreprend ni ne se crée sans confiance.**

Le développement des paiements à distance a été longtemps handicapé par les risques perçus de ces nouvelles modalités de paiement, des risques souvent fantasmés mais qui ne sont pas sans fondement objectif. Un manque de confiance qui explique, en grande partie, pourquoi la frontière entre commerce physique et commerce en ligne a mis du temps à s'estomper[14]. Et si le e-commerce a fini par entrer dans les mœurs, c'est parce que les conditions de la confiance ont été peu à peu réunies. Inversement, **c'est précisément parce que leurs décisions scient parfois la branche de confiance sur laquelle sont assises leurs activités, que ces géants que sont Google, Amazon, Facebook, Apple ou Microsoft, essuient régulièrement de vives critiques,** que l'économie numérique rencontre encore certaines résistances. **Cercle vicieux que celui d'une époque digitalisée qui a besoin de confiance mais ne l'accorde pas toujours, voire ne semble plus du tout y croire.**

C'est pourquoi l'Institut Messine, *think tank* de la profession des commissaires aux comptes, a voulu explorer plus spécifiquement le thème de la confiance à l'ère de la révolution numérique. Pour mener à bien cette exploration, **six praticiens ou témoins aux points de vue complémentaires ont été consultés : entrepreneur, spécialiste du cyber, commissaire aux comptes, expert de la transformation des métiers du conseil, journaliste, essayiste…** Chacun a pu éclairer depuis son poste d'observation particulier les bouleversements rencontrés par la confiance à l'heure numérique, les enjeux posés par le numérique pour la confiance. Car, c'est là toute

11. Yann Algan, Pierre Cahuc, *La Société de défiance. Comment le modèle social français s'autodétruit,* Paris, Éditions rue d'Ulm/Presses de l'École normale supérieure, coll. du CEPREMAP, 2007. Dans cet ouvrage, les auteurs soutiennent que *« le déficit de confiance des Français est intimement lié au fonctionnement de leur État et de leur modèle social »*, modèle qui *« s'est construit sur des bases corporatiste et étatiste »*. Cela influe selon eux sur l'intervention de l'État puisque, dans une logique dirigiste et corporatiste bien établie, celle-ci *« consiste généralement à accorder des avantages particuliers aux groupes qui en font la demande, souvent au détriment du dialogue social, du respect des règles de la concurrence et de la transparence des mécanismes de solidarité. Ce type d'intervention ne peut qu'entretenir la défiance mutuelle et favoriser, en retour, l'expansion du corporatisme et de l'étatisme »*. Un cercle vicieux qui, selon Yann Algan et Pierre Cahuc, *« mine l'efficacité et l'équité du fonctionnement de notre économie »*.
12. Sciences Po, CEVIPOF, *Baromètre de la confiance politique,* « En qu(o)i les Français ont-ils confiance aujourd'hui ? », vague 12, Février 2021. Cette douzième édition a été l'occasion de poursuivre la comparaison européenne entamée en mars 2020, en élargissant l'étude à l'Italie, après le Royaume-Uni et l'Allemagne.
13. Depuis trois années consécutives, celle-ci reste stable. Les Français sont ainsi 94 % à déclarer faire confiance aux membres de leur famille. Le taux de confiance envers les personnes d'une autre nationalité, en revanche, a grimpé en flèche, passant de 55 % en février 2021 à 63 % en janvier 2022. Tels sont les résultats donnés par la vague 13 du *Baromètre de la confiance politique* (« En qu(o)i les Français ont-ils confiance aujourd'hui ? ») réalisée du 23 décembre 2021 au 10 janvier 2022 auprès d'un échantillon de 10 566 personnes inscrites sur les listes électorales, lui-même issu d'un échantillon de 11 842 personnes représentatif de la population française âgée de 18 ans et plus.
14. Selon les chiffres communiqués par la Fédération e-commerce et vente à distance dans son dernier « Bilan du e-commerce en France », les ventes en ligne ont dépassé les 129 milliards d'euros en 2021, soit une hausse de 15,1 % contre 8,5 % en 2020.

la particularité de ce recueil : **esquisser de la confiance numérique une représentation non pas exhaustive mais synoptique[15].** C'est en effet à la seule condition de faire l'expérience des différents aspects de la confiance numérique qu'il devient possible de se libérer de l'emprise de certaines images, qui voudraient soit que l'on se méfie absolument du numérique, soit qu'on l'embrasse sans se poser suffisamment de questions.

Ces enjeux spécifiques de confiance, liés à la numérisation de nos économies et de nos sociétés, les commissaires aux comptes et les auditeurs y sont les premiers confrontés. Dans leur contribution, **la commissaire aux comptes Nathalie Malicet et le responsable de l'activité Data analytics et Intelligence artificielle de PwC France et Maghreb Jean-David Benassouli** soulignent ainsi combien « la confiance dans les chiffres » a changé de dimension avec l'augmentation des volumes de données traitées par les entreprises. Les commissaires aux comptes doivent plus que jamais « viser la résilience, c'est-à-dire être capables de détecter les risques » en menant des missions de diagnostic[16] pour estimer, par exemple, le coût d'une paralysie des systèmes d'information ou d'une violation des données. Preuve s'il en fallait encore une qu'ils **participent pleinement à bâtir une société de la confiance numérique.**

Or de cela, toutes les institutions ne peuvent se targuer. Dernier exemple en date ? Les banques. Nous ne nous attarderons pas sur la crise financière des *subprimes* causée par un excès de confiance des opérateurs sur les marchés financiers. La défiance généralisée qui s'est ensuite répandue sur le marché interbancaire permet certes *« de comprendre pourquoi les prêts entre établissements de crédit furent gelés à l'automne 2008[17] »*. Elle donne surtout un argument de plus à ceux qui, comme l'essayiste et analyste en politiques publiques **Ferghane Azihari**, estiment que **nous aurions tort de nourrir une confiance aveugle dans les banques centrales.** À force d'imprimer de la monnaie à tout va pour stabiliser le système financier, celles-ci ont en effet fini par fragiliser la confiance dans sa solidité. En réalité, selon Ferghane Azihari, ***« les problèmes de confiance sont (…) monnaie courante dans l'histoire de la banque et de la finance »***, que seules des cryptomonnaies comme le Bitcoin peuvent espérer résoudre. Comment ? *« [P]ar la promesse de ne pas mettre plus de 21 millions d'unités en circulation »*. ***« Le Bitcoin***, affirme Ferghane Azihari, ***augmente la rareté et règle de façon probante le problème de méfiance, voire de défiance, que l'on peut nourrir à l'égard des banques »***. En revanche, il ne résorbe pas tous les problèmes de confiance existant dans cet espace si particulier qu'est l'espace numérique.

La confiance numérique touche à l'amitié, reconfigurée à coup de *« likes »* sur les réseaux sociaux, **mais aussi à la vie de couple,** pimentée par ces plateformes technologiques qui autorisent les rencontres adultères en toute discrétion… ou, au contraire, au vu et au su de tous. **Les organisations, de leur côté, cherchent des solutions managériales pour « recréer de la confiance » et transformer les métiers et compétences à mesure que progresse la digitalisation de notre société et de notre économie.**

Les marques doivent quant à elles trouver de nouveaux moyens pour **construire une relation de confiance avec les consommateurs** et ce alors même que le numérique a bouleversé la manière dont une entreprise

15. Selon Ludwig Wittgenstein (1889-1951), *« l'une des sources principales de nos incompréhensions est que nous n'avons pas une vue synoptique de l'emploi de nos mots »*. En l'absence d'une représentation synoptique, il semble difficile pour le philosophe et mathématicien autrichien de parvenir à clarifier le sens d'un concept puisque seule cette forme particulière de représentation permet de *« voir les connexions »*, de *« trouver et [d']inventer des maillons intermédiaires »*. Voir notamment Ludwig Wittgenstein, *Recherches philosophiques*, Paris, Gallimard, 2014.
16. Pour mener à bien ces missions de diagnostic, les commissaires aux comptes peuvent avoir recours à des outils comme CyberAUDIT et RGPDAUDIT, deux plateformes mises à leur disposition par la Compagnie Nationale des Commissaires aux Comptes.
17. Éloi Laurent, *Économie de la confiance,* Paris, La Découverte, coll. « Repères », 2019.

vend et communique. La construction de cette relation passe ainsi par une **démarche de transparence sur la valeur effective apportée par la collecte des données.** En effet, **le développement de la sphère marchande sur le web a entraîné un questionnement sur l'usage et le traitement des données.** En Europe, celles-ci font désormais l'objet d'un cadre juridique renforcé grâce notamment au Règlement Général sur la Protection des Données **(RGPD)**[18]. *« Il n'en demeure pas moins,* regrette l'experte en marketing digital et fondatrice du groupe Numberly **Yseulys Costes**, *que l'**on peut se poser la question de son efficacité et s'interroger sur la capacité des consommateurs à en comprendre les tenants et les aboutissants »***. Il faut donc expliquer aux consommateurs pourquoi on collecte leurs données. Mais ces derniers doivent aussi acquérir une **culture numérique solide.** Ne serait-ce que pour comprendre ce qu'ils font et pourquoi ils le font… **Une nécessité quand on sait combien le numérique a totalement inversé le cycle de pénétration des innovations.**

Jusqu'à la création d'Internet, les innovations entraient dans nos sociétés par la porte des entreprises avant de franchir, dans un second temps, le seuil de nos habitations. Or *« [l']inversion des flux de diffusion a bouleversé la vitesse d'adoption des innovations et, surtout, leur « encadrement » ».* À défaut de structure normative solide, on s'expose ainsi à *« des **problèmes d'encadrement et d'apprentissage** de l'usage lui-même »*. Le numérique apporte avec lui de nouvelles inégalités par le biais de l'« **illectronisme** ». Cela est d'autant plus inquiétant que *« [l]e digital reste un outil complexe car multiforme »*, nous explique Yseulys Costes. En effet, **l'espace numérique est tout à la fois un espace marchand dans lequel des transactions ont lieu, *« une technologie qui modifie les processus, les flux d'opérations et d'activités dans l'ensemble des secteurs »* mais aussi un terrain d'expression individuelle et un espace informationnel.**

Comment ne pas se réjouir d'avoir accès, grâce à la transformation digitale, **aux journaux du monde entier en un clic ?** Comment ne pas apprécier de trouver dans la seconde l'information utile pour rédiger un exposé ou remplir un document administratif ? Comment ne pas reconnaître le rôle des réseaux sociaux dans l'entretien de relations avec des personnes éloignées géographiquement ou, à certains moments de notre histoire récente, dans l'émergence de soulèvements populaires dans des pays non-démocratiques où les médias étaient censurés ?

Le numérique, chacun le sait, transforme notre relation aux médias et au mode d'expression individuelle. Pour le meilleur comme pour le pire. Médias traditionnels, nouveaux médias, réseaux sociaux : aucun d'entre eux n'obtient désormais une majorité de confiance de la part des Français, en témoigne le 35e *Baromètre de confiance dans les médias* Kantar-Onepoint pour le journal *La Croix*[19]. Et **si le numérique fait souffler un vent de renouveau sur un secteur en proie à de grandes difficultés, *« il encourage la surenchère, la polémique et la caricature au détriment du recul, de la distance et de l'analyse ».*** Ce qui conduit le journaliste économique spécialiste du numérique **Frédéric Filloux** à craindre que ne **se développe une information à deux vitesses : *« l'information de qualité [risque de] se verticaliser peu à peu, au point de devenir l'apanage de gens éduqués, âgés et aisés financièrement (…) tandis qu'une majorité, plus jeune, s'informera médiocrement,* via *les chaînes d'infos ou les réseaux sociaux construits sur le clivage et la polarisation ».***

18. Le Règlement Général de Protection des Données (RGPD) est un texte réglementaire européen qui encadre le traitement des données de manière égalitaire sur tout le territoire de l'Union européenne. Il est entré en application le 25 mai 2018.
19. L'édition 2022 du baromètre, menée du 5 au 11 janvier 2022, montre ainsi que la radio a perdu 3 points de crédibilité pour se retrouver au même niveau que la presse écrite (49 %). Et si la confiance dans la télévision progresse de deux points (44 %), celle envers Internet (24 %) renoue avec ses plus bas niveaux historiques.

Sans compter la **propagation des *fake news* et des *deep fakes*** facilitée par la multiplication des plateformes de médias sociaux. Qui croire et que croire en ligne où rien ne semble fiable ? La réponse à cette menace doit passer, nous dit Frédéric Filloux, par **davantage de moyens alloués aux journalistes.** À ce titre, l'intelligence artificielle peut également être vecteur d'espoirs si elle est mise, par exemple, au service de l'investigation par sa capacité à extraire d'un très gros volume de data des informations pertinentes. Nous ne pourrons pas non plus faire l'économie d'**une refonte de la formation professionnelle des journalistes et, très en amont, d'une éducation aux médias pour nos enfants.**

Qui croire et que croire en effet quand même certains États initient des campagnes de désinformation ? ***« Avec le numérique,* analyse le spécialiste des sujets cyber et de défense Jean-Louis Gergorin*, nous sommes entièrement entrés dans l'ère de la guerre en temps de paix. Son utilisation, à des fins d'influence ou de contrôle, représente un moyen alternatif de continuation de la politique ».*** Selon lui, le numérique signe en effet *« l'avènement d'une nouvelle forme de conflictualité, située toujours en dessous du seuil de la guerre ouverte »*.

Le danger dans un tel contexte ? Réduire les enjeux de souveraineté aux appels à la réindustrialisation de l'Europe ou aux cris insurgés contre la décision du gouvernement de remettre les données de santé des Français entre les mains de Microsoft. **La cybersécurité doit elle aussi être considérée comme une composante centrale de la souveraineté des États.** Cette souveraineté passe par la capacité des entreprises et des organisations à assurer leur cybersécurité. Jean-Louis Gergorin appelle à un **décloisonnement** et à une **plus grande coopération dans la cyberdéfense** en France, envisageant même la création d'une *« réserve nationale de tous les intervenants et experts cyber en entreprise qui pourrait se mobiliser en cas de situation critique »*.

Attention, toutefois, à ne pas confondre cybersécurité et approche (cyber)sécuritaire au risque sinon de se focaliser sur les menaces externes et, ce faisant, négliger ce qui mine la confiance de l'intérieur. À ce titre, le paradoxe et la mise en garde formulés par Jean-Louis Gergorin sont on ne peut plus clairs : ***« plus on se numérise, plus on se vulnérabilise ».*** Vulnérabilité que la sécurité court-circuite et qui pourtant est, avec l'absence de garantie, l'une des deux conditions mêmes de la confiance.

C'est en tout cas ce que donne à penser son étymologie. *« Au sens strict du terme*, rappelle la philosophe Michela Marzano, ***la confiance renvoie à l'idée qu'on peut se fier à quelqu'un ou à quelque chose.*** *Le verbe confier (du latin* confidere *:* cum, *« avec »* et fidere *« fier »*) *signifie, en effet, qu'on remet quelque chose de précieux à quelqu'un, en se fiant à lui et en s'abandonnant ainsi à sa bienveillance et à sa bonne foi.* ***L'étymologie du mot montre par ailleurs les liens étroits qui existent entre la confiance, la foi, la fidélité, la confidence, le crédit et la croyance[20] ».*** Elle n'en est pas moins trompeuse. Au sens propre, **la confiance n'émerge *« qu'entre deux êtres humains, éventuellement par la médiation d'une institution et donc d'une norme sociale***, *mais en tout cas pas entre un être humain et lui-même ou un être humain et une abstraction, fût-elle de nature spirituelle[21] »*. Ce rapprochement entre foi et confiance s'avère d'autant plus problématique qu'il occulte le fait que cette dernière *« suppose l'exercice de la volonté (mais pas nécessairement celui de la raison, du jugement informé ou de la perspicacité) »*, là où la foi s'apparente davantage *« à l'abandon au moins partiel du libre arbitre[22] »*.

20. Michela Marzano, « Qu'est-ce que la confiance ? », *Études,* 2010/1, Tome 412, p. 53-63.
21. Éloi Laurent, *Économie de la confiance, op. cit.*
22. *Ibid.*

Cette précision apportée, nous comprenons mieux pourquoi depuis la Modernité, *« nombreux sont ceux qui préfèrent* ***concevoir la confiance comme un mécanisme de réduction des risques****, ou encore comme le fruit d'un calcul rationnel[23] »*. L'appréhender par un tel prisme laisse en effet la possibilité de **se positionner en maître et possesseur de la confiance.** Comment ? Par la mise en place de *« dispositifs de confiance »*[24]. **Il suffit d'observer les textes réglementaires se multiplier pour mesurer l'importance prise par les « chartes de confiance » pour encadrer les échanges interpersonnels et, plus largement, la vie collective**. Au point d'ériger ces dispositifs en nouveaux fétichismes. Ainsi, *« la fée confiance[25]»* enchante la loi « sur la confiance dans l'économie numérique[26] » comme celles pour « un État au service d'une société de confiance[27] » ou « une École de la confiance[28] ». Plus récemment, la loi « pour la confiance dans l'institution judiciaire[29] » s'inscrit, selon l'économiste français Éloi Laurent, *« dans le même registre d'invocation performative[30] »*.

La « pensée magique » peut bien impulser voire dicter l'action publique. Mais, aussi puissante soit-elle, elle ne parviendra jamais à gommer totalement l'état d'incertitude et même de vulnérabilité de ceux et celles qui accordent leur confiance. **En effet, qu'est-ce que faire confiance sinon *« se rendre vulnérable à l'égard d'un partenaire alors que ce partenaire ne peut être contrôlé ou surveillé[31] »* ?** *« Celui qui sait tout*, résume le sociologue et philosophe allemand Georg Simmel (1858-1918), *n'a pas besoin de faire confiance[32] »*. D'ailleurs, les notions d'« abus de confiance » sanctionné par le Code pénal et de « personne de confiance » prévue par le Code de la santé publique traduisent bien **la dimension de vulnérabilité inhérente à toute relation de confiance.** Le premier désigne le fait pour une personne *« de détourner, au préjudice d'autrui, des fonds, des valeurs ou un bien quelconque qui lui ont été remis et qu'elle a acceptés à charge de les rendre, de les repré-*

23. Michela Marzano, « Qu'est-ce que la confiance ? », *op. cit.*
24. Développée récemment en économie, la problématique des *« dispositifs de confiance »* permet de comprendre pourquoi des individus s'engagent dans un échange économique en minimisant les risques et en dépit de l'incertitude, de l'opacité et des tentations opportunistes. On doit à Lucien Karpik d'avoir distingué, dans un article publié en 1996 dans la revue *Sociologie du travail,* les *« dispositifs de jugement »* qui *« permettent de réduire l'ignorance sur la qualité des biens et des services, dans une économie dite "de la qualité", où l'on a le choix entre des biens de qualités différentes »* des *« dispositifs de promesse »* qui *« protègent de l'opportunisme des partenaires ».* Louis Quéré (« Les "dispositifs de confiance" dans l'espace public », *Réseaux*, 2005/4, n° 132, p. 185-217) étend ces réflexions aux institutions en formulant l'hypothèse selon laquelle il n'est possible de leur faire confiance que si sont levées l'opacité qui entoure l'exercice du pouvoir et le fonctionnement des institutions et l'incertitude qui concerne *« la conformité de l'institution à l'idée normative qui la constitue ».* Et, le sociologue d'ajouter, *« elles ne peuvent l'être que par des dispositifs qui œuvrent non seulement à l'information, mais aussi à l'enquête, à la critique et à la discussion publiques »*.
25. Nous empruntons cette formule à Éloi Laurent *(Économie de la confiance, op. cit.)*.
26. La loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, en transposant la directive européenne sur le commerce électronique, établit un droit français de l'Internet et pose des règles relatives au commerce électronique.
27. Parue au *Journal officiel* le 11 août 2018, la loi n° 2018-727 du 10 août 2018 pour un État au service d'une société de confiance, dite « loi ESSOC », vise en particulier à créer les *« conditions d'une confiance retrouvée du public dans l'administration »* et promouvoir une *« action publique modernisée, simple et efficace »*. C'est elle qui a instauré le principe du *« droit à l'erreur »*.
28. La loi n° 2019-791 du 26 juillet 2019 pour une école de la confiance, promulguée au *Journal officiel* le 28 juillet 2019, abaisse notamment l'instruction obligatoire de six à trois ans. Elle revoit également la formation des enseignants.
29. Dans son article premier, la loi n° 2021-1729 du 22 décembre 2021 pour la confiance dans l'institution judiciaire prévoit, par exemple, la possibilité d'enregistrer et de filmer des audiences civiles, pénales, économiques et administratives *« pour un motif d'intérêt public d'ordre pédagogique, informatif, culturel ou scientifique »*.
30. Éloi Laurent, *Économie de la confiance, op. cit*.
31. Roger C. Mayer *et al.,* "An integrative model of organizational trust", *Academy of Management Review,* 1995, vol. 20, p. 709-734.
32. Et Simmel de poursuivre : *« Celui qui ne sait rien ne peut raisonnablement même pas faire confiance ».* Ce qui le conduit à décrire la confiance comme *« un état intermédiaire entre le savoir et le non-savoir sur autrui »*. Voir notamment Georg Simmel, *Sociologie. Étude sur les formes de socialisation*, Paris, PUF, 1999.

senter ou d'en faire un usage déterminé[33] ». Quant à la seconde, elle peut être désignée par toute personne majeure et *« consultée au cas où [celle-ci] serait hors d'état d'exprimer sa volonté et de recevoir l'information nécessaire à cette fin*[34] ».

Or, comment ne pas craindre de devenir la victime de prochains abus quand on sait que, désormais, la moindre donnée informatique peut être détournée ? La Cour de cassation a ainsi confirmé, dans un arrêt daté du 22 octobre 2014, que le détournement d'un fichier informatique est susceptible de constituer un abus de confiance au sens de l'article 314-1 du Code pénal[35]. En revanche, bien malin sera celui ou celle qui parviendra à démasquer les personnes de confiance dans le cyberespace. Ici plus qu'ailleurs, le règne de l'anonymat a consacré la victoire des « trolls »… au détriment parfois de la liberté d'expression[36]. **Comme si finalement la montée en puissance des nouvelles technologies de l'information et de l'économie numérique avait fait monter d'un cran l'état d'incertitude sociale.**

Avec la digitalisation du monde, nous interagissons en effet davantage. Et ce, peu importe les distances spatio-temporelles. Mais surtout, *« nous interagissons davantage… avec des gens dans lesquels nous n'avons pas confiance (et peut-être même à l'égard desquels nous éprouvons de la défiance) qu'avec des gens dans lesquels nous avons confiance*[37] ». Ajoutez à cela la prolifération des objets connectés et vous obtenez un cocktail explosif. Balance numérique, lecteur de glycémie, moniteur cardiaque, pacemaker réglable à distance, etc. : **notre hyperconnectivité multiplie les points d'entrée et porte de fait notre vulnérabilité à son paroxysme.** La question de la cybersécurité est bien sûr transverse aux nouvelles technologies. Elle revêt, toutefois, une dimension critique quand elle concerne un domaine aussi sensible que celui de la santé. Cyber-attaques contre les infrastructures sanitaires, menaces, intrusions, piratages voire manipulations des données de santé : dans ce domaine aussi, toute la panoplie de la cybersécurité se décline. Preuve s'il en fallait encore une que ***« plus nos sociétés se numérisent, plus elles se vulnérabilisent »***, pour reprendre l'expression de Jean-Louis Gergorin.

Comment, après ce propos liminaire, concevoir encore que le numérique puisse participer d'une quelconque manière à la réinvention de la confiance ? C'est pourtant ce que pensent toutes les personnes interrogées dans le cadre de ce recueil. Pour elles, il ne fait aucun doute que le numérique influe considérablement sur la confiance. Si, à ce stade de nos réflexions, la vérification de l'hypothèse de la « confiance numérique » s'annonce encore audacieuse, voire périlleuse, elle devra, quoi qu'il en soit, prendre à bras le corps l'exigence

33. Code pénal, article 314-1, ordonnance n° 2000 du 19 septembre 2000, art. 3 du *Journal officiel* du 22 septembre 2000, entré en vigueur le 1er janvier 2002.
34. Code de la santé publique, article L. 1111-6, modifié par la loi n° 2005-370 du 22 avril 2005, art. 10 *Journal officiel* du 23 avril 2005.
35. Cass. Crim., 22 octobre 2014, n° de pourvoi 13-82.630. La Chambre criminelle de la Cour de cassation a rejeté le pourvoi d'un salarié d'un cabinet de courtage aux motifs que *« le prévenu a, en connaissance de cause, détourné en les dupliquant, pour son usage personnel, au préjudice de son employeur, des fichiers informatiques contenant des informations confidentielles et mis à sa disposition pour un usage professionnel, la Cour d'appel, qui a caractérisé en tous ses éléments, tant matériel qu'intentionnel, le délit d'abus de confiance, a justifié sa décision ».*
36. Sur les réseaux sociaux, dans les forums ou tout espace d'expression sur Internet, les « trolls » n'ont d'autre raison d'être que de générer des polémiques quel que soit le sujet de conversation en exacerbant notamment les divergences de points de vue et en créant, ce faisant, des dissensions au sein des groupes de discussion.
37. Russel Hardin, *Trust,* Cambridge, Polity Press, 2006.

posée par la coopération sociale. Car la confiance, Georg Simmel l'avait compris bien avant nous, est *« une des forces de synthèse les plus importantes au sein de la société*[38] *»*. Sans elle, *« la société tout entière se disloquerait*[39] *»*.

C'est sans doute d'ailleurs pour conjurer ce scénario catastrophe que l'économie du numérique, rebaptisée pour l'occasion « économie du partage », **invente ses propres *« dispositifs de confiance »***. Le modèle « DREAMS », conçu par les équipes de la plateforme communautaire payante de covoiturage française BlaBlaCar, décrit par exemple **les six piliers de la confiance en ligne.** Ainsi, pour construire sa confiance envers les autres utilisateurs de la plateforme de covoiturage, chaque membre doit avoir accès à des **informations « déclarées »** *(« declared »)*, comme le nom ou l'âge, **« notées »** *(« rated »)*, comme les avis reçus de la part d'autres utilisateurs, **« engagées »** *(« engaged »)*, ce que permet le paiement en ligne à l'avance, **« actives »** *(« active »)*, au travers de mentions telles *« vu aujourd'hui à 16 h 20 »* ou *« membre depuis 2018 »*, et enfin **« modérées »** *(« moderated »)* et **« sociales »** *(« social »)*. Le service modère les échanges et, quand cela est possible, les équipes vérifient les informations communiquées, informations qui peuvent être reliées à d'autres profils en ligne sur les réseaux sociaux[40].

Si le modèle DREAMS est spécifique à la licorne cofondée par Frédéric Mazzella, Nicolas Brusson et Francis Nappez, **chaque plateforme numérique s'est dotée de ses propres indicateurs de confiance.** Ainsi, eBay a promu un système d'évaluation par étoiles. Quant aux utilisateurs de Airbnb et de LinkedIn, ils peuvent se reposer respectivement sur les profils ou les recommandations professionnelles avant d'accepter une réservation ou une demande de connexion. Et le moins que l'on puisse dire, c'est que cela fonctionne. Qui aurait cru, il y a encore dix ans, que nous monterions à bord de la voiture du premier venu sans la moindre appréhension ou que nous ferions davantage confiance à de parfaits inconnus qu'à nos voisins d'*open space*[41] ?!

La technologie peut donc participer à réinventer la confiance. Son pari le plus disruptif ? Supprimer tout sentiment de défiance en s'attaquant paradoxalement aux tiers de confiance. La *blockchain*, nous le verrons, symbolise en effet pour certains l'avènement de ces nouvelles *« trust machines »* qui promettent de « distribuer la confiance[42] ». **Mais de la « confiance aveugle » à la « confiance trahie », il n'y a parfois qu'un pas, et c'est peu dire, que derrière la supposée réinvention de la confiance, nous pourrions être tentés de verser une fois encore dans l'illusion du progrès.**

38. Georg Simmel, *Sociologie, op. cit.*
39. Georg Simmel, *Philosophie de l'argent*, Paris, PUF, 1987. Et le sociologue de préciser : *« rares en effet sont les relations uniquement fondées sur ce que chacun sait de façon démontrable de l'autre, et rares celles qui dureraient un tant soit peu, si la foi n'était pas aussi forte, et souvent même plus forte, que les preuves rationnelles »*.
40. Voir notamment Frédéric Mazzella, Laure Claire Reillier, Benoît Reillier, *Mission BlaBlaCar. Les coulisses de la création d'un phénomène*, Paris, Eyrolles, 2022.
41. C'est en tout cas ce que suggère l'étude « Entering the Trust Age » (2016). Cette enquête, réalisée conjointement par BlaBlaCar et NYU Stern, l'école de commerce de l'Université de New York, a en effet montré qu'il était possible de créer, grâce au modèle DREAMS, une vraie confiance en ligne et entre des personnes ne s'étant pourtant jamais rencontrées. 88 % des personnes interrogées ont ainsi déclaré faire confiance à un autre membre BlaBlaCar ayant un profil complet. Un chiffre proche des 92 % qui font confiance à leurs amis et nettement supérieur aux 58 % qui font confiance à leurs collègues.
42. Voir notamment Serge Soudoplatoff, Yves Caseay, *La blockchain, ou la confiance distribuée*, Paris, Fondation pour l'innovation politique, 2016.

Aussi, la confiance numérique confirme-t-elle l'existence d'un double mouvement à l'œuvre dans les sociétés du XXIe siècle : ***« une confiance interpersonnelle de moins en moins nécessaire du fait de l'édification d'institutions qui permettent justement de s'en dispenser ; une défiance banalisée, car justifiée par la complexité sociale, le progrès technique et l'ouverture au monde »***[43]. Signe que **la confiance est moins en crise qu'en transition.** Une idée qui n'est pas sans rappeler l'*« état intermédiaire »* évoqué par Simmel ou celui d'une époque, la nôtre, en pleine transformation numérique. Personne ne sait, en revanche, combien de temps durera cette transition. Nul ne prédit non plus qu'elle ôtera tout risque. Ce serait sonner sinon le glas de la confiance numérique qui *« transforme l'incertitude en risque et accélère la réciprocité entre individus*[44] *»*.

En conclusion, **peut-on raisonnablement faire confiance à la confiance numérique ?** La confiance numérique ne saurait être sacralisée. Mais le numérique ne doit pas non plus susciter une méfiance disproportionnée. **L'idéal consisterait donc à trouver un juste milieu entre confiance aveugle et défiance totale… ce que suggère chacune des contributions à suivre.** Bien que toutes reposent sur des expertises différentes et des angles d'analyse très spécifiques, celles-ci résonnent les unes avec les autres. Elles se provoquent et se répondent. Entre les lignes, des discussions s'engagent et, surtout, se dégage l'enseignement principal de ces entretiens : ***la confiance numérique naît du lien mais « sa véritable force réside dans le fait que, même si elle demeure à jamais fragile, elle engendre toujours du lien***[45] ***»***.

43. Éloi Laurent, *Économie de la confiance, op. cit.*
44. Éloi Laurent, *L'impasse collaborative. Pour une véritable économie de la coopération*, Paris, Les Liens qui libèrent, 2018.
45. Michela Marzano, « Qu'est-ce que la confiance ? », *op. cit.*

Jean-Louis Gergorin

Ne pas faire confiance aveuglement au numérique : la menace souveraine du cyber

Jean-Louis Gergorin, maître des requêtes honoraire au Conseil d'État, est consultant en stratégie aérospatiale, défense et cyber, et chargé de cours à Sciences Po Paris.

Co-auteur de Cyber, La guerre permanente *(Éditions du Cerf, 2018), il est également co-fondateur et l'un des coordinateurs de la French American Cybersecurity Conference.*

Auparavant, il a notamment été vice-président exécutif chargé de la stratégie d'EADS (aujourd'hui Airbus) et co-fondateur puis chef du Centre d'analyse et de prévision au ministère français des Affaires étrangères.

Jean-Louis Gergorin est ancien élève de l'École Polytechnique, de l'ENA et du programme exécutif de la Stanford Business School.

Il y a une dimension géopolitique à la question de la confiance numérique : comment éviter des actions d'intrusion informatique ou de manipulation du contenu de l'information, souvent venues de l'étranger ? C'est là un enjeu majeur pour la souveraineté des démocraties. Mais cette question est encore trop peu prise en compte par les pouvoirs publics comme par les entreprises. Celles-ci seraient prudentes de ne pas accorder une confiance absolue à leurs stratégies de transformation numérique ou à celles de leurs sous-traitants en matière de cybersécurité.

La guerre a toujours su tirer parti des innovations technologiques. Il était donc prévisible que les technologies numériques n'échapperaient pas à ce destin. Pourtant, dans votre dernier ouvrage[46],* Cyber, La Guerre permanente*, vous distinguez le numérique des autres technologies qui l'ont précédé et le cyber des guerres « classiques ». Pourquoi le cyber n'est-il pas une guerre comme une autre ?

Je préfère parler de *« conflictualité dans l'espace numérique »* plutôt que de « cyber », pour ne pas risquer de réduire le cyber à la cyberguerre. À ce titre, il est frappant de remarquer que les Anglo-saxons ne parlent pas de *« cyberwar »* mais de *« cyberwarfare »*, autrement dit d'un mode de combat qui serait comme tapi dans l'ombre.

Ce qu'il faut comprendre, donc, c'est que le numérique signe l'avènement d'une nouvelle forme de conflictualité, située toujours en dessous du seuil de la guerre « ouverte ». Elle résonne beaucoup avec les mots de Carl von Clausewitz, le théoricien prussien de la guerre moderne, qui concevait cette dernière comme *« une simple*

46. Jean-Louis Gergorin, Léo Isaac-Dognin, *Cyber. La Guerre permanente*, Paris, Cerf, 2018.

continuation de la politique par d'autres moyens[47] ». Bien avant la naissance d'Internet, l'auteur de *De la guerre* avait conscience de l'existence d'un espace entre la guerre déclarée et la paix officielle, un espace qui trouve au travers du cyber un puissant moyen d'expression.

> « Avec le numérique, nous sommes entièrement entrés dans l'ère de la guerre en temps de paix. »

Avec le numérique, nous sommes entièrement entrés dans l'ère de la guerre en temps de paix. Son utilisation, à des fins d'influence ou de contrôle, représente un moyen alternatif de continuation de la politique, ce qu'ont parfaitement compris les Russes si l'on en croit la nouvelle stratégie de sécurité nationale signée en juillet 2021 par Vladimir Poutine[48]. Si ce texte entérine le fait que la confrontation avec l'Occident est appelée à durer, il accorde surtout une importance centrale à la « sécurité informationnelle ». Le texte se fait l'écho d'une analyse selon laquelle les nouvelles technologies de l'information seraient utilisées de manière croissante pour interférer dans les affaires intérieures russes. Aussi, la stratégie 2021 prévoit-elle toute une série de mesures qui, de la création d'un segment souverain d'Internet au développement systématique de technologies nationales, œuvrent toutes à se donner les moyens d'une « confrontation informationnelle »[49].

Mais une personne avait, bien avant l'heure de la confrontation informationnelle, senti que les choses étaient en train d'évoluer. Il s'agit de Valéri Guérassimov. Ce chef de l'État-Major de l'armée russe a publié en 2013, soit un an après sa nomination, un article dans lequel il explique que les règles de la guerre ont changé et ce, d'au moins deux façons[50]. Premièrement, dans les conflits contemporains, la phase la plus importante est désormais celle qui *précède* les hostilités elles-mêmes. Deuxièmement, au cours de cette phase initiale, la confrontation informationnelle offre de très larges possibilités de stratégie asymétrique pour celui qui attaque le premier[51]. Autrement dit, il existerait une sorte de prime à l'attaquant. Guérassimov recommande ainsi d'agir dans un secteur où l'on détient une supériorité écrasante sur son adversaire, celui-ci ne pouvant pas riposter sur le même terrain. Et, quand bien même il tenterait de le faire dans un autre domaine, il irait au-devant de sérieuses difficultés.

Le cyber crée donc, ou amplifie, un espace flou entre guerre et paix et, de fait, change les règles et les termes de la conflictualité. Mais introduit-il de nouveaux modes d'action ?

Les moyens numériques peuvent être divisés en deux grandes familles. D'une part, l'intrusion informatique, plus communément désignée sous l'appellation de *hacking*, c'est-à-dire le fait de pénétrer un ordinateur ou un système d'information dans le but de le détourner, de l'espionner ou de le détruire. D'autre part, la mani-

47. Carl von Clausewitz, *De la guerre*, Paris, Les Éditions de Minuit, 1955, p. 67.
Carl von Clausewitz (1780-1831), est un général et théoricien militaire prussien, considéré par Lénine comme *« l'un des plus grands, l'un des plus remarquables philosophes et historiens de la guerre »*. Officier prussien engagé dans l'armée à douze ans, il a combattu face aux troupes de la France révolutionnaire puis contre la Grande Armée de Napoléon lors de la campagne de Russie, avant de devenir directeur de l'École militaire de Berlin. Nourrie de philosophie allemande et de l'expérience du feu, sa pensée dialectique du conflit a inspiré les grands stratèges du XXe siècle.
48. On ne trouve pas de traduction anglaise de cette nouvelle édition de la stratégie de sécurité nationale. On se contentera donc de renvoyer au commentaire qu'en fait Dmitri Trenin pour le *Carnegie Moscow Center :*
https://carnegiemoscow.org/commentary/84893 [dernière consultation le 18 février 2022].
49. Les Russes ne parlent jamais de cyber mais de « confrontation informationnelle » *(information confrontation)* ce qui, pour eux, présente l'avantage de renvoyer tout à la fois au contenu et au contenant.
50. Originellement publié le 27 février 2013 dans la discrète revue *VPK* (acronyme de *Courrier du complexe militaro-industriel*), on trouve une traduction anglaise de cet article sur : https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160228_art008.pdf [dernière consultation le 18 février 2022].
51. Les Russes ne parlent jamais de cyber mais de « confrontation informationnelle » *(information confrontation)* ce qui, pour eux, présente l'avantage de renvoyer tout à la fois au contenu et au contenant.

pulation du contenu de l'information, au travers principalement des plateformes de médias ou des réseaux sociaux. Le numérique signe, en effet, l'avènement d'une nouvelle ère dans l'histoire de la manipulation. Désormais, des techniques permettent de produire des faux et, ce faisant, de transformer l'information. La plus célèbre de ces techniques est celle des *deep fakes*. À supposer, par exemple, qu'une banque d'images de moi-même ou de vous-même existe en ligne, il serait possible de faire une vidéo de cet entretien dans laquelle vos questions et mes réponses seraient complètement différentes.

Ces deux modes d'action peuvent être employés par des acteurs étatiques ou non, à des fins d'influence ou de contrôle, sur des personnes ou des populations, des organisations ou des entreprises. Ils sont très complémentaires l'un de l'autre et s'interpénètrent de plus en plus, comme en témoigne l'élection présidentielle américaine de 2016.

Selon le gouvernement et la justice américaine, des *hackers* russes, proches des services officiels du renseignement militaire russe, auraient alors piraté le système d'information du Comité national démocrate et l'ordinateur du directeur de campagne de Hillary Clinton. Les informations, authentiques, qui ont pu être recueillies ont été diffusées par Wikileaks et relayées simultanément par des comptes fictifs sur les réseaux sociaux.

Tous les sondages et analyses livrés par des politologues s'accordent pour dire que des millions d'Américains ont été touchés par les messages qui provenaient de ces faux comptes créés depuis Saint-Pétersbourg. Ces informations, qui, j'insiste, étaient authentiques, ont eu un effet dévastateur. Le parti démocrate a dû non seulement faire face au *hacking* de son système d'information mais surtout rendre des comptes. En effet, l'électorat ouvrier n'a pas particulièrement apprécié la dissonance entre les discours prononcés à leur attention par Hillary Clinton et celui tenu devant les dirigeants de Goldman Sachs… Cet incident a incontestablement contribué à la victoire de Donald Trump.

En parlant de Donald Trump, son gouvernement n'a cessé, au cours de son mandat, de minimiser la cybermenace russe. Nombreux sont pourtant les indicateurs qui donnent à penser que la Russie représente plus que jamais un grand danger pour le processus démocratique des États-Unis, comme pour d'autres pays[52]. Comment expliquer cette « supériorité » russe ?

> « Sur le plan technologique, plus on se numérise, plus on se vulnérabilise. »

Sur le plan technologique, par définition, plus on se numérise, plus on se vulnérabilise. Or, nous vivons dans une société où la transformation numérique est devenue une véritable obsession, des entreprises jusqu'au sommet de l'État. Quel est le rôle de Cédric O, parfaitement assumé, sinon celui d'être le *chief digital transformation officer* du gouvernement ?!

C'est comme si le piège se refermait sur nous. Une impression partagée par le général américain Paul M. Nakasone, qui dirige depuis mai 2018 la *National Security Agency* (NSA) et le *United States Cyber*

52. On soupçonne le groupe de hackers *« Fancy Bear »* (« ours raffiné » en français), plus connu des services de renseignement sous le code APT28, d'être non seulement responsable de l'attaque contre Hillary Clinton mais aussi d'avoir infiltré la campagne d'Emmanuel Macron en 2017. Dans un rapport, des experts du géant Microsoft avaient identifié 200 attaques sur Emmanuel Macron, provenant de Russie mais également de Chine ou d'Iran. La singularité d'APT28 ? Son objectif plus destructeur, puisque le groupe de hackers russes, contrairement à ses homologues chinois ou iraniens, vise à déstabiliser les pays qu'il cible.

Command[53]. Selon lui, lorsque les États-Unis ou l'Europe envisagent de riposter à une cyberattaque, les gouvernements n'ont d'autre choix que de tenir compte du fait qu'ils offrent beaucoup plus de cibles à l'adversaire qu'ils n'en ont à viser chez lui… Les Russes, eux aussi, se numérisent bien sûr. Mais ils le font beaucoup moins et beaucoup moins vite que la Chine ou les États-Unis par exemple. Ainsi, si le rapport de force entre la Chine et les États-Unis tend à se rééquilibrer, on ne peut pas en dire autant avec la Russie. Le pays de Vladimir Poutine conserve, en matière de numérisation globale de la société et de l'économie, son retard… et donc sa supériorité !

Néanmoins, les Américains ont quelque peu changé de stratégie quand ils ont découvert, en 2019, des implants logiciels[54] dans des centrales électriques et des gazoducs répartis sur leur territoire. Le *Cyber Command* de l'armée américaine a alors décidé de passer à l'offensive en implantant à son tour des logiciels malveillants dans le réseau électrique de la Russie. Et lancer un avertissement n'était pas le seul but de la manœuvre. Il s'agissait aussi de préparer des cyberattaques paralysantes en cas de conflit avec la Russie[55], objectif symétrique à celui des Russes dans leurs déploiements d'implants.

En revanche, en réaction à ces implants, la France n'a jamais doctrinalement envisagé de passer à l'offensive. En juin 2020, *L'Express* révélait ainsi qu'un *malware*, un logiciel malveillant, avait été détecté début 2018 dans une ferme éolienne française[56]. Cette dernière, en réalité, ne représentait qu'une porte d'entrée, une « porte dérobée » ou *backdoor* en anglais, devant permettre au logiciel malveillant de pénétrer, en fait, dans le réseau de distribution électrique géré par Enedis. L'attaque a fini par échouer. Mais elle n'en visait pas moins une infrastructure civile critique. Ce sont les services techniques de la Direction Générale de la Sécurité Extérieure (DGSE) qui ont réussi à identifier la main invisible derrière l'intrusion : un groupe de hackers russes baptisé *« Cozy Bear »* et connu pour être proche du Service fédéral de sécurité, le fameux FSB, successeur du KGB…

Contrairement aux États-Unis, la France opte pour la désescalade en choisissant ici de ne pas médiatiser l'affaire ou en préférant la voie diplomatique, comme ce fut le cas début 2018 lorsque l'Ambassade de France à Moscou a subi une intrusion informatique. Le président de la République, Emmanuel Macron, avait alors choisi d'évoquer ces questions avec Vladimir Poutine en marge de sa participation au Forum de Saint-Pétersbourg en mai 2018. Il en résulta l'établissement d'un dialogue périodique entre responsables de la cybersécurité des deux pays qui a permis une meilleure compréhension mutuelle mais n'a pas encore, semble-t-il, réduit les flux d'implants déposés dans les infrastructures critiques françaises…

53. Découverte par le grand public à l'occasion des révélations du lanceur d'alerte Edward Snowden en 2013, la NSA (en français « Agence nationale de la sécurité ») remplit des missions de renseignement et assure la sécurité des systèmes de communications et de traitement des données. Quant au USCYBERCOM, il est l'un des onze commandements interarmées de combat des forces armées des États-Unis, chargé tout particulièrement de la sécurité de l'information pour le Département de la Défense.
54. Une fois implantés, ces logiciels peuvent être ultérieurement activés pour mettre hors service ou perturber des structures critiques. Le plus souvent utilisés lors d'attaques de type rançongiciel, le procédé est de plus en plus exploité par des États. Les rançongiciels (en anglais *ransomwares*) désignent les intrusions informatiques qui visent à obtenir des rançons en bloquant les données d'un système.
55. David E. Sanger, Nicole Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid", *The New York Times*, 15 juin 2019, disponible en ligne : https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html?searchResultPosition=1 [dernière consultation le 18 février 2022].
56. Emmanuel Paquette, « Entre Moscou et Paris, la cyberguerre est déclarée », *L'Express,* 23 juin 2020, disponible en ligne : https://lentreprise.lexpress.fr/high-tech-innovation/entre-moscou-et-paris-la-cyberguerre-est-declaree_2128786.html [dernière consultation le 18 février 2022].

Faut-il comprendre que, si nous n'agissons pas plus vigoureusement, c'est simplement par pragmatisme ?

Je suis convaincu que les implants russes sont faits pour être partiellement trouvés à des fins d'intimidation, et non pas seulement pour se « prépositionner[57] » afin d'être activés en période de confrontation. Les implants présentent en cela de fortes ressemblances avec l'espionnage. Comme celui-ci, ils demeurent sous le seuil de la guerre ouverte et garantissent l'anonymat. Mais à la différence de l'espionnage, avec le cyber, l'accès est instantané et aucun agent n'a besoin de prendre de risque physique sur le terrain.

> « La France en regorge, mais la doctrine enjoint de « cacher cet implant que je ne saurais voir ». »

Il n'en demeure pas moins qu'il faut se garder d'être naïfs. La France regorge d'implants mais la ligne politique semble être de *« cacher cet implant que je ne saurais voir »*. Cette politique de l'autruche a l'avantage de nous déculpabiliser. Car si, dans l'affaire Enedis, on a renoncé à riposter, c'est aussi et surtout parce que l'on n'a pas de réponse à apporter !

Tarder à prendre conscience de l'existence et de la gravité d'une nouvelle menace peut, néanmoins, nous coûter très cher, comme le montre dans un autre domaine celui de la guerre informationnelle au Mali. L'opinion publique l'ignore encore, mais c'est en grande partie pour des raisons de guerre d'influence que nos troupes se sont fait éjecter du Mali. Bien sûr, officiellement, ce n'est pas le terme qui est employé pour qualifier ce retrait des troupes françaises de Tombouctou à la mi-décembre 2021, après avoir quitté les bases de Kidal et Tessalit. Ce redéploiement obligé s'explique sans doute à la lumière d'une inefficacité tactique et, dans ce dossier, nous avons commis tout un tas d'erreurs. Nous n'avons pas su écouter les populations sur place ni faire preuve de fermeté à l'égard des dirigeants corrompus.

Mais l'image française dégradée a précipité cette reconfiguration. Nous avons compris trop tard le rôle et l'influence des équipes russophones qui ont propagé et créé des réseaux de propagation de fausses informations. La bataille informationnelle continue de faire rage au Mali. Elle vise ni plus ni moins à décrédibiliser l'action de l'armée française et à donner le sentiment qu'il s'agit d'une armée d'occupation, et non plus d'une armée régulièrement appelée par les autorités locales dans le cadre d'accords de défense.

Est-ce à dire que nous devons perdre toute confiance dans notre capacité d'adaptation, face à la démultiplication des implants ou au développement de la cybercriminalité ?

Il ne faut pas sous-estimer l'effort constant depuis 14 ans ! Le « Livre Blanc sur la défense et la sécurité nationale » présenté le 17 juin de 2008 par Nicolas Sarkozy, alors président de la République, a été le premier à faire du cyber un enjeu majeur. Trois mesures ont été prises dans la foulée. L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) a été créée en 2009[58]. Ce « Livre Blanc » a également reconnu comme

57. C'est en tout cas ce que le directeur général de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), Guillaume Poupard, confiait à Hedwige Chevrillon dans le *Journal de l'éco* de BFM TV en date du 11 janvier 2021, disponible en ligne : https://youtu.be/zZH8FQHMuz8 [dernière consultation le 18 février 2022]. Stratégies de cybercoercition par excellence, les stratégies de prépositionnement consistent très concrètement à positionner des implants sur des infrastructures critiques. Il s'agit ni plus ni moins d'un avertissement, d'une mise en garde : toute attaque contre les intérêts ciblés se paiera *cash*. Les acteurs, pour la plupart étatiques car cela suppose des moyens techniques importants, se rendront coup pour coup.
58. Par le décret n° 2009-834 du 7 juillet 2009.

fonction stratégique le renseignement. Enfin, en mai 2017, a été mis sur pied le commandement de la cyberdéfense, devenu depuis un commandement opérationnel, le COMCYBER.

Je pense que, après une période de confiance un peu naïve dans la transformation numérique qui a sous-estimé la dimension sécurisation, nous sommes sur la bonne voie, en témoigne l'effort récent consenti sur le renseignement. En 2021, dans le cadre de la Loi de programmation militaire 2019-2025, la DGSE s'est vu attribuer un budget de 880 millions d'euros, contre 816 millions d'euros en 2020, soit une augmentation de 7,8 %. Ces moyens supplémentaires vont permettre d'accompagner pleinement le passage à une approche cyber centrée aussi sur la capacité contre-offensive et non plus seulement sur la défense[59].

Par ailleurs, le 20 octobre dernier, en réaction aux campagnes informationnelles préjudiciables à la force Barkhane, la ministre des Armées, Florence Parly, a dévoilé les grandes lignes de la nouvelle doctrine française de lutte informatique informationnelle. Celle-ci prévoit de confier ces nouvelles actions à des unités militaires spécialisées du Centre Interarmées des Actions sur l'Environnement (CIAE), placées sous le contrôle du COMCYBER. Déjà expérimentées en matière de lutte contre la propagande terroriste, elles vont ainsi élargir leur spectre de compétences pour lutter contre les manipulations de l'information sur les théâtres d'opération, en s'inspirant notamment des unités de veille et d'action numérique américaines, les « WebOps[60] ».

Il y a donc eu des changements majeurs en France, mais nous continuons encore trop souvent de dissocier ce qui relève de la protection des actions de renseignement, d'une part, et de la contre-attaque militaire, de l'autre. La doctrine française ne prévoit actuellement de riposte qu'en en cas d'attaques visant des cibles militaires mais est muette en ce qui concerne les infrastructures civiles critiques.

> « La doctrine française actuelle ne prévoit pas de riposte en cas d'attaques visant des infrastructures civiles critiques. »

Faut-il autoriser le « hack back », c'est-à-dire accorder un droit de riposte aux entreprises en cas de cyberattaque ?

Le faire serait catastrophique. La tentation existe cependant aux États-Unis. Deux propositions de loi visant à dépénaliser les intrusions dans des systèmes informatiques en réponse à des attaques ont déjà été déposées par le Représentant Tom Graves. Son idée ? Autoriser les entreprises à s'introduire dans les systèmes des hackers pour stopper l'attaque et récupérer les données dérobées. Mais certains grands groupes américains n'ont même pas attendu l'onction législative. Des structures offensives ont été créées dans des pays peu regardants comme Dubaï ou Abu Dhabi. Très souvent, ce sont des anciens de la NSA qui conçoivent et fournissent ces services de *hacking*. Ces tentatives visent ni plus ni moins à retranscrire dans le domaine cyber l'esprit du deuxième amendement de la Constitution des États-Unis qui donne à chaque Américain le droit d'avoir des armes à feu et a abouti aux drames que l'on sait…

59. Dans son discours prononcé le 22 janvier 2019, à l'occasion du Forum international de la cybersécurité, Florence Parly indiquait ainsi vouloir *« intégrer l'arme cyber à tous nos programmes »*. Son discours est accessible en ligne : https://www.vie-publique.fr/discours/269260-florence-parly-22012019-cyberdefense [dernière consultation le 18 février 2022].
60. Cette lutte informatique informationnelle (« L2I ») n'est pas propre à notre pays, les armées la pratiquent en réalité depuis le milieu des années 2010. Mais, à l'inverse de la plupart de ses alliés, la France a fait le choix de communiquer sur ce sujet. Voir notamment le discours de Florence Parly, prononcé le 20 octobre 2021, à l'occasion de la présentation de la doctrine militaire de lutte informatique d'influence : https://www.defense.gouv.fr/salle-de-presse/discours/discours-de-florence-parly/discours-de-florence-parly-ministre-des-armees-a-l-occasion-de-la-presentation-de-la-doctrine-militaire-de-lutte-informatique-d-influence-le-20-octobre-2022 [dernière consultation le 18 février 2022].

Je pense que, dans le domaine cyber comme dans celui des agressions militaires ou criminelles, les États doivent conserver le monopole de la force et de la riposte. Mais, pour riposter, il faut savoir qui est l'agresseur. Or, dans le domaine cyber, l'attribution demeure la principale difficulté. En plus de l'efficacité des hackers pour couvrir leurs traces, le réseau Internet lui-même n'a pas été conçu pour tracer les échanges. Le web forme une zone d'échanges ouverts, libres et anonymes. Loin de lui l'objectif de mettre en contact des numéros et des personnes identifiées, comme le ferait par exemple un réseau téléphonique traditionnel.

> « Les États doivent conserver le monopole de la riposte. »

Or, cette capacité d'attribution constitue un facteur clef de la hiérarchie des puissances. Les Américains possèdent, en la matière, un excellent niveau et il y a de fortes raisons de penser que les Russes s'en rapprochent. Elle fait figure de priorité pour les Européens qui veulent rester maîtres de leur sécurité.

Quel pourrait être précisément le juste périmètre et le contenu concret d'une politique de la souveraineté numérique européenne qui soit réaliste et efficace ?

Comment rêver à une potentielle souveraineté européenne quand l'Allemagne est dans une situation de dépendance stratégique à l'égard des États-Unis, de dépendance énergétique à l'égard de la Russie, de dépendance commerciale à l'égard de la Chine ? Les Allemands sont – ou plutôt étaient jusqu'à tout récemment – comme ligotés de toute part et, en plus, rien ne dit qu'ils désirent vraiment voir advenir cette souveraineté numérique.

Il existe, en fait, une « échelle » pour estimer où en sont les pays européens en termes de cybersécurité. Les Allemands se situent tout en bas de l'échelle, comme nous avons pu le constater au printemps 2018. La ministre de la Défense de l'époque avait alors annoncé le lancement d'une agence pour l'innovation dans le domaine de la cybersécurité dotée d'un budget initial de 350 millions d'euros. Près de quatre ans plus tard, cette agence n'existe toujours pas… Pourquoi ? Parce que le Parti social-démocrate avait posé une condition à sa création : le directeur de l'agence ainsi que son autorité de tutelle, à savoir le ministre de l'Intérieur, devaient garantir que les outils employés ne pouvaient en aucun cas entraîner des conséquences létales… Ce qui, vous en conviendrez, est impossible !

Les Allemands sont certes prêts à participer aux actions américaines si le « seuil de la guerre ouverte » prévu par l'OTAN est dépassé. Mais cela ne risque pas non plus d'arriver puisque, avec la conflictualité numérique, tout se joue précisément en dessous de ce seuil ! L'OTAN a prévu qu'en cas d'une multiplication des attaques sur des infrastructures « critiques » le seuil pouvait être considéré comme atteint. Cependant, le principe d'unanimité qui prévaut à l'échelle européenne limite drastiquement les chances que cette considération surgisse un jour et ce, même en cas d'attaques multiples.

Certains Européens ont pourtant réussi à développer des compétences très poussées, à l'image des Hollandais qui sont les plus équipés et les plus offensifs. Ils ont même réalisé de très belles opérations, en rentrant notamment dans le groupe de hackers russes *« Cozy Bear »*, ce qui leur a permis d'obtenir des informations relatives à des attaques imminentes sur les États-Unis et de prévenir les autorités américaines.

On doit néanmoins aux Allemands d'avoir initié les discussions autour de la « boussole stratégique » qui vise à définir les grandes lignes d'une feuille de route vers une Europe plus souveraine. Et, dans son discours du 9 décembre 2021, Emmanuel Macron a réaffirmé son souhait de la voir aboutir, d'une manière concrète, sous la présidence française de l'Union européenne de janvier à juillet 2022.

Sans surprise, dans ce discours de présentation de la présidence française du conseil de l'Union européenne, le président de la République a salué le combat de l'Europe en faveur de la protection des données individuelles. Il a évoqué également l'accord international sur la taxation des multinationales et les deux textes sur lesquels va se concentrer la présidence française, à savoir l'acte pour le marché numérique et l'acte pour les services numériques[61].

Mais si Emmanuel Macron a souligné l'importance pour les Européens de définir *« une organisation commune sur les nouveaux espaces de conflictualité que sont l'espace maritime, le spatial et le cyber »*, il n'a eu alors aucun mot pour la problématique des *ransomwares*[62].

On s'inquiète à longueur de journée des menaces que feraient peser les GAFAM (Google, Apple, Facebook, Amazon et Microsoft) sur la souveraineté numérique des pays européens. On s'insurge de la décision du gouvernement français d'héberger le *Health Data Hub* (Plateforme des données de santé)[63] dans les serveurs de Microsoft. En revanche, personne ne s'émeut du fait que, toutes les semaines, des infrastructures françaises sont attaquées par des rançongiciels ou que notre pays est régulièrement imbibé d'implants. Cela ne toucherait pas la fameuse « souveraineté numérique », vraiment ?

> « Arrêtons de considérer que les violations quotidiennes à coups de *ransomwares* ou de logiciels malveillants ne relèvent pas de la souveraineté numérique ! »

Arrêtons de considérer que les violations quotidiennes à coups de *ransomwares* ou de logiciels malveillants ne relèvent pas de cette souveraineté numérique ! Que dirait-on si des commandos étrangers attaquaient nos entreprises ? C'est pourtant ce qui se produit continûment en cyber, même si ce n'est pas au travers de commandos humains.

Justement quel est l'état de la menace cyber qui pèse aujourd'hui sur les entreprises ?

Entre 2017 et 2019, en France et en Europe occidentale, le nombre de *ransomwares* a été multiplié par quatre. Et l'on a assisté à une nouvelle multiplication par quatre lors des deux dernières années – et ces chiffres ne correspondent qu'aux attaques connues, ils ne prennent pas en compte les rançons payées. C'est spectaculaire et les sommes en jeu sont importantes. Aux États-Unis, les *ransomwares* auraient rapporté 150 millions de dollars en six ans… Sans parler des dégâts qu'ils causent et qui sont considérables. C'est d'autant plus inquiétant que notre capacité de détection est limitée. Une partie d'entre eux reste donc nécessairement inconnue.

Il y a de cela sept ou huit ans, on estimait ainsi qu'identifier une attaque pouvait prendre jusqu'à six mois. C'est précisément ce qui s'est produit pour SolarWinds. Le nom de cette entreprise américaine ne vous dit peut-

61. Comme le rappelle Emmanuel Macron dans son discours du 9 décembre 2021, l'acte pour le marché numérique ou DMA *« vise à éviter que les géants du numérique deviennent des monopoles sans règles et tuent cet esprit d'innovation qui, hier, leur a permis d'émerger »*. Le second texte discuté avec le Parlement européen, c'est l'acte pour les services numériques. Le DSA a pour objectif d'établir *« un régime de responsabilité des grandes plateformes au titre des produits qu'elles vendent et surtout des contenus qu'elles diffusent »*. Il est possible de consulter le texte du discours du président de la République en ligne : https://www.elysee.fr/front/pdf/elysee-module-18912-fr.pdf [dernière consultation le 18 février 2022].
62. Les *ransonwares* ou rançongiciels désignent les intrusions informatiques qui visent à obtenir des rançons en bloquant les données d'un système.
63. Projet de centralisation de plusieurs bases de données médicales françaises à des fins de recherche créé en 2019 créé à la suite de la remise du rapport du député Cédric Villani sur l'intelligence artificielle en 2018. Celui-ci recommandait la création d'une plateforme *« adaptée aux usages liés à l'IA »* où seraient rassemblés de larges pans des bases de données de santé françaises, très riches, mais difficiles à exploiter par des algorithmes d'intelligence artificielle.

être rien. Mais cet éditeur de logiciels de gestion informatique et d'outils de surveillance à distance a fait l'objet d'une attaque lancée par des pirates en mars 2020 et découverte seulement en décembre de la même année.

Le cas de SolarWinds est révélateur de la menace la plus pernicieuse qui pèse, selon moi, sur les entreprises. Dans cette attaque, comme dans celle ciblant Enedis, les pirates ont visé la chaîne logistique de l'entreprise américaine à l'aide d'une « porte dérobée ». Grâce à cette fonctionnalité cachée, les hackers ont pu installer des logiciels malveillants et mener à bien leurs opérations d'espionnage. En tout, ce sont près de 18 000 clients et une centaine de sociétés qui auraient été affectés. Parmi eux, de nombreuses agences gouvernementales et des entreprises faisant partie des 500 plus grandes compagnies américaines en termes de chiffre d'affaires.

Par-delà l'exemple de SolarWinds, les grands groupes ont la fâcheuse tendance de nourrir une confiance aveugle à l'égard des stratégies de cybersécurité de leurs sous-traitants. Or, très souvent, ceux-ci n'ont pas les moyens de se protéger.

Que pourraient-ils faire pour y remédier et restaurer un minimum de confiance numérique ?

Il s'agirait déjà de changer la manière de concevoir la cybersécurité. Cette dernière, en effet, ne saurait se résumer à cocher des cases, à imposer aux sous-traitants de respecter certaines normes. C'est une condition nécessaire mais non suffisante. Pourtant, on se contente encore trop souvent de ce contrôle purement administratif, en témoigne l'affaire SolarWinds. Les logiciels étaient parfaitement certifiés, ils remplissaient tous les critères de qualité et de sécurité imposés. Mais, il a suffi d'introduire un seul virus pour que tout s'emballe…

Ensuite, il me semble vital que les grands groupes prennent conscience de leur vulnérabilité du fait de sous-traitants vulnérables. À l'instar de Bernard Gavgani, le directeur des systèmes d'information de BNP-Paribas, je plaide pour que les entreprises se prennent en main et s'organisent collectivement[64]. Ces entreprises devraient ainsi pouvoir partager avec prestataires et clients leurs bonnes pratiques et leurs expériences en la matière. Elles pourraient également constituer, à partir de leurs équipes d'experts, un soutien aux entreprises de leur secteur en proie à de graves attaques. Pourquoi ne pas imaginer que les capacités d'experts d'un même domaine d'activité se fédèrent en une capacité nationale ? En cas de cyberattaques simultanées au sein du secteur concerné, celle-ci serait mise à la disposition de l'ANSSI.

> « Il me semble vital que les grands groupes prennent conscience de leur vulnérabilité du fait de sous-traitants vulnérables. »

Pour ma part, je souhaiterais voir créer une association d'utilisateurs ou de firmes de cybersécurité comme il en existe déjà aux États-Unis. L'idée serait de faciliter et de fluidifier le partage d'informations sur les menaces cyber. Je vois d'un œil très favorable la création d'une Réserve Citoyenne de Cyberdéfense (RCC) qui est constituée de volontaires agréés auprès des autorités militaires du fait de leurs compétences, de leur expérience et/ou de leur intérêt pour les questions relevant de la défense nationale. Mais son rôle se limite à mener des actions d'information et de sensibilisation aux enjeux de cyberdéfense. Elle n'intervient pas en cas de cyberattaque de grande ampleur. On pourrait envisager, au contraire, de créer une réserve nationale de tous les intervenants et experts cyber en entreprise qui pourrait se mobiliser en cas de situation critique.

64. Nicolas Barotte, « Face à la menace cyber, les entreprises doivent s'organiser. Entretien croisé entre Bernard Gavgani et Jean-Louis Gergorin », *Le Figaro*, lundi 25 octobre 2021, disponible en ligne : https://www.lefigaro.fr/international/bernard-gavgani-et-jean-louis-gergorin-face-a-la-menace-cyber-les-entreprises-doivent-s-organiser-20211024 [dernière consultation le 18 février 2022].

Vous plaidez également pour la création d'un coordinateur national cyber. Quel serait précisément son rôle ?

Ce coordinateur national cyber devrait être placé au sein de la Présidence et, afin de pallier le risque d'être déconnecté de l'interministériel, il faudrait s'assurer qu'il puisse avoir, dans sa mission et dans la mise en œuvre de celle-ci, une interaction positive avec le secrétaire général de la défense et de la sécurité nationale chargé de la coordination interministérielle, qui a sous son autorité l'ANSSI et l'agence de lutte contre les manipulations numériques étrangères VIGINUM. Il aurait pour rôle de conseiller le président de la République mais assorti d'une mission d'alerte et d'impulsion. C'est lui qui, par exemple, pourrait inciter à une action prioritaire contre ces dangers immédiats que sont les *ransomwares*.

De manière plus générale, je regrette qu'il n'y ait pas davantage de coopération et de coordination entre l'État et les entreprises. Prenons le *National Cyber Security Center*, l'équivalent britannique de l'ANSSI. Cette autorité fait partie du service de renseignement britannique. Mais cela ne l'empêche pas de communiquer amplement avec les entreprises dès qu'elle a connaissance d'une difficulté, d'une information sur l'imminence d'une attaque. Chez nous, rien de tel ne se produit. Quand l'ANSSI est au courant de quelque chose c'est parce qu'elle a été prévenue par les Britanniques. Et l'information n'est pas partagée avec les entreprises puisqu'elle est immédiatement classifiée. Notre système est trop cloisonné. Certes, des synergies interministérielles existent et fonctionnent plutôt bien. Mais les entreprises en sont encore complètement exclues.

> « Des synergies [entre État et entreprises] dépendent aussi notre souveraineté et, plus généralement, le climat de confiance à l'heure du numérique et des menaces cyber. »

Cela en dit long sur la confiance absolue que l'on voue aux autorités en matière de cybersécurité. On attend encore trop de l'État. On se contente de vérifier que tous les boulons sont bien serrés et, en cas d'attaque, on attend patiemment que les pompiers de l'ANSSI viennent sauver nos entreprises. Il faut vraiment que l'on se donne les moyens d'être en capacité de mobiliser au-delà des forces de l'ANSSI. C'est crucial face à la démultiplication des *ransonwares*. De ces synergies dépendent aussi notre souveraineté et, plus généralement, le climat de confiance à l'heure du numérique et des menaces cyber.

Quel est le rôle des moyens numériques dans la guerre déclenchée par la Russie contre l'Ukraine ?

L'escalade des pressions russes sur l'Ukraine en janvier 2022 s'est manifestée par une campagne massive d'attaques par dénis de service (aussi appelées « DDoS », ces attaques mettent hors service les serveurs, services ou infrastructures) le 14 janvier, submergeant un grand nombre de sites officiels ukrainiens. Cet assaut s'est accompagné d'actions de *defacing*, ou défacement, c'est-à-dire le remplacement de leurs pages d'accueil par des textes provocateurs.

Le même jour, le FSB lançait, principalement à Moscou, des raids, filmés puis diffusés médiatiquement, d'arrestations de membres du groupe de *ransomware* REvil « à la demande des autorités américaines ». Après une éclipse temporaire, ce groupe cybercriminel russe, identifié par le FBI comme responsable de l'attaque majeure contre le prestataire américain de logiciels de supervision informatique Kaseya en juillet 2021, avait repris ses attaques par *ransomware* contre des cibles américaines en septembre avant d'être techniquement démantelé le 21 octobre par une opération de grande ampleur menée conjointement par le *Cyber Command* et le FBI – officieusement annoncée par un article Reuters, pas plus démentie à Moscou qu'à Washington.

La simultanéité du raid FSB contre REvil et des cyberattaques contre les sites officiels ukrainiens a été généralement interprétée comme un message des autorités russes qu'elles pouvaient aussi bien neutraliser que libérer de toutes restrictions les groupes de *ransomware* si les États-Unis ripostaient numériquement aux cyberattaques subies par l'Ukraine. Le lendemain, 15 janvier 2022, le Microsoft Security Blog révélait que l'attaque visible de la veille dissimulait une dissémination massive dans les infrastructures ukrainiennes de malgiciels de type WIPER, activés ou seulement implantés, ayant la capacité d'effacer totalement les données des systèmes ainsi infectés. Ces attaques de type WIPER visant de multiples sites critiques ukrainiens sont devenues quasi permanentes depuis le 23 février, veille du déclenchement de l'offensive russe, avec une capacité notable des Ukrainiens à se cyberdéfendre assez efficacement.

Parallèlement, un certain nombre de groupes russes de *ransomware* annonçaient leur soutien à l'offensive de leur pays, confirmant ainsi publiquement leur rôle de corsaires de leur nation… Conti, l'un des principaux d'entre eux, subissait alors une scission de ses membres ukrainiens, provoquant des fuites très utiles pour la compréhension du fonctionnement de ce groupe. En face, une mobilisation mondiale de groupes cyber activistes, à commencer par Anonymous – le plus important d'entre eux –, appelait à attaquer les sites gouvernementaux russes.

Dans le même temps, un affrontement informationnel sans précédent se produit sur les réseaux sociaux, amenant Facebook, Twitter et YouTube à fermer des séries de comptes opérant sous de fausses identités et faux drapeaux. Le *think tank* genevois CyberPeace Institute, dirigé par Stéphane Duguin (ancien haut responsable français de l'agence de l'UE pour la coopération des services répressifs Europol), publie régulièrement sur son site web un recensement de ces cyber affrontements liés à la guerre russe contre l'Ukraine.

Frédéric Filloux

Restaurer la confiance dans les médias : la démocratie délibérative à l'épreuve du numérique

Frédéric Filloux est journaliste économique. Il collabore régulièrement à L'Express *comme chroniqueur et enquêteur.*

Auparavant, il a été directeur des activités numériques aux Échos*, responsable de projets au groupe de presse norvégien Schibsted et avant directeur de la rédaction de* 20 Minutes*. Frédéric Filloux a aussi passé douze ans à* Libération *comme journaliste économique, correspondant à l'étranger, et enfin directeur de la rédaction.*

Il a passé sept ans aux États-Unis, d'abord comme correspondant à New York, puis en 2016-2018 comme chercheur invité à l'Université de Stanford où il a travaillé sur un projet d'intelligence artificielle consacré à l'information.

En 2007, il a créé la lettre d'information « Monday Note » sur l'économie des médias numériques, complétée en 2020 par une version française intitulée « Episodiqu.es ».

Frédéric Filloux a enseigné pendant plus de dix ans à l'École de Journalisme et au département media studies de Sciences Po. Il est administrateur de Reporters Sans Frontières.

Le numérique a bouleversé notre manière de nous informer tout en diluant les piliers fondamentaux de la confiance dans les médias et en multipliant les risques de désinformation. Pour que l'information vérifiée et de confiance ne soit pas accessible qu'à une minorité de la population, il apparaît urgent de renouer avec une forme de traçabilité et une certaine qualité de l'information, seules à même de préserver et d'encourager la démocratie.

En cette année d'élection présidentielle, la confiance des Français envers les médias n'a jamais été aussi faible. Même la radio, qui bénéficiait encore d'une crédibilité de 52 % en 2021, a perdu 3 points de crédibilité pour se retrouver au même niveau que la presse écrite (49 %). Et la confiance envers Internet (24 %) renoue avec ses plus bas niveaux historiques[65].

Comment expliquer que la défiance reste aussi forte et ce alors même que près de neuf Français sur dix (88 %) jugent important que la population s'intéresse à l'actualité pour le bon fonctionnement de la démocratie ?

Ce baromètre se veut être le miroir d'un microcosme constitué principalement de médias linéaires comme la presse écrite, la télévision, la radio et, il faut bien le dire, plébiscités par une audience largement vieillissante.

65. L'édition 2022 du baromètre *La Croix*/Kantar Public, à laquelle s'est joint cette année Onepoint, a été menée du 5 au 11 janvier 2022, sur un échantillon national de 1 016 personnes, représentatif de l'ensemble de la population française âgée de 18 ans et plus. Les interviews réalisées l'ont été en face-à-face au domicile des personnes interrogées.

Il ne tient donc pas compte de la « délinéarisation » de la consommation média, autrement dit du passage à une consommation qui rompt avec le direct comme le permettent, par exemple, le *replay* ou la vidéo à la demande. J'ai donc du mal à penser que ces éléments soient significatifs.

Deux chiffres retiennent, cependant, mon attention. Si l'on en croit le *Baromètre*, 61 % des Français jugent essentiel que *« les médias leurs fournissent des informations fiables et vérifiées »*, mais c'est une réalité pour seulement 44 % d'entre eux… Cet écart renforce ma crainte de voir l'information de qualité se verticaliser peu à peu, au point de devenir l'apanage de gens éduqués, âgés et aisés financièrement. En somme, bientôt, c'est une élite âgée qui écrira pour une autre élite âgée, tandis qu'une majorité, plus jeune, s'informera médiocrement, *via* les chaînes d'infos ou les réseaux sociaux construits sur le clivage et la polarisation… C'est là que se situe, selon moi, la plus grande menace pour la démocratie.

Cela est d'autant plus vrai que l'on est entré dans le règne de la subjectivité jusqu'au sein des écoles de journalisme elles-mêmes ! Il y a vingt ans, un journaliste rêvait d'écrire sur la culture, l'économie, la politique, etc. Maintenant, les étudiants qui vous font face dans les amphithéâtres veulent surtout couvrir la vaste galaxie des victimes de tous ordres, des minorités, des opprimés ou des personnes souffrant d'une condition particulière. On privilégie l'obsession pour la vie personnelle au détriment de la curiosité à l'égard du monde ou, plus simplement, des faits. D'ailleurs, dans les programmes des écoles de journalisme, et dans la société de manière plus générale, on ne rappelle pas suffisamment que dans ce métier, les faits sont sacrés. Dans un tel contexte, comment s'étonner que la voix des *fact-checkers* portent si peu ? Vous pouvez toujours monter une cellule de *fact-checking* dans votre rédaction, corriger une information. Cette correction sera à peine audible face aux décibels des « infox » et votre cellule de *fact-checking* bien impuissante à résister à l'avalanche d'informations et d'approximations qui circulent sur les réseaux sociaux[66].

> « L'information vérifiée, de confiance, ne sera bientôt accessible qu'à une minorité de la population. »

Ainsi, l'information vérifiée, de confiance, ne sera bientôt accessible qu'à une minorité de la population. J'ai donc bien peur que se crée une forme d'inégalité entre ceux qui pourront faire un choix politique éclairé et informé, et tous les autres.

Révolution technologique sans précédent, l'émergence d'Internet a-t-elle accéléré cette crise de confiance envers les médias et, par extension, démultiplié les menaces qui pèsent sur la démocratie ? En d'autres termes, Internet : opportunité ou danger pour la démocratie ?

Il n'est pas facile de répondre de manière binaire à cette question. Il y a quelques années, Internet pouvait être considéré comme un bloc monolithique, mais ce n'est plus le cas désormais. L'époque où le Web était simplement constitué d'un ensemble de sites statiques, chaque propriétaire de site publiant ses propres informations, est totalement dépassée. Le nombre de sites a explosé, le Web a commencé à devenir « participatif » avec l'apparition des messageries instantanées, des premiers réseaux sociaux ou encore des blogs. À

66. *« Pratique journalistique qui consiste à contrôler l'exactitude des informations ou la cohérence des propos délivrés par les hommes politiques »*, selon la définition donnée par Françoise Laugée dans la *Revue européenne des médias* (2011, n° 20, p. 52), le *fact-checking* est apparu aux États-Unis à compter des années 2000 et tend à se développer depuis une quinzaine d'années au sein des médias français. On peut citer entre autres rubriques et chroniques dédiées à cette pratique « Désintox » dans les pages de *Libération*, « Les Décodeurs » dans celles du *Monde*, « Le Vrai du Faux » sur *France Info*, « Le Vrai-Faux de l'Info » sur *Europe 1* ou encore « L'œil du 20 heures » sur *France 2*.

chaque nouvelle étape se sont intégrés de nouvelles fonctions, de nouveaux utilisateurs mais aussi de nouveaux usages, comme le partage de vidéos personnelles, d'éléments sonores et même de fichiers illégaux sur des plateformes de téléchargement. Aujourd'hui, les réseaux sociaux sont au cœur du Web. C'est pourquoi il me semble important de distinguer trois grands groupes de médias : les médias institutionnels, qui comme la presse écrite quotidienne ou la radio migrent mal vers le numérique en raison notamment de problèmes de management, de formation et d'investissements ; les nouveaux médias, souvent spécialisés à l'instar de l'autoproclamé *« 100 % vidéo, 100 % digital »* Brut ou de *The Conversation* un objet médiatique curieux qui mêle brillamment journalisme et recherche ; et, enfin, les réseaux sociaux au sens large, allant du groupe restreint sur Facebook à un média conversationnel comme Reddit qui va s'introduire en bourse.

Les premiers, ceux que l'on qualifie de médias traditionnels, ont été les plus affectés par la révolution Internet. Ils ont perdu très largement en crédibilité car ils ont eux-mêmes souvent succombé aux démons de la rapidité et de la quête de l'audience superficielle. On est passé d'un système constitué de « médias de l'offre », connecté à la fonction d'agenda propre aux journalistes et qui élevait ces derniers au rang de détenteurs du magistère de la vérité, à un système où, à l'inverse, sous prétexte d'écouter l'audience, les rédactions passent tout leur temps à regarder les scores de clics ou de vues des articles ou des vidéos. En somme, le journalisme de l'offre, qui se voulait être un journalisme de défricheurs éclairant le monde, a cédé sa place à un journalisme de la demande au service exclusif des lubies ponctuelles du public, lesquelles sont analysées en temps réel et dûment documentées et mesurées. En principe moins connectés aux audiences, les médias traditionnels souffrent par ailleurs du vieillissement de leur public historique. La télévision et la radio sont en train de mourir au profit de YouTube, du podcast ou de la consommation à la demande. Il faut néanmoins créditer ces médias traditionnels d'apporter au débat public une certaine contradiction, une diversité d'opinions et de points de vue qui ouvrent la discussion, et dont sont totalement dépourvus les médias sociaux.

> « Il faut néanmoins créditer ces médias traditionnels d'apporter au débat public une certaine contradiction, une diversité d'opinions et de points de vue. »

On retrouve ce pluralisme au sein des médias nouveaux. Certes, leur catalogue semble plus vertical car spécialisé. Mais il est aussi plus vaste, plus large, sur le plan des opinions avec le risque, parfois, d'ouvrir la porte aux extrêmes. Cette réserve ne doit, cependant, pas occulter la plus grande réussite de ces médias : parvenir à rajeunir leur audience et à instaurer avec elle une interaction peut-être plus saine.

Mais, pour moi, le plus grand danger provient des réseaux sociaux. En effet, ils témoignent à eux seuls du fait que la promesse du numérique ne s'est pas réalisée. Par construction, le digital nous apporte une infinité d'informations hiérarchisées et approfondies, un accès quasiment illimité à des articles universitaires, des titres de presse et des contenus de qualité. Pourtant, cela n'a pas suffi à limiter son effet néfaste sur la qualité du débat public. Ce paradoxe s'explique par la facilité avec laquelle le numérique encourage la surenchère, la polémique et la caricature au détriment du recul, de la distance et de l'analyse.

> « Sur Facebook, et plus largement sur les réseaux sociaux, la nuance est la garantie de l'inexistence. »

Sur Facebook, et plus largement sur les réseaux sociaux, la nuance est la garantie de l'inexistence. La plateforme dispose même d'un algorithme qui mesure le potentiel publicitaire en fonction d'une analyse de l'agressivité sémantique d'un message. Chaque fois qu'un utilisateur laisse défiler son fil d'actualité, la régie publicitaire – qui fait

le lien entre annonceurs et utilisateurs – doit décider quelle publicité lui montrer. La valeur attribuée à chaque publicité en concurrence est évaluée en fonction de trois critères : l'enchère (le prix que l'annonceur est prêt à payer pour cibler une audience précise), la qualité de la publicité mais également le taux d'interaction estimé. Or, il y a fort à parier que celui-ci augmentera avec un ton plus provocateur, plus clivant…

Pendant la dernière campagne présidentielle américaine, cela a abouti à ce que Joe Biden et son langage policé paient l'espace publicitaire digital sur Facebook plus cher que Donald Trump : les équipes de Facebook savaient qu'avec son outrance légendaire, le président sortant allait « exploser les compteurs ». Tout cela répond bien sûr à une logique commerciale compréhensible mais, avec de tels dispositifs, je ne donne pas cher de la peau de la démocratie. Elle risque bel et bien d'être pulvérisée. D'ailleurs aujourd'hui, il n'y a pas un seul processus électoral dans le monde qui ne soit pas affecté par des *fake news*…

Comment, dès lors, restaurer la relation de confiance et le lien entre médias et citoyens ?

> « Le numérique a dilué deux piliers fondamentaux de la confiance dans les médias : d'une part, la notion de marque et, d'autre part, l'identification des auteurs, des signatures. »

Le numérique a dilué deux piliers fondamentaux de la confiance dans les médias : d'une part, la notion de marque et, d'autre part, l'identification des auteurs, des signatures. Auparavant, on savait exactement qui écrivait l'information et où on l'avait trouvée. On ne se contentait pas d'un vulgaire *« J'ai vu ça sur Facebook »* … La possibilité de restaurer la confiance envers les médias est conditionnée au fait de renouer avec une forme de traçabilité de l'information. D'où toute l'importance, voire l'urgence, de retrouver ces deux piliers afin de rebâtir un socle commun pour apprécier la qualité de l'information.

Je crois également qu'il nous faut réinventer la relation avec le lecteur pour entendre la majorité, rendue silencieuse par les réseaux sociaux parce que ne tenant pas de propos radicaux et extrêmes. J'ai eu l'occasion, il y a quelques années, de rencontrer Kai Diekmann, le rédacteur en chef du *Bild-Zeitung*, le quotidien tabloïd allemand qui peut se targuer d'avoir la plus forte diffusion d'Allemagne et même d'Europe occidentale. Si je ne suis pas un adepte de ce type de presse *trash*, j'avais été frappé à l'époque par les initiatives mises en place pour sentir le pouls du lectorat. Les journalistes du *Bild* n'hésitaient pas aller au-devant de leurs lecteurs en organisant des forums ou des assemblées spécialement conçus pour des temps d'échange. Ils avaient organisé tout un dispositif pour recueillir leurs opinions.

Tout n'est donc pas perdu ! Mais cela va nécessiter de fournir un effort colossal pour restaurer la qualité du journalisme. S'assurer que la qualité de l'information soit perçue et même valorisée suppose en effet de se donner les moyens, de prendre le temps. Or, comment y arriver quand on vous demande de produire à la chaîne des articles dont la plupart n'aura une durée de vie que de quelques heures ? Les journalistes n'ont plus le temps de réaliser correctement leur travail. Et, moins bien formée, la nouvelle génération n'est pas forcément la mieux outillée pour y parvenir.

C'est pourquoi je plaide pour revenir à une certaine rigueur vis-à-vis des faits et pour stimuler la créativité des futurs journalistes. Tant de formats restent encore à inventer ! On doit aussi aider cette nouvelle génération à comprendre comment fonctionne le *business* d'une entreprise de média. Toutefois, on ne s'en sortira pas si cette refonte de la formation

> « On ne s'en sortira pas si la refonte de la formation professionnelle ne s'accompagne pas, très en amont, d'une éducation aux médias, à l'image de celle que l'on reçoit en histoire. »

professionnelle des journalistes ne s'accompagne pas, très en amont, d'une éducation aux médias pour l'ensemble des citoyens, à l'image de celle que l'on reçoit, par exemple, en histoire.

Si une telle éducation s'avère nécessaire, n'est-ce pas aussi et surtout parce que le numérique a bouleversé notre manière de nous informer ?

C'est en tout cas ce que donnent à penser les enquêtes successives menées par le *Pew Research Center*. En effet, d'après ce centre de recherche américain indépendant et non partisan, près de la moitié des adultes américains (48 %) déclarent s'informer *« souvent »* ou *« parfois »* sur les médias sociaux[67]. Facebook se distingue même comme une source régulière d'informations pour 36 % d'entre eux[68]. Et pourtant, six Américains sur dix ne font pas confiance à Facebook pour obtenir des informations relevant des élections ou, plus largement, de la politique. Seuls 15 % d'entre eux font confiance à la plateforme en général tandis que 19 % des personnes interrogées déclarent ne nourrir ni confiance ni méfiance à son égard[69].

En somme, nous vivons à une époque où l'information se consomme comme le tabac ou les sucreries : nous savons que c'est mauvais pour notre santé psychologique et celle de nos démocraties, mais nous replongeons chaque fois délibérément, sous l'effet du même phénomène d'addiction !

> « Nous vivons à une époque où nous consommons l'information comme le tabac ou les sucreries : nous savons que c'est mauvais, mais le même phénomène d'addiction fait son œuvre ! »

À cette nouvelle forme d'addiction s'ajoute, plus inquiétante encore, l'impossibilité d'accéder désormais à un contenu que nous n'aurions pas intuitivement choisi de consulter. Facebook a poussé cette logique de bulle cognitive à son paroxysme. Quand j'étais à Stanford entre 2016 et 2018, j'avais eu l'occasion d'échanger avec des cadres de l'entreprise. Il se trouve qu'ils lisaient la *Monday Note*, la lettre d'information anglophone sur l'économie des médias numériques que je publiais. Si certaines des positions que je défendais chaque lundi les dérangeaient, ils trouvaient intéressant d'en discuter. À l'époque, ils s'interrogeaient sur l'opportunité d'exposer les membres du réseau social à des opinions différentes des leurs… au risque de mettre en péril leur *business model*. Je leur avais conseillé de le faire. Sans surprise, ils ont choisi de préserver la « bulle cognitive » qui a fait leur fortune…

Rétrospectivement, cela n'est guère surprenant. Ces cadres de Facebook ne comprenaient pas, par exemple, que des journalistes du *Guardian* (un journal situé au centre-gauche de l'échiquier politique), décident de partir à la rencontre des électeurs de Donald Trump. Ils avaient l'impression qu'une telle initiative s'apparentait à de l'éditorial, au sens opinion, qu'elle devait participer à définir l'identité du média. Cela en dit long sur l'incapacité de ces entreprises à comprendre et saisir ce que sont réellement les médias.

67. Pew Research Center, "News Consumption Across Social Media in 2021", septembre 2021, disponible en ligne : https://www.pewresearch.org/journalism/2021/09/20/news-consumption-across-social-media-in-2021/ [dernière consultation le 18 février 2022].
68. Pew Research Center, "News Use Across Social Media Platforms in 2020", janvier 2021, disponible en ligne : https://www.pewresearch.org/journalism/2021/01/12/news-use-across-social-media-platforms-in-2020/ [dernière consultation le 18 février 2022].
69. Pew Research Center, "An Oasis of Bipartisanship: Republicans and Democrats Distrust Social Media Sites for Political and Election News", janvier 2020, disponible en ligne : https://www.pewresearch.org/journalism/2020/01/29/an-oasis-of-bipartisanship-republicans-and-democrats-distrust-social-media-sites-for-political-and-election-news/ [dernière consultation le 18 février 2022].

Et, inversement, de l'incapacité des groupes de presse traditionnels à voir les géants du numérique autrement que comme des pilleurs de contenus ?

Ou comme un nouveau guichet de subventions ! La presse voit dans les GAFAM (Google, Apple, Facebook, Amazon et Microsoft), une nouvelle source de revenus justifiée par leur domination économique et leurs pratiques souvent prédatrices. C'est s'affranchir un peu vite de la lenteur des médias à s'adapter et surtout à innover…

Je regrette d'autant plus cette incompréhension mutuelle que l'une et l'autre partie aurait pu profiter d'une coopération en bonne intelligence. Elles auraient pu, par exemple, envisager de développer ensemble des plateformes de gestion de contenus éditoriaux (texte, audio, vidéo), autrement dit le centre névralgique des médias mais avec toutes ses ramifications sur la gestion de la publicité, le marketing, les abonnements ou encore les analyses d'audience. La presse aurait pu mettre à profit les immenses capacités techniques de ces entreprises et il était parfaitement possible de protéger l'intégrité et l'indépendance des médias par des contrats en béton. Encore fallait-il vouloir se donner les moyens de les négocier.

> « Il faut reconnaître que les plateformes ne sont pas parvenues à instaurer un climat de confiance en offrant des perspectives à long terme. Ce qui explique que nous pouvons que constater le rendez-vous manqué entre médias et géants du numérique. »

Mais, culturellement, les patrons de presse se sont montrés bien incapables d'appréhender le problème sous cet angle. Et il faut reconnaître que les plateformes ne sont pas parvenues à instaurer un climat de confiance en offrant des perspectives à long terme. Ce qui explique que nous ne pouvons que constater le rendez-vous manqué entre médias et géants du numérique.

En ces temps de défiance numérique généralisée, à quels autres défis le secteur des médias doit-il faire face pour, cette fois-ci, être au rendez-vous ?

Le principal défi auquel il faudra s'attaquer est celui de la concurrence. Aujourd'hui, cette dernière est protéiforme. Sur un même écran de mobile, tout est au même niveau : l'information de qualité, le divertissement, le social, Netflix… C'est autant une compétition sur le revenu discrétionnaire des utilisateurs que sur le temps dont ils disposent.

Comme beaucoup d'autres à la fin des années 2000, je pensais que les abonnements allaient résoudre ce problème[70]. Je pronostiquais même que les ménages disposeraient à terme de trois types d'abonnement : un premier pour les informations générales, un deuxième pour les informations locales, un troisième pour les loisirs. Je me suis trompé… La moyenne tourne autour d'un abonnement par foyer… et ce n'est qu'une moyenne, donc tous les foyers ne sont pas concernés.

Ce déficit en termes d'abonnement a forcément un impact sur le financement des médias puisque les revenus n'ont pas été compensés. Il faut savoir, en effet, qu'un lecteur numérique rapporte six fois moins qu'un lecteur papier. Ce sont en tout cas les chiffres concernant un mastodonte comme le *New York Times*, mais ils sont révélateurs : aujourd'hui, l'arbitrage budgétaire individuel n'est pas du tout en faveur de la presse.

70. Le premier système de péage de lecture numérique ou *« paywall »* en anglais aurait été mis en place par le *Financial Times*. Depuis, de nombreux journaux ont adopté cette méthode de restriction d'accès à un contenu numérique pour augmenter leurs revenus en incitant les lecteurs à souscrire à un abonnement payant.

Cette dernière voit ses recettes fondre année après année, preuve s'il en fallait encore une que son modèle économique a été complètement dévasté par le numérique. Avec un chiffre d'affaires de 1,9 milliard d'euros en 2019, les recettes publicitaires de la presse écrite ont reculé de 57 % en euros constants en une décennie[71].

« Avec un chiffre d'affaires de 1,9 milliard d'euros en 2019, les recettes publicitaires de la presse écrite ont reculé de 57 % en euros constants en une décennie. »

La presse a perdu la bataille de l'« actu chaude ». Mais l'erreur historique des médias pour tenter de faire volte-face a consisté à créer des départements entiers consacrés au *social media*. Cela a eu pour conséquence de remettre des intermédiaires, de disséminer et donc, *de facto*, de dévaloriser leur contenu, alors même que le numérique leur permettait justement de décloisonner les salles de rédaction, de supprimer une telle intermédiation. La conséquence ? Un avantage sans précédent concédé à des tiers que sont Google, Facebook et tous les autres.

Vous parlez « d'erreur historique ». Faut-il comprendre que vous tenez pour responsables les grands patrons de presse ? Quel rôle ces derniers peuvent-ils ou doivent-ils jouer dans la restauration de la confiance envers les médias ?

« De mon point de vue, la concentration des médias participe davantage à entretenir la méfiance qu'à l'atténuer. »

De mon point de vue, la concentration des médias participe davantage à entretenir la méfiance qu'à l'atténuer. Comment, en effet, restaurer la confiance quand tous les médias sont entre les mains de quelques-uns ? Comment rêver à une information de confiance quand le nombre de médias est en baisse constante et avec lui le nombre d'employeurs potentiels pour les journalistes ? Ces derniers ont de moins en moins la possibilité, voire la liberté, de refuser de se plier aux directives des directions. Au risque sinon de se mettre à dos tout un groupe de médias et donc de ne pas retrouver un nouvel emploi. Cela explique en partie pourquoi les journalistes figurent parmi les professionnels les moins bien rémunérés…

Mais, au-delà du mouvement de concentration à l'œuvre dans l'univers médiatique français, il me semble plus important encore de s'assurer de maintenir une dualité des rôles entre, d'une part, le directeur de la publication et, d'autre part, le directeur de la rédaction. Cela permettrait de prendre à bras le corps le moteur principal de la défiance : à savoir le manque de qualité des papiers. Cette dernière est, en effet, souvent sacrifiée au profit de la tenue d'objectifs chiffrés, pour le nombre d'articles à publier. Pas sûr, néanmoins, que cela permette de répondre à la relative médiocrité de certains patrons de médias et, plus largement, du management intermédiaire, mal formé et démotivé, que je tiens en partie pour responsables de l'effondrement de la compétence interne.

Si cette dernière tend à disparaître c'est parce que les investissements nécessaires n'ont pas été consentis et que, par ailleurs, les journalistes ne font pas toujours de bons managers et n'ont pas eu de vision sur les « produits » commercialisés par les groupes de médias – ce qui n'a pas forcément non plus fonctionné lorsqu'ils ont été remplacés par de purs financiers. Partout dans le monde, les effectifs des journaux sont en train de

71. Ministère de la Culture, Département des études, de la prospective, des statistiques et de la documentation (DEPS-Doc), *Chiffres clés, statistiques de la culture et de la communication 2021*, décembre 2021.

> « Partout dans le monde, les effectifs des journaux sont en train de s'effondrer au point qu'il existe aux États-Unis des « déserts informationnels ». »

s'effondrer au point qu'il existe aux États-Unis des *« news deserts »*, des « déserts informationnels » pour l'actualité locale. L'affaiblissement de toute dimension managériale dans la presse, vérolée par les syndicats ou les *guilds* anglo-saxonnes, n'a fait que précipiter cette disparition. À ce titre, les grilles salariales empêchent toute évolution et donc toute rétention des talents, là où les géants du numérique allouent beaucoup d'énergie et de moyens à ces préoccupations. Les journaux ne font plus rêver. Ce sont les marques qui vont s'imposer comme entité de référence dans la détection des « talents éditoriaux », qui ne seront plus des journalistes comme on l'entendait précédemment, et dans la production de contenus.

L'intelligence artificielle offre-t-elle la perspective d'un ré-enchantement pour le journalisme ?

On ne peut pas ignorer la possible instrumentalisation de la technologie et le risque de voir l'intelligence artificielle s'emparer du quatrième pouvoir. L'exemple le plus connu est celui de GPT-3 ce qui signifie *« Generative Pre-trained Transformer »*. Créé par la société californienne OpenAI, cet algorithme de traitement du langage naturel utilise l'apprentissage automatique pour analyser et générer du texte. Concrètement, le programme a été entraîné par la lecture de l'intégralité de Wikipédia, de tous les blogs et de tous les articles de presse disponibles, soit des milliards de pages. Grâce à cet entraînement musclé, l'algorithme peut générer de nouvelles phrases à partir d'instructions écrites. Autrement dit, cet algorithme, accessible gratuitement, peut écrire en masse et sur n'importe quel sujet avec un résultat bluffant. On imagine aisément ce qui arriverait si un algorithme aussi puissant que GPT-3 tombait entre de mauvaises mains. Contenu biaisé, désinformation de masse, manipulation de l'opinion publique, etc., les dommages seraient considérables.

Et plus encore si la bonne information se retrouvait noyée sous un déluge idéologique de *fake news* et autres demi-vérités. N'est-ce pas en effet problématique quand les *fake news* ne sont même plus identifiables, quand elles ont la possibilité d'être formatées en fonction du destinataire ? Les plus dangereuses étant celles qui contiennent certaines informations vraies, donnant donc une apparence de contenu sérieux et légitime à l'ensemble. Si on dit à chaque citoyen ce qu'il veut entendre, alors il n'y a plus de cité. Le plus grand danger vient donc bel et bien de cette capacité à ajuster le discours, puis à le livrer en masse. Et les moyens et capacités disponibles pour faire du *fact-checking* sont anecdotiques face aux cent millions de contenus qui sont mis en ligne chaque jour sur Facebook.

> « Si on dit à chaque citoyen ce qu'il veut entendre, alors il n'y a plus de cité. Le plus grand danger vient donc bel et bien de cette capacité à ajuster le discours et à le livrer en masse. »

Mais il faut admettre que ce sont ces mêmes technologies qui permettent de produire davantage de contenus pour les lecteurs en automatisant, par exemple, l'écriture de brèves factuelles à partir de résultats électoraux. C'est grâce à un outil technologique baptisé « Heliograf » que les journalistes du *Washington Post* ont notamment pu couvrir plus de 500 élections depuis 2014[72]. Sur le plan de la production d'actualités, on retrouve certains outils liés à l'intelligence artificielle pour faciliter la transcription automatique des *verbatims* d'entrevue

72. Rob Lever, « L'intelligence artificielle gagne du terrain dans les salles de nouvelles », *Le Devoir*, 11 mars 2019, disponible en ligne : https://www.ledevoir.com/culture/medias/549562/l-intelligence-artificielle-gagne-du-terrain-dans-les-salles-de-redaction [dernière consultation le 18 février 2022].

ou encore l'écriture automatisée de nouvelles routinières dans les sports ou le domaine de la finance. L'information économique a d'ailleurs l'avantage de se traduire de manière purement quantitative (voire monétaire), ce qui lui confère une certaine valeur après des décennies passées à dévaloriser l'information…

Malheureusement, la technologie n'en est qu'à ses débuts dans les salles de rédaction, la presse n'investissant encore que trop peu, voire pas du tout dans ce genre d'outils.

Mise au service de l'investigation, la puissance informatique représente aussi l'un des grands espoirs du journalisme de demain. Par exemple, l'intelligence artificielle se montre très utile quand il s'agit d'extraire des informations pertinentes d'un très gros volume de documents. Elle est aussi capable de détecter les signaux faibles parmi le bruit ambiant des réseaux sociaux et, donc, de sentir le pouls de la société et de ses évolutions. Les grandes agences de type *Reuters* possèdent d'ores et déjà des outils qui leur permettent de faire ce que l'on appelle de la « fusion de données ». Il s'agit là de faire ressortir des tendances à partir de jeux de données éparses en leur donnant du sens. La détection des signaux faibles renforce ainsi la capacité d'enquête et d'alerte des journalistes. C'est pourquoi la profession aurait tort de ne pas la considérer avec le plus grand sérieux.

> « La détection des signaux faibles renforce la capacité d'enquête et d'alerte des journalistes, c'est pourquoi la profession aurait tort de ne pas la considérer avec le plus grand sérieux. »

Yseulys Costes

Entretenir la relation de confiance avec les consommateurs : une question de pédagogie

Passionnée par le Marketing Digital, Yseulys Costes est CEO du groupe Numberly, qu'elle a cofondé avec Thibaut Munier en 2000.

Opérant maintenant dans plus de 40 pays, le Groupe, né en France sous le nom de 1000mercis, est coté en Bourse sur Euronext-Alternext. « Marketing Technologist », Numberly aide les annonceurs à se différencier par la qualité de leur relation avec leurs clients, en faisant levier sur les données pour rendre les actions marketing de fidélisation et de conquête plus utiles, pertinentes et ciblées pour les consommateurs et plus efficaces et mesurables pour les marques et les distributeurs.

Issue du monde universitaire – DEA de Marketing et Stratégie de Paris Dauphine, Visiting Researcher Harvard Business School –, Yseulys Costes a gardé des liens étroits avec le monde de la recherche et de l'enseignement aussi bien en France qu'aux États-Unis.

Elle est par ailleurs membre des conseils d'administration de Kering et du Groupe SEB, et ancien membre du Conseil Stratégique de la Ville de Paris.

Le numérique apporte de grands progrès mais comporte des risques importants pour les consommateurs et utilisateurs. Aussi, ces derniers doivent en être informés, et formés, afin d'avoir un usage sécurisé et éclairé du numérique. L'enjeu pour les marques et les entreprises ? Faire la transparence sur la valeur effective apportée par la collecte des données… pour elles comme pour les consommateurs. Car, si la confiance numérique requiert de la pédagogie, elle suppose aussi, et surtout, de maintenir Internet comme un espace ouvert.

Selon vous, quels changements le numérique a-t-il engendrés ces dernières décennies en ce qui concerne le lien de confiance entre consommateurs et entreprises ?

Le rapport entre consommateurs et entreprises s'est transformé à mesure que le numérique a bouleversé la manière dont ces dernières vendent et communiquent. Internet, en effet, est tout à la fois un media et un lieu de commerce. Un mix inédit qui donne la possibilité de faire du marketing « relationnel »[73] et « adressé »[74].

73. Le marketing « relationnel » peut être défini comme un marketing visant à créer, développer et entretenir une relation individualisée avec les clients potentiels (les prospects) et les clients acquis. La connaissance client, le marketing direct et la fidélisation sont des concepts clés au cœur du marketing relationnel. Il ne s'agit plus, pour une entreprise, de chercher prioritairement à maximiser ses parts de marché, mais bien ses parts de clientèle. On s'éloigne de l'idée du marketing « opérationnel » traditionnel où l'objectif ultime était la vente, même si celle-ci se faisait au détriment de la confiance du client. Le marketing relationnel repose sur l'existence de bases de données recensant des informations sur les prospects ou clients. Le dialogue entre le client et la marque passe notamment par l'information régulière [sources : Éva Delacroix, Alain Debenedetti, Ouidade Sabri, *Maxi fiches de Marketing – 2e éd.*, Paris, Dunod, 2014 ; Jean-Jacques Lambin, Chantal de Moerloose, *Marketing stratégique et opérationnel – 9e éd. – La démarche marketing dans l'économie numérique*, Paris, Dunod, 2016].
74. Le marketing « adressé » ou « direct » permet, à partir d'une cible précise, d'adresser à chaque individu un message personnalisé.

Auparavant, entretenir ainsi une relation personnalisée et continue avec chaque client, en s'adressant à lui individuellement et précisément, n'était à la portée que d'une poignée d'entreprises, comme les banques et compagnies d'assurance ou les compagnies aériennes, par le biais notamment des programmes de fidélisation de leurs clients. Depuis, grâce au numérique, ce paradigme s'est largement diffusé, révolutionnant au passage les pratiques des équipes marketing. Et ce d'autant plus que les consommateurs ne consomment plus sur les mêmes canaux, ni avec les mêmes considérations en tête ou selon les mêmes parcours.

Ces changements expliquent en partie le poids croissant des marques. Il faut se souvenir que, à l'origine, les marques n'étaient que de petits signes apposés sur les marchandises pour identifier leur provenance, leur propriétaire et donc aussi leur qualité. Le terme renvoie à l'action de « marquer » et, en anglais, le mot *« brand »* est issu du vieux français « brandon », qui désigne un outil pour marquer le bétail au fer rouge avec le signe de l'éleveur. Si la marque est depuis longtemps un support de contexte, de propriété, de qualité, de confiance, le numérique renforce son importance. Car, dans un monde digital comme le nôtre, cette confiance se gagne aussi vite qu'elle ne se perd. Et, surtout, elle se travaille.

> « Si la marque est depuis longtemps un support de contexte, de propriété, de qualité, de confiance, le numérique renforce son importance. »

Les marques peuvent ainsi construire une relation de confiance avec les consommateurs en faisant la transparence sur la valeur effective apportée par la collecte des données. Il faut expliquer aux consommateurs pourquoi on collecte leurs données. Il faut tout autant leur montrer ce qu'eux aussi ont à gagner dans le traitement de ces données, en termes de qualité de service ou de pertinence des produits proposés grâce à un travail de personnalisation.

Si les marques peuvent travailler à entretenir la confiance entre elles et les consommateurs, un cadre législatif renforcé n'œuvre-t-il pas davantage à faire toute la lumière sur la collecte des données et donc à restaurer la confiance ? Quel regard portez-vous sur un texte qui, comme le* Règlement Général sur la Protection des Données (RGPD)*, encadre le traitement des données personnelles sur le territoire de l'Union européenne[75] ?

Le RGPD, je le rappelle, ne s'adresse pas uniquement aux entreprises mais à toute structure privée ou publique effectuant de la collecte et/ou du traitement de données, et ce quel que soit son secteur d'activité et sa taille. Il s'applique à tous les organismes établis sur le territoire de l'Union européenne comme à ceux implantés hors de l'Union européenne mais dont l'activité cible directement des résidents européens.

Ce règlement repose sur l'idée selon laquelle la transparence participe à générer de la confiance. Cette vision, européenne, me semble parfaitement juste. Il n'en demeure pas moins que l'on peut se poser la question de son efficacité et s'interroger sur la capacité des consommateurs à en comprendre les tenants et les aboutissants.

> « Le RGPD repose sur l'idée selon laquelle la transparence participe à générer de la confiance. »

75. La Commission Nationale de l'Informatique et des Libertés (CNIL) désigne comme donnée personnelle *« toute information se rapportant à une personne physique identifiée ou identifiable »* et distingue deux types d'identification : l'une directe (nom, prénom, etc.), l'autre indirecte (identifiant, numéro, etc.).

Concrètement, quelle expérience font-ils du RGPD ? Ils ont face à eux, sur leur écran, des cases en guise d'avertissement, qu'ils doivent cocher, selon qu'ils acceptent ou refusent la collecte de leurs données personnelles. Mais est-on vraiment certain que ces choix sont faits en toute connaissance de cause ? Constituent-ils pour autant des choix éclairés et même libres ? Pour des entreprises comme Facebook ou Google, on peut en effet douter qu'on a vraiment le choix de donner ou non son consentement si l'on souhaite utiliser leur service… qui est perçu comme indispensable. Le RGPD alerte les consommateurs. Il n'améliore cependant pas leur capacité à comprendre et à répondre à cette alerte.

> « Le RGPD alerte les consommateurs. Il n'améliore pas leur capacité à comprendre et à répondre à ces alertes. »

Pourtant, aujourd'hui, plus de deux tiers des Français (69 %) affirment être attentifs au traitement qui est fait de leurs données personnelles lorsqu'ils utilisent Internet[76]. N'est-ce pas là la preuve, qu'à l'heure du « tout-numérique », le RGPD a participé à faire entrer cette préoccupation dans les mœurs ?

En Europe continentale, nous entretenons un rapport émotionnel à la donnée personnelle, contrairement aux États-Unis ou à la Grande-Bretagne où le rapport à la donnée est davantage transactionnel. Ce rapport diffère en effet en fonction de l'histoire de chaque pays. En Europe, l'accès aux données personnelles renvoie encore très souvent à l'histoire de régimes totalitaires pas si lointains dans le temps, ce qui explique pourquoi l'appréhension de la donnée est encore plus émotionnelle dans des pays comme l'Allemagne ou l'Espagne. Cette histoire représente un terreau propice à la protection des données des consommateurs européens. Aux États-Unis ou en Grande-Bretagne, la liberté d'entreprendre a favorisé le développement d'un rapport plus apaisé, et même pragmatique, à la donnée.

> « En Europe, nous entretenons un rapport émotionnel à la donnée. (…) Générer de la confiance sur un sujet émotionnel suppose de fournir un effort d'explication et de pédagogie supplémentaire. »

Ces terreaux différents ont des conséquences qui vont de l'appréhension de la donnée au cadre de la concurrence[77]. Un Français, le prix Nobel d'économie Jean Tirole, a d'ailleurs parfaitement résumé ces différences en distinguant les marchés bifaces – dont l'agencement entretient, voire nécessite l'existence de deux clientèles tout à fait différentes quoique finalement interdépendantes l'une de l'autre pour les produits qui y sont échangés – et les modèles trifaces – qui, comme le font les plateformes numériques, relient des utilisateurs, des annonceurs et des éditeurs.

Générer de la confiance sur un sujet émotionnel suppose de fournir un effort d'explication et de pédagogie supplémentaire. Or, je ne suis pas certaine qu'avec le RGPD ce travail d'accompagnement et d'explication ait été engagé. Ne pas connaître les risques que l'on prend en acceptant la collecte de telle ou telle donnée, ne

76. « Les Français et la souveraineté numérique », enquête menée par l'Ifop pour OVHCloud auprès d'un échantillon de 1 028 personnes, représentatif de la population française âgée de 18 ans et plus. Les interviews ont été réalisées par questionnaire auto-administré en ligne du 7 au 8 janvier 2021.

77. En termes de réglementation du « spam », l'Europe et les États-Unis ont par exemple adopté deux types d'approche en tout point opposés. En Europe, l'*opt-in* est la règle. Cette approche oblige les prospecteurs à obtenir, préalablement à tout envoi, le consentement de l'internaute à recevoir des publicités dans sa boîte de courrier électronique. L'approche *opt-out*, qui prévaut aux États-Unis, est plus favorable aux prospecteurs puisqu'elle permet l'envoi de messages à toutes les personnes qui ne s'y opposent pas. Concrètement, l'internaute doit signifier son opposition auprès du prospecteur ou s'inscrire sur un registre d'opposition, sorte de liste rouge 3.0.

pas savoir différencier les données personnelles et les cookies[78], cela crée un contexte plus anxiogène que jamais. Et la décision de Google d'un arrêt de l'utilisation de cookies tiers[79] sur Chrome, le navigateur Web propriétaire de Google, risque d'ajouter de l'incompréhension à l'incompréhension.

En annonçant ce changement en janvier 2020, la firme de Mountain View a mis en avant son programme *« Privacy Sandbox »* qui vise à créer *« des technologies Web protégeant à la fois la vie privée des personnes en ligne et donnant aux entreprises et aux développeurs les outils nécessaires pour créer des activités numériques florissantes afin de garder le Web ouvert et accessible à tous »*. Prévue initialement pour début 2022, la disparition des cookies tiers de Chrome a été repoussée à mi-2023. Google explique ce report par la nécessité de mettre en place des alternatives pouvant être testées en amont, son navigateur Chrome étant toujours présenté comme visant à mieux protéger la vie privée. Mais, objectivement, cela n'est pas le cas.

> « Google va donc continuer à tracer le comportement sur ses propres services, souvent leaders du marché. »

Pour permettre de continuer à cibler la publicité malgré l'absence de cookies tiers, Google envisage d'adopter une méthode consistant à former de grandes cohortes. L'idée est de réunir ensemble les internautes ayant, par exemple, l'intention d'acheter un aspirateur, ou bien ceux qui ne lisent que des livres de loisirs créatifs, en les « cachant » dans de larges groupes. Google va donc continuer à tracer le comportement sur ses propres services, souvent leaders du marché. Fort de la connaissance fine de ses clients qui s'enregistrent chez lui avec un *login,* Google va surtout participer à la création de « jardins fermés ». Or, on peut s'interroger sur cette décision de fermer de la sorte son écosystème en interdisant le ciblage aux autres acteurs publicitaires. Google le fait-il réellement pour protéger les utilisateurs ou plutôt… pour protéger sa marge ? La question reste entière. En revanche, cette annonce participe à coup sûr à diaboliser les cookies.

En somme, lier inextricablement transparence et confiance, comme le fait l'Europe, est louable. Mais le consommateur se sent, à raison, un peu perdu et cela cristallise des positions.

78. La CNIL définit un cookie comme étant *« un petit fichier stocké par un serveur dans le terminal (ordinateur, téléphone, etc.) d'un utilisateur et associé à un domaine web. Ce fichier est automatiquement renvoyé lors de contacts ultérieurs avec le même domaine. Les cookies ont de multiples usages : ils peuvent servir à mémoriser votre identifiant client auprès d'un site marchand, le contenu courant de votre panier d'achat, la langue d'affichage de la page web, un identifiant permettant de tracer votre navigation à des fins statistiques ou publicitaires, etc. Certains de ces usages sont strictement nécessaires aux fonctionnalités expressément demandées par l'utilisateur ou bien à l'établissement de la communication et donc exemptés de consentement. D'autres, qui ne correspondent pas à ces critères, nécessitent un consentement de l'utilisateur avant lecture ou écriture. »* [source : https://www.cnil.fr/fr/definition/cookie ; dernière consultation le 18 février 2022].

79. La CNIL distingue les cookies « internes » (ou *« first-party »*) des cookies « tiers » (ou *« third-party »*) de la manière suivante : *« Lorsqu'un utilisateur visite un site web, il consulte en pratique un « domaine » qui termine en général par une extension de type .com ou .fr […], les contenus peuvent être transmis depuis le domaine qu'il visite ou bien via d'autres domaines qu'il n'a pas entré lui-même et qui appartiennent à des tiers. En effet, chaque cookie est associé à un domaine et envoyé ou reçu à chaque fois que le navigateur va « appeler » ce domaine. En pratique :*
Les cookies « internes » sont déposés par le site consulté par l'internaute, plus précisément sur le domaine du site. *Ils peuvent être utilisés pour le bon fonctionnement du site ou pour collecter des données personnelles afin de suivre le comportement de l'utilisateur et servir à des finalités publicitaires.*
Les cookies « tiers » sont les cookies déposés sur des domaines différents de celui du site principal, généralement gérés par des tiers *qui ont été interrogés par le site visité et non par l'internaute lui-même : ces cookies peuvent aussi être nécessaires au bon fonctionnement du site mais ils servent majoritairement à permettre au tiers de voir quelles pages ont été visitées sur le site en question par un utilisateur et de collecter des informations sur lui, notamment à des fins publicitaires.*
[source : https://www.cnil.fr/fr/definition/cookie ; dernière consultation le 18 février 2022].

Face à la cristallisation des positions et à la détérioration de la confiance des consommateurs, ne peut-on pas s'interroger sur la possibilité réelle de concilier confidentialité des données et personnalisation de l'expérience client ?

Il y a différentes manières de s'y prendre. Soit, vous optez pour l'axe pris par Google et décidez de travailler par cohorte, et non par individu. Le problème ? Les marques n'ont pas accès au traitement qui permet de regrouper les données en cohortes. Cohortes qui ne sont rien d'autre qu'un ensemble d'individus… Par ailleurs, est-ce rassurant pour le consommateur de savoir que ses données ne sont traitées que par un seul et unique acteur ? Je n'en suis pas si sûre.

Soit, vous vous intéressez au contexte individuel, au contexte d'une personne anonyme. Mais cette solution est, *in fine*, moins efficace, moins personnalisée. Le contexte explique beaucoup moins de choses sur un individu qu'une connexion au travers d'identifiants par exemple. Il n'y a pas de secret, ni de miracle : plus vous connaissez les gens, plus vous êtes pertinent dans l'approche commerciale.

C'est pourquoi les consommateurs que nous sommes tous doivent prendre conscience de l'ensemble des enjeux qui entourent ces problématiques. Schématiquement, Internet peut être représenté comme un monde. Avant, ce monde était complètement ouvert puis, peu à peu, des blocs se sont constitués, se sont fermés. Vous avez ces mondes fermés que sont, bien sûr, la Chine, mais aussi Facebook ou Google par exemple, puisque, pour entrer dans leur univers, il faut un *login*. Et puis, vous avez tout le reste, le plus gros volume, l'Internet ouvert *(open Internet)*.

Que les consommateurs veuillent pouvoir concilier personnalisation et gratuité d'Internet n'est donc pas problématique en soi. Mais cela suppose des investissements publicitaires et marketing qui constituent le véritable fuel de l'Internet ouvert car ce sont eux qui font vivre l'ensemble de l'écosystème. En effet, l'Internet ouvert n'existe que grâce aux budgets publicitaires et marketing. Et ces budgets ne sont acceptés par les consommateurs et efficaces pour les entreprises que s'ils aboutissent à davantage de personnalisation. Or, pour cela, il faut de la data… Il me paraît donc essentiel que les entreprises investissent dans cet Internet ouvert et non uniquement dans les GAFAM, ces géants du numérique que sont Google, Apple, Facebook, Amazon et Microsoft, qui constituent l'Internet fermé. Ce serait en effet problématique si la production de contenus ne relevait plus que des GAFAM, et que l'Internet ouvert, du coup, disparaissait.

> « Que les consommateurs veuillent pouvoir concilier personnalisation et gratuité d'Internet n'est donc pas problématique en soi. Mais cela suppose des investissements publicitaires et marketing. »

> « Pour moi, la confiance numérique est essentielle ne serait-ce que pour que les consommateurs aient un usage éclairé et donc une compréhension de ce qu'ils font et pourquoi ils le font. »

Pour moi, la confiance numérique est essentielle, ne serait-ce que pour que les consommateurs aient un usage éclairé et donc une compréhension de ce qu'ils font et pourquoi ils le font. Chacun doit pouvoir être maître de ses propres données, chacun doit pouvoir être informé des risques qu'il court lors de ses connexions, tant dans ses usages personnels que professionnels. Cette culture du numérique me semble propice au développement d'un esprit critique et d'une connaissance du fonctionnement des technologies. C'est pourquoi elle doit être appréhendée de manière transversale, et par-delà la seule approche technique.

Elle doit surtout s'étendre au-delà des bancs de l'école pour entrer pleinement au sein des entreprises. En effet, le besoin de confiance, de sécurité et protection des consommateurs crée une exigence nouvelle pour les organisations et ces dernières n'auront d'autre choix que d'y répondre pour utiliser harmonieusement et de manière équitable les données. Aussi, la confiance numérique passe-t-elle par la transparence et la constance dont les entreprises font preuve sur ces sujets. L'écosystème doit donc favoriser cette constance pour que l'on soit capable de créer un équilibre satisfaisant pour la majorité des consommateurs.

Il me semble également important que les consommateurs voient la totalité du tableau, qu'ils comprennent qu'ils consomment dans l'Internet ouvert et chez les GAFAM, dans l'Internet fermé, de manière gratuite mais que, dans l'un et l'autre univers, le modèle diffère. Il leur revient donc de choisir entre l'un ou l'autre modèle, à condition toutefois que ce choix soit véritablement éclairé. C'est pourquoi il me paraît important qu'ils continuent à avoir ce choix, qu'aucun monopole ne puisse s'installer même si, sur ce sujet, on s'en rapproche dangereusement… De nouveau, garder un Internet ouvert vivant suppose que les investissements dans l'écosystème de l'*open Internet* se poursuivent.

Vous avez souligné à plusieurs reprises l'importance, pour les consommateurs, d'avoir un usage éclairé du numérique. Mais comment justement permettre une utilisation pleine et sûre d'Internet ?

Le digital reste un outil complexe car multiforme. Si l'on y réfléchit bien, en effet, il est tout à la fois un média, un terrain d'expression individuelle mais aussi un lieu de consommation grâce au e-commerce et, de manière plus générale, une technologie qui modifie les processus, les flux d'opérations et d'activités dans l'ensemble des secteurs. Le plus grand danger vient donc de cet aspect systémique, c'est-à-dire du fait que le digital concerne chacun des pans de nos vies, leur dimension personnelle comme professionnelle.

> « Le monde digital a complètement inversé le cycle de pénétration des innovations, désormais d'abord imposées dans la sphère personnelle avant de se diffuser dans l'univers professionnel. »

À ce titre, il est frappant que le monde digital ait complètement inversé le cycle de pénétration des innovations dans nos sociétés. Jusqu'à la création d'Internet, toutes les innovations ont d'abord pénétré nos sociétés par le biais de l'entreprise, de la sphère professionnelle, avant d'être adoptées, dans un second temps, dans la sphère personnelle. Cela vaut pour le téléphone filaire, le fax ou encore le *Global System for Mobile communication* (GSM) qui a permis l'avènement de la téléphonie mobile. À l'inverse, les réseaux sociaux, les *smart phones,* les protocoles de messagerie enrichie *(Rich Communication Services)* se sont d'abord imposés dans la sphère personnelle avant de se diffuser, ensuite seulement, dans l'univers professionnel. La diffusion de l'utilisation de la visioconférence en est un exemple. C'est comme si nous étions passés, en somme, d'une diffusion pyramidale à une autre, sans doute plus horizontale.

Or, cette inversion des flux de diffusion a bouleversé la vitesse d'adoption des innovations et, surtout, leur « encadrement ». Quand la diffusion partait de l'entreprise, elle était assortie d'une batterie de normes, de tests de robustesse, de sécurisation, etc. Désormais, cette structure normative n'est plus aussi solidement construite, ce qui pose des problèmes d'encadrement et d'apprentissage de l'usage lui-même. Si les réseaux sociaux étaient nés au sein des entreprises pour ensuite seulement se déployer dans les foyers, je pense que

> « Quand la diffusion partait de l'entreprise, elle était assortie d'une batterie de normes. Désormais, cette structure normative n'est plus solidement construite. »

cela aurait été complètement différent. Peut-être n'aurions-nous pas eu besoin d'imaginer *a posteriori* un droit à la déconnexion…

À cette théorie de la diffusion de l'innovation, qui permet d'expliquer un certain nombre d'éléments, s'ajoutent les problématiques d'accès à la technologie, qui relèvent autant du pouvoir d'achat que des difficultés à comprendre et à manipuler les nouveaux outils numériques. J'ignore si, comme on l'entend parfois, la crise sanitaire liée à la pandémie de Covid-19 a réellement creusé davantage la fracture entre des élites technophiles et des populations en situation d'illectronisme. Ce que je sais, en revanche, c'est qu'elle a accéléré l'usage des outils numériques. Les familles n'ont eu d'autre choix que d'accompagner, d'éduquer les personnes de leur entourage les plus déconnectées des écrans. C'est une excellente nouvelle pour toute une génération qui a peu ou pas du tout de culture technologique et data.

Plus largement, ce travail d'accompagnement me paraît essentiel et les entreprises ont un rôle à jouer. Si l'école éduque les enfants à l'usage du numérique, et par conséquent, d'une manière indirecte, également leurs parents, d'autres catégories de la population passent à la trappe, notamment celles qui n'ont pas d'enfants scolarisés. Ces générations disposent d'une culture tech et de la data relativement faible par rapport à d'autres pays, comme le Royaume-Uni par exemple où la vitesse d'adoption du numérique y est plus rapide.

C'est pourquoi nous y participons par le biais de notre fondation *1000mercis impacts* et le soutien d'associations engagées sur ces questions. Grâce au mentorat, nous aidons ainsi les populations les plus éloignées du numérique à en acquérir les usages de base (*i.e.,* communiquer, s'informer, apprendre). Il s'agit également de les former pour qu'elles puissent, *in fine,* saisir ce que signifie réellement donner son consentement, accepter de recevoir des informations mais aussi comprendre les risques que cela comporte. La crise sanitaire a, sur cette question aussi, joué un rôle d'accélérateur.

Que les utilisateurs prennent confiance en eux dans leur maîtrise des outils est incontestablement nécessaire et une excellente nouvelle. Peut-on pour autant imaginer qu'ils revendiquent à terme de devenir propriétaires de leurs données ?

On pourrait, en effet, vouloir tout monétiser, mais l'idée de créer un marché de la donnée où chacun serait « payé » pour l'utilisation de ses données me paraît surprenante, voire saugrenue, dans un pays où le rapport à la donnée est si peu transactionnel… Cela supposerait surtout de monétiser aussi l'accès au contenu et à l'information. Or, cela ne peut pas être fait dans le cadre de l'Internet gratuit mais davantage dans celui des microtransactions, comme celles qui, en vogue dans le monde du jeu vidéo, permettent d'acheter un bien numérique de faible valeur unitaire. Cela soulève néanmoins de grands enjeux en termes de faisabilité.

Par ailleurs, l'Europe a-t-elle vraiment intérêt à encourager une monétisation de la donnée ? Cette dernière ne tournerait-elle pas à l'avantage exclusif des seuls géants du numérique ? Autant de questions qui méritent d'être posées. À mon sens, le sacre d'une telle souveraineté individuelle, voire individualiste, sonnerait le glas de la philosophie à l'origine de la création d'Internet. Elle signerait la fin de l'*open Internet* pour aboutir à un modèle purement transactionnel. Parvenir à trouver à chaque instant un équilibre dans la transaction me paraît ambitieux et pas forcément à l'avantage des consommateurs…

> « L'Europe a-t-elle intérêt vraiment à encourager une monétisation de la donnée ? »

Comment les entreprises européennes peuvent-elles alors rassurer les consommateurs et continuer à garantir l'intégrité et la sécurité de leurs données ?

En Europe, la souveraineté des entreprises passe par la capacité de ces dernières à traiter et à garantir un traitement de la donnée conforme à leur éthique et à ce qu'elles disent à leurs consommateurs. La souveraineté, pour moi, passe davantage par cette capacité à collecter et à traiter de manière sécurisée et intelligente les données que par la possibilité d'aller acheter des segments à cette sorte de « tiers de confiance », que serait par exemple Google sans pour autant avoir accès aux données individuelles. Bien sûr, il faut travailler avec des géants comme Google, mais cela ne doit pas empêcher les entreprises de se doter d'une véritable stratégie data reposant sur la constance et la transparence.

> « Une donnée, il faut le rappeler, n'a pas de valeur en soi. Ce qui lui confère de la valeur, c'est ce qu'elle apporte du fait de son activation. »

Car, une donnée, il faut le rappeler, n'a pas de valeur en soi. Ce qui lui confère de la valeur, c'est ce qu'elle apporte du fait de son activation. De ce point de vue, dire que la donnée est le pétrole du XXIe siècle n'est pas tout à fait exact. Un baril de pétrole, on sait combien il coûte. Pour un « baril de data », les choses sont bien différentes. Vous ne connaîtrez son prix qu'à condition de l'utiliser. La souveraineté ne saurait donc se résumer à la collecte des données seules, mais à celles utilisées, ce qui suppose une parfaite traçabilité. Cela pose également la question de la conservation de ces données en Europe, le fameux « *cloud* souverain » réclamé par nombre d'Européens, qui déplorent la puissance et le quasi-monopole d'acteurs américains. Cependant, nous avons un problème d'échelle et d'options alternatives au niveau européen.

De son côté, l'Europe a manifesté sa détermination à réguler et protéger l'espace numérique. L'acte pour le marché numérique (DMA) et l'acte pour les services numérique (DSA) pourraient entrer en vigueur début 2022 puisque le Parlement européen a voté le DMA dès la mi-décembre 2021 et adopté le DSA le 20 janvier 2022[80]. Cette règlementation pourra-t-elle contribuer à rétablir durablement la confiance au sein de l'économie digitale européenne ?

Le sujet est, si je peux me permettre, un peu « jonctif ». Le numérique, encore une fois, englobe des domaines aussi divers que les services, les contenus ou la modération de ceux-ci. Tous constituent autant d'éléments de la confiance mais différents des enjeux de consentement. Le problème que pose l'activité législative en la matière, c'est l'impression donnée de faire face à un engrenage qui ne s'arrête jamais. Pour le législateur, c'est comme s'il s'agissait sans cesse d'essayer de rattraper son retard.

Ceci dit, je salue bien sûr les objectifs poursuivis par ces deux textes et en particulier la lutte contre les contenus illicites, la haine en ligne et la désinformation pour le DSA. Avec le DMA, l'Europe prend acte des risques liés au quasi-monopole dont je parlais auparavant. En se plaçant sur le terrain de l'abus de position dominante et non plus seulement sur la *privacy*, elle montre son souci de l'*open Internet* et la nécessaire sauvegarde d'un environnement qui laisse toute sa place à l'innovation.

80. Comme le rappelle Emmanuel Macron dans un discours, prononcé à l'Élysée le 9 décembre 2021 à l'occasion d'une conférence de presse sur la Présidence française du Conseil de l'Union européenne, l'acte pour le marché numérique dit DMA *« vise à éviter que les géants du numérique deviennent des monopoles sans règles et tuent cet esprit d'innovation qui, hier, leur a permis d'émerger »*. Le second texte discuté avec le Parlement européen, c'est l'acte pour les services numériques. Le DSA a pour objectif d'établir *« un régime de responsabilité des grandes plateformes au titre des produits qu'elles vendent et surtout des contenus qu'elles diffusent »*. Il est possible de consulter le texte du discours du président de la République en ligne : https://www.elysee.fr/front/pdf/elysee-module-18912-fr.pdf [dernière consultation le 18 février 2022].

Une triste réalité cependant : la décision de Google de mettre fin aux cookies en 2023 semble avoir un impact bien plus important que n'importe quelle régulation ou texte. En effet, là où des réglementations européennes comme le RGPD ont des impacts très variables sur les entreprises étrangères, l'impact de l'action de Google est énorme et, à l'exception de la Chine, quasiment global.

Par ailleurs, les textes réglementaires, adoptés au niveau de l'Union européenne ou à l'échelle nationale, pourront sans doute contribuer au rétablissement de la confiance au sein de l'économie digitale européenne mais à condition d'apporter un minimum de stabilité. Et j'ai tout à fait conscience qu'il n'est pas simple d'insuffler de la stabilité dans un monde en perpétuelle évolution… C'est pourquoi je suis convaincue que c'est davantage grâce à la pédagogie qu'à la loi que l'on parviendra à réduire la défiance.

> « Je suis convaincue que c'est davantage grâce à la pédagogie qu'à la loi que l'on parviendra à réduire la défiance. »

Ferghane Azihari

Réinventer la confiance par le numérique : la promesse des cryptomonnaies

Ferghane Azihari est essayiste et analyste en politiques publiques, membre de la Société d'économie politique et délégué général de l'Académie libre des sciences humaines.

Il a publié son premier essai Les écologistes contre la modernité, Le Procès de Prométhée *en 2021 aux Presses de la Cité.*

Il intervient régulièrement dans les médias audiovisuels et publie des notes sur les politiques publiques, aussi bien françaises qu'européennes et internationales, pour divers médias et think tanks francophones et anglophones.

Né en 1993, il a suivi des études de droit et de sciences politiques.

Monnaie courante dans l'histoire de la numismatique, les problèmes de confiance pourraient, sinon disparaître, du moins reculer avec l'émergence et la démocratisation des cryptomonnaies. Mais, si la confiance numérique réside autant dans la technique que dans un système de gouvernance et dans un cadre de règles, ces nouvelles technologies de la confiance, véritables « trust machines », ne règlent en rien la confiance vis-à-vis de l'homme.

Les cryptomonnaies apportent-elles un gage de confiance supplémentaire, que d'aucun qualifierait de « numérique », par rapport aux monnaies « traditionnelles » ?

Je crois que pour le déterminer il nous faut revenir aux trois *fonctions* de la monnaie déjà définies par Aristote[81]. Elle est à la fois, nous dit le Stagirite, une « unité de compte », un « outil d'échange » et une « réserve de valeur ».

Les deux premières fonctions sont très simples : permettre de chiffrer une valeur pour les choses, de les placer sur une sorte d'échelle (unité de compte), est parfaitement utile pour pouvoir envisager la seconde fonction (outil d'échange) qu'est le transfert d'objets ou de services entre les personnes. La monnaie facilite une sorte de transmission de valeur entre nous tous en permettant aux objets et aux services de « muter », de nous servir puis de se transformer en une chose utile pour quelqu'un d'autre. La troisième fonction, la réserve de valeur, est plus complexe, surtout lorsque l'on commence à la concevoir dans le temps. Car l'argent thésaurisé peut lui-aussi servir à générer de la valeur.

Ce qui nous renvoie aux *caractéristiques* de la monnaie. Pour remplir au mieux ses fonctions, la monnaie doit, en effet, être facilement divisible en sous-unités, facilement transportable et durable. C'est pour cette raison que nos ancêtres ont abandonné les denrées alimentaires périssables, qui servaient jadis à faire du troc, pour sélectionner les matériaux précieux par exemple. Et, enfin, cette monnaie doit avoir une certaine rareté. Et c'est là-dessus, je crois, que les cryptomonnaies, et le Bitcoin en particulier, disposent d'un réel avantage comparatif par rapport aux monnaies officielles.

81. Aristote, *Les Politiques*, Livre I, Paris, Flammarion, 2008 ; Aristote, *Éthique à Nicomaque*, Livre V, Paris, Flammarion, 2004.

De quoi parle-t-on au juste quand on évoque les cryptomonnaies ?

L'Institut National de la Consommation (INC) englobe sous le terme de cryptomonnaies toute *« monnaie virtuelle que repose sur un protocole informatique de transactions cryptées et décentralisées, appelé block-chain ou chaîne de blocs »*. Et, plus largement, les cryptoactifs sont *« des actifs virtuels stockés sur un support électronique permettant à une communauté d'utilisateurs les acceptant en paiement de réaliser des transactions sans avoir à recourir à la monnaie légale »*. Ces définitions, grossières, rappellent à juste titre que sur un plan juridique une cryptomonnaie n'est pas une monnaie dépendant d'une institution ou bénéficiant d'un cours légal dans quelque pays que ce soit. En revanche, elles oublient à mon sens la qualité intrinsèque à la première des cryptomonnaies, à savoir le Bitcoin, créé en 2009 par l'énigmatique Satoshi Nakamoto. Car le Bitcoin est fondé sur la promesse qu'il n'y aura jamais plus de 21 millions d'unités en circulation[82]. C'est donc une monnaie qui s'est structurellement prémunie contre le faux-monnayage, par opposition aux monnaies officielles : historiquement, la dimension étatique de la monnaie n'a jamais été un gage de qualité…

> « Le Bitcoin est fondé sur la promesse qu'il n'y aura jamais plus de 21 millions d'unités en circulation. »

Dans quelle mesure justement l'émergence des cryptomonnaies s'insère-t-elle dans l'histoire de l'industrie bancaire ?

D'un côté, vous avez l'école selon laquelle au commencement était le troc, qui a peu à peu laissé sa place à la monnaie. De l'autre se tiennent les anthropologues qui, dans la lignée par exemple d'un David Graeber[83], estiment que la monnaie succède à la dette. Selon eux, la monnaie, parce qu'elle constitue un gage de paiement immédiat, résoudrait l'incertitude où je suis quant à la solvabilité de celui qui me doit quelque chose.

Cependant, c'est oublier un peu vite que ceux qui battent monnaie ont toujours dû faire face à un problème de confiance pratique. Comment, en effet, garantir la qualité du métal utilisé ou la crédibilité de l'émetteur ? Certes, le poinçonnage servait précisément à attester la qualité du métal utilisé pour les transactions. Mais, il ne résolvait pas tous les problèmes. Comment faire confiance à ce poinçonnage quand on sait que les historiens ont découvert que les monarques trafiquaient leur propre monnaie ?! Philippe le Bel[84] était d'ailleurs surnommé le « roi faux-monnayeur » … et ses successeurs ont fait bien pire que lui !

Cette incertitude a participé à la création du métier de banquier. Il paraissait plus aisé de recourir à un tiers de confiance pour lui déléguer notamment la tâche laborieuse qui consiste à tenir la comptabilité. Mais cela n'a pas mis fin pour autant aux problèmes de confiance. Comment, par exemple, m'assurer que ce tiers de

82. La quantité de cryptomonnaie en circulation a été fixée dès sa création. Une façon de limiter la masse monétaire et de faire du bitcoin un actif rare, renforçant ainsi sa valeur potentielle.
83. Auteur de plusieurs essais majeurs sur la dette, la bureaucratie ou les *« bullshit jobs »*, David Graeber (1961-2020) était considéré comme l'un des intellectuels les plus en vue de la gauche radicale anglo-saxonne et l'une des figures de proue du mouvement *« Occupy Wall Street »*. Voir notamment David Graeber, *Dette : 5 000 ans d'histoire*, Paris, Les Liens qui Libèrent, 2011.
84. Philippe IV (1268-1314), dit aussi « le Bel » ou « le Roi de fer », est roi de France de 1285 à 1314. Bien que, sous son règne, le royaume de France atteint l'apogée de sa puissance médiévale et connaît une grande prospérité économique, il est particulièrement agité sur le plan monétaire. Le roi et ses conseillers multiplient les émissions de nouvelles monnaies. Aux dévaluations succèdent les réévaluations, qui donnent un sentiment d'incohérence de la politique royale et aboutissent à un mécontentement général. Entre 1306 et sa mort, le roi fait face à des émeutes populaires mais aussi à des ligues nobiliaires qui exigent, entre autres, le retour à la bonne monnaie [source : *Wikipédia, https://fr.wikipedia.org/wiki/Philippe_IV_le_Bel* ; dernière consultation le 18 février 2022].

> « Les problèmes de confiance sont, si je puis dire, monnaie courante dans l'histoire de la banque et de la finance et ce, bien avant l'apparition du billet et de la monnaie scripturale. »

confiance ne falsifie pas mon livre de compte ou ne me débite pas de manière aléatoire ? Les problèmes de confiance sont, si je puis dire… monnaie courante dans l'histoire de la banque et de la finance et ce, bien avant l'apparition du billet et de la monnaie scripturale.

La virtualisation de la monnaie a engendré d'autres problèmes de confiance. Comment s'assurer que le prestataire n'émette pas trop de monnaie ? Comment s'assurer, quand je suis une banque, que mes clients ne retirent pas tous en même temps leur argent, ou pas trop ? Pendant très longtemps, le système de l'étalon-or[85] a rempli ce rôle de garant. Mais le système a vite été perverti. En autorisant le banquier à ne pas honorer ses engagements, à suspendre ses paiements, on procède à la démonétisation de fait, ni plus ni moins.

Faut-il comprendre que les cryptomonnaies participent à redonner de la valeur à la monnaie ?

> « Que fait le Bitcoin, sinon redonner ses lettres de noblesse à cette rareté perdue qu'avait la monnaie ? »

Parfaitement, du moins en ce qui concerne le Bitcoin. La rareté, nous l'avons vu, fait partie des caractéristiques indispensables de la monnaie. Si cette rareté n'existe plus, on anéantit la réserve de valeur qui justifie l'utilité de la monnaie. Or, que fait le Bitcoin, sinon redonner ses lettres de noblesse à cette rareté perdue ?

La promesse de ne pas mettre plus de 21 millions d'unités en circulation reproduit en quelque sorte la rareté qui valut à l'or d'être choisi comme monnaie il y a des siècles, mais sans pâtir de l'unique défaut du métal jaune : sa vulnérabilité à la prédation. Car le Bitcoin repose également sur un système de gouvernance quasi inaltérable.

Il est peu probable, en effet, que soit modifiée la règle des 21 millions. Personne n'a d'ailleurs intérêt à espérer une telle modification. Le Bitcoin a instauré le principe du minage que l'on appelle aussi « la preuve de travail ». Concrètement, cela signifie que les cryptomonnaies sont créées par une communauté d'internautes, les « mineurs ». Ces derniers conçoivent et améliorent des algorithmes qui sécurisent la *blockchain*. En d'autres termes, ce sont eux qui valident les transactions effectuées dans un certain laps de temps en les regroupant dans un « bloc ». À chaque bloc « miné », c'est-à-dire validé, crypté et intégré à la *blockchain*, les mineurs sont eux-mêmes récompensés en Bitcoins[86]. Ils ont donc un intérêt personnel à ce que la valeur de l'actif soit la plus élevée possible. Aussi, œuvrent-ils naturellement à préserver l'intégrité des règles.

Quant aux détenteurs de Bitcoin, c'est précisément l'adhésion à des règles, à une forme d'appartenance politique, qu'ils achètent aussi. La règle des 21 millions d'unités en circulation est inviolable, mais elle n'interdit pas la possibilité de mettre à jour le protocole. Le Bitcoin concilie ainsi flexibilité et stabilité. Une fois qu'elles sont effectuées, les transactions sont irréversibles et ne peuvent donc pas être modifiées.

85. L'étalon-or désigne le système monétaire international en vigueur entre les années 1870 et 1914. Ses mécanismes de fonctionnement ont permis de garantir à l'époque la fixité des cours de change et la stabilité des prix. Voir notamment Bertrand Blancheton, *Maxi fiches – Histoire des faits économiques. De la révolution industrielle à nos jours*, 3e éd., Paris, Dunod, 2020.
86. Les détenteurs de Bitcoins procèdent aux échanges de leur cryptomonnaie au travers du réseau Bitcoin. Mais comment savoir qui doit combien à qui si personne n'enregistre toutes les transactions ? Pour remédier à ce problème, le réseau Bitcoin rassemble toutes les transactions réalisées sur une période dans une sorte de liste, qu'on appelle un « bloc ». Le rôle du mineur consiste à confirmer toutes ces transactions et à les consigner dans un grand registre.

Mais cela n'explique pas pourquoi le Bitcoin serait plus résistant à la censure ou aux pressions politiques ?

Pour vous en convaincre, arrêtons-nous un instant, si vous le voulez bien, sur le système des assignats. Pour soutenir la mise en place, sous la Révolution française, de cette monnaie fiduciaire, plusieurs lois ont été votées, toutes plus dures les unes que les autres. Ainsi, le pouvoir politique de l'époque a-t-il ordonné la fermeture provisoire de la Bourse de Paris ou encore la fin de la publication des taux de change de manière à limiter la spéculation. De lourdes amendes et de graves peines d'emprisonnement étaient également prévues pour toute personne surprise en train de vendre de l'or ou des pièces d'argent, ou de refuser un paiement en assignats. La non-acceptation de l'assignat devint même passible de la peine de mort, dès les premiers jours de la Terreur. Et comme l'interdiction du commerce au moyen des métaux précieux s'avéra insuffisante, on alla jusqu'à décider en mai 1794 que serait condamnée à mort toute personne qui aurait demandé en quelle monnaie le contrat serait conclu…

On pourrait supposer que l'épisode des assignats représente une parenthèse dans l'histoire de la monnaie. Mais ce n'est pas le cas. Au début du XVIIIe siècle, John Law de Lauriston[87] avait lui aussi tenté de démonétiser l'or et les matériaux précieux en interdisant de posséder du mobilier en or. Ces deux exemples montrent bien combien l'or a pour principal défaut d'être vulnérable aux pressions politiques.

Ce qu'il faut comprendre, c'est que la confiance dans le Bitcoin repose moins dans la monnaie elle-même que dans le protocole Bitcoin, à savoir l'ensemble des règles de base qui permettent le partage de données entre ordinateurs[88]. Ce dernier tient sur deux promesses : celle de limiter le nombre d'unités en circulation, d'une part, déjà évoquée, mais aussi celle de proposer une infrastructure fiable, d'autre part.

> « Pour bloquer le Bitcoin, il faudrait couper Internet. Les personnes qui investissent dans le Bitcoin parient que jamais aucun gouvernement ne s'y risquera. »

Parce qu'elle est décentralisée, l'infrastructure du Bitcoin est très compliquée à stopper, y compris dans un État très autoritaire, voire totalitaire[89]. Il y a dix ans, je n'aurais pas été aussi catégorique. Mais maintenant que le réseau s'est agrandi, que les mineurs sont aux quatre coins du monde, la seule solution qu'il reste aux gouvernements pour bloquer le Bitcoin, ce serait de couper Internet, avec les conséquences qu'on imagine sur l'opinion… Les personnes qui investissent dans le Bitcoin parient que jamais aucun gouvernement ne s'y risquera !

87. John Law (1671-1729), est un financier écossais. Après la mort de Louis XIV, le Régent fait appel à lui pour redresser les finances publiques. Il entreprend une vaste opération de monétisation de la dette fondée sur un échange des titres de dette publique contre des actions d'une société – la Compagnie perpétuelle des Indes – chargée de mettre en valeur les colonies. La spéculation sur les actions de cette compagnie va déboucher sur un krach monumental en 1720. Law est obligé de fuir à Venise où il meurt. En 1726, le cardinal de Fleury met un terme définitif à l'expérience Law et redéfinit la monnaie métallique qui circule dans le royaume. Il mène une politique de redressement budgétaire pour contenir la dette publique. Voir notamment Jean-Marc Daniel, *Histoire vivante de la pensée économique. Des crises et des hommes*, Montreuil, Pearson, 2021.
88. Les protocoles ne sont pas exclusifs aux cryptomonnaies. Sans eux, en effet, Internet ne pourrait pas fonctionner. Les courriels, par exemple, reposent sur plusieurs protocoles comme le protocole de transfert hypertexte, le fameux HTTP qui figure au début de chaque URL. Mais on doit au protocole Bitcoin d'avoir mis fin au « problème de double dépense » puisqu'il permet la création de devises numériques pouvant être négociées ou dépensées sans qu'aucune personne impliquée dans la transaction ne s'inquiète que l'argent ait *déjà* été dépensé. D'autres cryptomonnaies ont instauré leur propre protocole. Il en va ainsi de l'Ethereum dont le protocole est conçu autour de « contrats intelligents » *(smart contracts)*, des protocoles de transaction informatisés qui exécutent automatiquement les termes d'un contrat.
89. Seule la Chine s'y est jusqu'ici risquée. Nouvelle étape dans la guerre livrée contre le secteur des cryptomonnaies, Pékin vient d'ajouter le procédé d'extraction de cryptomonnaies, le « minage », dans sa « liste négative », autrement dit dans *« la liste des secteurs, des domaines et des entreprises restreints ou interdits aux investisseurs »*. Une décision qui ne surprend personne puisque la Chine avait déjà interdit d'autoriser le commerce des cryptomonnaies aux institutions financières, sociétés de paiement et plateformes Internet.

Ce qui est fascinant dans l'analyse que vous faites du Bitcoin, c'est qu'il suscite la confiance alors même que l'on ignore qui en est le créateur. Cette connaissance, cette familiarité, apparaît même presque superflue. Pourtant, on peut se demander si créer les conditions de la confiance ne devrait pas être du ressort des banques centrales, des acteurs que, pour le coup, nous connaissons bien ?

> Les banques centrales détestent les cryptomonnaies ! Elles les perçoivent comme un acte de défiance, comme un désaveu.

C'est pour cette raison que les banques centrales détestent les cryptomonnaies ! Elles les perçoivent comme un acte de défiance, comme un désaveu. Ce dont on peut convenir si l'on s'en tient à la théorie conventionnelle qui associe l'invention des banques centrales à la restauration de la confiance.

Mais toute une école issue du *public choice*[90] assimile la naissance des banques centrales à un système d'organisation de rente. Les banques centrales, dont la présence et l'*imperium* nous paraissent aller de soi, n'ont pas toujours existé ! Tout a commencé aux États-Unis avec le système de « banques libres », première étape vers l'uniformisation du système bancaire. La législation imposait alors un ensemble de conditions bien précises qui, si elles variaient d'un État à l'autre, comprenaient notamment la nécessité de couvrir l'émission de billets par l'achat d'obligations. Ainsi, les banques libres devaient-elles acheter des obligations émises par l'État fédéré ou l'État fédéral pour couvrir chaque billet.

Concrètement, cela fonctionnait de la manière suivante. La banque déposait ces obligations auprès d'un représentant de l'État qui, en échange, lui remettait la même valeur en billets. Si jamais la banque ne pouvait plus honorer une demande de remboursement de billets en pièces d'or ou d'argent, ce représentant la fermait et liquidait ses obligations pour rembourser les billets en circulation. L'obligation de couvrir l'émission de billets était donc à la source de l'instabilité de ce système. Il n'empêche que des banques libres stables existaient. Elles atténuaient le risque de faillite par le biais de la diversification et émettaient une plus faible proportion de billets. En général, elles n'émettaient pas de dette pour obtenir davantage de billets.

Si l'instabilité du système des banques libres a signé son arrêt de mort, la fonction de prêteur en dernier ressort lui a survécu. Pour de nombreux économistes, cela constitue d'ailleurs en soi un aléa moral : dès lors qu'une organisation est chargée de renflouer les banques, difficile de parler encore d'un système authentiquement capitaliste… Les banques centrales seraient nées de la volonté de socialiser les pertes des banques commerciales. Imposer le cours légal d'une monnaie permet de manipuler des flux de revenus avec une plus grande discrétion. C'est un jeu dangereux, mais que pratiquent en réalité les institutions monétaires. Si l'on en croit l'indice des prix à la consommation – qui exclut l'achat d'actifs comme les actions ou l'immobilier –, l'euro a ainsi perdu au moins 2 % de sa valeur chaque année. Et le dollar s'est déprécié, en pouvoir d'achat, de plus de 84 % depuis la fin des accords de Bretton Woods (lesquels avaient instauré un système monétaire basé sur la libre convertibilité des monnaies et la fixité des taux de change). Nos monnaies ont donc objectivement cessé d'être des réserves de valeur. On aurait tort cependant de limiter cette analyse aux pays occidentaux : la dilution de la monnaie est encore plus forte dans les pays gouvernés par des régimes autoritaires. Si l'on considère que les banques centrales sont nées dans l'objectif de stabiliser la monnaie, on n'a d'autre choix que de constater leur échec. D'autres observateurs, plus cyniques, affirmeront au contraire qu'elles n'ont jamais été inventées pour cela (mais au contraire pour « faciliter » la manipulation monétaire) et, donc, qu'elles remplissent parfaitement leur rôle… Mais c'est un rôle nuisible !

90. Développée dans les années 1960 aux États-Unis, la théorie des choix publics vise à analyser les phénomènes politiques à l'aide des méthodes économiques.

Tout cela donne encore davantage de crédit aux cryptomonnaies. Elles commencent en réalité à dissiper l'illusion selon laquelle l'émission monétaire serait une activité exclusivement « régalienne », parce ce qui est régalien serait plus sûr. En fait, rien, dans la définition de la monnaie que nous avons rappelée en début d'entretien, ne renvoie à quelque figure étatique que ce soit. Divisibilité, rareté, transposabilité : ces caractéristiques ne sont pas nécessairement l'apanage de l'État. Comment, demandera-t-on dès lors, les peuples ont-ils pu supporter un tel monopole indu, et souvent utilisé pour les tromper ? C'était précisément un *second best*… jusqu'à l'apparition des cryptomonnaies.

Mais ne pourrait-on pas envisager une coexistence entre celles-ci et des cryptomonnaies disons « publiques » ?

> « Le Bitcoin ne s'oppose pas à la création d'un écosystème avec des entreprises ou de nouveaux tiers de confiance. Il suppose seulement de renoncer au pouvoir de gonfler la valeur. »

Les banques centrales se sont positionnées pour émettre leur propre monnaie numérique et se passer ainsi des banques commerciales. Elles s'inspirent en partie des mécanismes à l'œuvre dans les cryptomonnaies en pensant que la vraie valeur ajoutée du Bitcoin réside dans la possibilité d'une désintermédiation totale. Or, le Bitcoin ne s'oppose pas à la création d'un écosystème avec des entreprises ou de nouveaux tiers de confiance. Il suppose seulement de renoncer au pouvoir de gonfler la valeur.

Le problème est que les monnaies numériques émises par les banques centrales, justement, ne sont pas dépourvues d'un tel pouvoir. De la *blockchain*, elles ne conservent que l'aspect technique, que le côté *buzzword*. Elles éclipsent, en revanche, l'esprit qui veut que la confiance numérique ne réside pas uniquement dans la technique, mais émerge aussi d'un cadre de règles qui garantit qu'il n'y aura pas de compromission sur la valeur de la monnaie.

De la part des banques centrales, cette omission n'est pas surprenante. Elle se comprend même aisément quand on sait combien ces monnaies numériques pourraient s'avérer pratiques pour mieux contrôler la masse monétaire ou encore le comportement des consommateurs… ceux-là même qu'on accuse aujourd'hui de trop épargner ! Les monnaies numériques des banques centrales permettraient certes aux politiques monétaires d'être plus efficaces, mais cela contredit précisément la philosophie initiale des cryptomonnaies et des Bitcoins.

Ne faut-il pas s'inquiéter du fait qu'une cryptomonnaie comme le Bitcoin ressemble de plus en plus à un investissement ? Cela ne revient-il pas aussi à trahir l'esprit originel ?

Par définition, tous les actifs sont spéculatifs. Si vous venez d'acheter une maison, il y a peu de chances que vous souhaitiez la voir perdre de la valeur au cours des années ! Ce caractère spéculatif présente notamment l'avantage de rendre le marché très liquide.

En revanche, ce qui s'avère encore problématique avec les cryptomonnaies, c'est la taille de la communauté. À l'échelle de la population mondiale, le nombre d'utilisateurs reste limité, malgré la croissance extrêmement rapide qu'a connue l'adoption des cryptomonnaies en 2021[91]. C'est pourquoi le moindre mouvement de

91. C'est en tout cas ce qu'ont constaté les chercheurs de la plateforme Crypto.com. Selon leur étude, le nombre de détenteurs d'actifs numériques dans le monde a plus que doublé au premier semestre 2021, passant de 106 millions d'utilisateurs en janvier 2021 à 221 en juin de la même année. Le rapport est disponible en ligne : https://crypto.com/images/202107_DataReport_OnChain_Market_Sizing.pdf [dernière consultation le 18 février 2022].

panique, la moindre phrase prononcée par un leader d'opinion de l'envergure d'Elon Musk peut provoquer des variations du cours aussi importantes et impressionnantes que celles que l'on a pu connaître avec le Bitcoin. Avec ses tweets décapants, tantôt encensant le Bitcoin, tantôt le descendant en flèche, le patron de Tesla est régulièrement accusé de manipulations. Bien qu'il se défende d'acheter à la baisse pour revendre ensuite au plus haut, le patron de Tesla est de ceux qui parviennent, grâce à leur influence sur les réseaux sociaux, à jouer avec le cours des cryptomonnaies. Une pratique pourtant interdite par les règles boursières et pour laquelle Elon Musk a déjà été condamné s'agissant du marché des actions…

Mais je ne doute pas que cette volatilité, comme l'impact des oracles des prescripteurs d'opinion, va s'amoindrir au rythme de l'extension du marché. Après tout, le Bitcoin est un actif qui n'a pas plus de dix ans d'existence. Ce n'est rien à l'échelle de l'histoire des monnaies ! Et dans dix ans, qui peut dire si Elon Musk sera toujours de ce monde ? Depuis la Terre ou l'espace, le patron de Tesla peut, si cela lui chante, critiquer le minage de Bitcoin pour son impact environnemental et promouvoir des Altcoins comme le Dogecoin[92]… Tout dépend de la confiance et du crédit que chacun accorde à sa parole. Mais cela vaut pour tous les actifs. Aucun n'est exempt de manipulation. Ce qui est en cause, ce ne sont pas les actifs eux-mêmes mais la réaction de la communauté et la crédibilité accordée aux prescripteurs d'opinion.

> « Rien n'interdit théoriquement d'imaginer que demain la confiance dans le Bitcoin s'effondre. »

Comme tous les actifs, le Bitcoin repose sur un système d'offre et de demande, administré en l'occurrence ici par une technologie. Rien n'interdit théoriquement d'imaginer que, demain, la confiance dans le Bitcoin s'effondre. Elle pourrait chuter pour des raisons culturelles comme la perte de confiance dans le numérique. La confiance fait appel à des éléments très subjectifs et d'autant plus pour ceux pour qui la monnaie reste encore quelque chose de tangible.

Donc nous voilà comme revenus au point de départ… Car, si je vous suis bien, ni le Bitcoin ni la technologie blockchain qui le soutient participent réellement à repenser la confiance ?

Pas tout à fait. Si on laisse ses Bitcoins sur une plateforme tierce, se pose effectivement de nouveau le problème de confiance. Chaque personne qui achète des Bitcoins a néanmoins toujours la possibilité de les rapatrier pour les stocker sur un *hardware wallet*[93], grâce auquel il a en quelque sorte ses bitcoins « chez lui » … Mais cette matérialisation fait fatalement réapparaître les problèmes liés à la détention physique : personne n'est à l'abri de voir ses clés cryptographiques dérobées… ou simplement de les oublier ! C'est là que réside en effet la contrepartie à l'absence de tiers de confiance. Le Bitcoin requiert une clé privée dont la perte siffle la fin de la partie… pour toujours.

92. Mot-valise composé de « alternative » et « coin », Altcoin désigne toutes les cryptomonnaies alternatives au Bitcoin. Présenté comme une blague le 6 décembre 2013, le Dogecoin est une cryptomonnaie avec pour logo le portrait du Shiba Inu, chien du même « Doge ». Le Dogecoin a rapidement développé sa propre communauté pour atteindre une capitalisation de 60 millions de dollars en janvier 2014. Récemment encore, son cours s'est envolé, sur fond de rumeurs d'option de paiement DOGE chez Tesla.
93. Sorte de portefeuille matériel qui protège les fonds qui y sont déposés et permet, avec un bon niveau de sécurité, l'envoi et la réception de Bitcoins depuis n'importe quel appareil, même compromis.

> Le Bitcoin règle de façon probante le problème de défiance que l'on peut nourrir à l'égard des banques. Il ne règle en rien le problème de la confiance vis-à-vis de l'homme.

Avec les Bitcoins, la responsabilité individuelle touche donc à son paroxysme. En cela, on se rapproche davantage de la monnaie métallique que de la monnaie scripturale. Le Bitcoin augmente la rareté et règle de façon probante le problème de méfiance, voire de défiance, que l'on peut nourrir à l'égard des banques. Il ne règle en rien le problème de la confiance vis-à-vis de l'homme.

Qu'en est-il du contrat intelligent ? De quelle façon les smart contracts peuvent-il apporter une réponse au problème de confiance en matière contractuelle ?

Je porte un regard sceptique sur les *smart contracts* qui visent à automatiser un certain nombre de procédés contractuels. Le commerce, physique ou non, requiert encore de s'en remettre à de trop nombreux facteurs pour attester la fiabilité et la qualité. Aussi, vouloir tout automatiser me semble utopique. Je pense qu'il faut séparer le bon grain de l'ivraie, distinguer les applications crédibles, car relevant de transactions simples, de celles qui, parce que trop complexes, ne peuvent se passer de tiers de confiance, d'arbitre.

Par exemple, je ne crois pas une seule seconde que la *blockchain* va s'imposer dans des domaines comme le cadastre ou l'assurance. Cela me paraît, en effet, trop complexe de certifier la propriété foncière. Que se passe-t-il par exemple si aucun accord n'est trouvé sur la délimitation d'une parcelle ? Concernant le secteur de l'assurance, peut-on déclencher des remboursements de manière automatique si aucun expert ne vient constater le sinistre ? Dans ces domaines, comme dans bien d'autres, impossible de se passer de tiers de confiance. Il faut un arbitre, ne serait-ce que pour trancher les litiges. Les *smart contracts* ont sans doute un avenir, mais au sein d'une utopie cyber punk !

Jean-David Benassouli et Nathalie Malicet

Garantir la confiance numérique : le rôle plus que jamais critique de l'audit

Jean-David Benassouli – Associé, Responsable de l'activité Data Intelligence de PwC France et Maghreb

Associé responsable de l'activité Data Intelligence pour PwC France et Maghreb, Jean-David Benassouli a pour mission de piloter les équipes et les activités en matière de Data Analytics et Intelligence Artificielle au sein des différents métiers de PwC France (conseil, audit, transactions, juridique et fiscal). Son rôle est d'accompagner la transformation « Data driven » des entreprises ainsi que des métiers de PwC en France et Maghreb. L'activité Data Intelligence de PwC France compte 300 experts (dont 50 data scientists) pour aider les entreprises de toutes tailles et tous secteurs d'activité confondus à repenser leur business et leur mode d'organisation, à gérer leurs risques et à respecter les réglementations dans un contexte où la donnée est au cœur de leurs préoccupations.

Jean-David Benassouli a précédemment occupé le poste de Directeur Exécutif chez Accenture Digital, où il a contribué au développement des offres Big Data pour l'Europe, l'Afrique et l'Amérique Latine pour les secteurs des Télécommunications, Médias & High Tech, et a ensuite pris la responsabilité de la practice Digital Data Management d'Accenture pour l'ensemble des industries en France.

Il co-préside par ailleurs la commission Data de Syntec Conseil.

Jean-David Benassouli est ingénieur en informatique, diplômé de l'EFREI ainsi que de l'IAE Paris La Sorbonne, il a débuté sa carrière chez Capgemini.

Nathalie Malicet – Expert-comptable, Commissaire aux comptes, Associée chez Anexis ; Présidente de la Commission Prospectives et Innovation de la Compagnie Nationale des Commissaires aux Comptes (CNCC)

Expert-comptable, Commissaire aux comptes et Expert Judiciaire, Associée au sein du cabinet Anexis (Bordeaux), Nathalie Malicet est Membre du bureau national de la CNCC et Présidente de la Commission Prospectives et Innovation de la CNCC depuis novembre 2019. La commission Prospectives et Innovation de la CNCC a pour mission d'apporter aux professionnels les outils et les compétences nécessaires pour répondre aux enjeux digitaux actuels et de demain et ainsi de créer les conditions de la confiance numérique, conditions nécessaires à la performance de l'économie dans son ensemble.

Engagée sur les problématiques de cybersécurité et de digitalisation, elle est la coconceptrice des outils « CyberAUDIT » & « RGPDAudit » développés par la CNCC pour offrir aux commissaires aux comptes des supports opérationnels aux prestations qu'ils réalisent auprès des entités économiques, dans le cadre de la sensibilisation à la sécurisation des données.

Elle préside par ailleurs la Compagnie des Experts de Justice près la Cour d'Appel de Bordeaux.

Si les données sont au cœur de l'économie numérique, la confiance numérique suppose de réduire au maximum les problèmes liés au manque de gouvernance de la donnée, notamment de qualité des données et à leur sécurisation.

Un défi de taille pour tous les commissaires aux comptes, qui se retrouvent, au titre de leur activité d'audit et de certification des comptes, en situation d'émettre une opinion sur ces données. Garants de la relation entre les entreprises et leurs parties prenantes, ils participent plus largement à bâtir la société de la confiance numérique.

Dans un monde de plus en plus pénétré par le digital, la donnée et l'intelligence artificielle, la profession d'auditeur risque moins de disparaître que de voir son rôle renforcé.

Que recouvre l'idée de confiance numérique dans le monde de l'audit ?

Nathalie Malicet : Confiance et audit sont, pour moi, deux notions inextricablement liées dans la mesure où un audit représente l'occasion de qualifier les comptes sur lesquels porte notre pratique. En revanche, confiance et numérique semblent être deux termes opposés et l'expression « confiance numérique » relève presque de l'oxymore.

Dans les plus petites entreprises, le numérique véhicule le message traditionnellement associé aux antibiotiques et la confiance qui lui est assortie. Automatique, le numérique ne pourrait que produire des vérités. Qui ne voudrait pas que cela soit le cas ? Personne. Néanmoins, la perte de confiance peut se jouer à plusieurs niveaux.

On peut ainsi rencontrer des problèmes de paramétrage ou une maîtrise insuffisante qui se traduisent, au sein des organisations, par des procédés pourvoyeurs de données plutôt fausses que vraies. Mal maîtrisé, le numérique peut alors produire l'effet inverse de celui qu'on lui attribue intuitivement. Il peut également engendrer un effet d'opacité. Toutes les équipes ne savent pas comment fonctionnent les outils qu'elles utilisent. Elles constatent qu'elles ont des données qui entrent et sortent de traitements automatisés mais sans possibilité aucune de vérifier si tel est bien le cas. Aussi, n'ont-elles d'autre choix que de reporter leur confiance sur ceux qui construisent machines et outils.

Le triptyque de notre métier reste donc finalement le même : les contrôles généraux de l'informatique qui se penchent autant sur la gouvernance que sur la sécurité et l'organisation du système ; les contrôles d'application et, aujourd'hui, des algorithmes ; et, enfin, la data, que l'on travaille quasiment systématiquement aujourd'hui. Que ce triptyque continue de s'appliquer témoigne à mon sens du fait que la confiance dans les chiffres a toujours été recherchée, par nous, commissaires aux comptes et auditeurs, comme par les entreprises.

> « La question de la confiance numérique a en fait émergé dès l'instant où la data a, si je puis dire, pris son indépendance. »
>
> Nathalie Malicet

La question de la confiance numérique a en fait émergé dès l'instant où la data a, si je puis dire, pris son indépendance…

Justement, quelle promesse la data offre-t-elle pour votre profession en termes de confiance apportée à la qualité des comptes ?

Jean-David Benassouli : Je distingue deux grandes évolutions sur les cinq dernières années. D'une part, l'*upskilling*[94] des auditeurs, qui se sont progressivement mais véritablement approprié tous les outils de collecte, de manipulation et de visualisation des données. Les auditeurs sont plus outillés qu'auparavant et cela constitue un vrai changement de paradigme. D'autre part, la montée en puissance de la visualisation, qui permet de repérer de manière graphique des tendances, des éléments relatifs au business, tout autant que de potentielles zones de risques ou sujets à analyser. Cette technique est vraiment différenciante par rapport aux tableaux Excel que les auditeurs avaient en général jusqu'ici à leur disposition. Elle nous offre notamment la possibilité d'aller beaucoup plus vite et plus loin qu'auparavant dans la compréhension des enjeux et de la réalité de l'activité de l'entreprise auditée.

En outre, l'utilisation des outils de data visualisation dans le cadre de la réalisation de la mission d'audit a contribué à un changement important dans les échanges et la collaboration avec les clients. Mieux à même d'expliquer leurs analyses et points d'attention, les auditeurs ont pu davantage impliquer leurs clients, et leur expliquer les travaux, leurs étapes, et les multiples demandes de documentation.

> « Les data visualisation ou le *process mining* permettent de faire, grâce à la data, des zooms sur des données sélectionnées, apportent de la confiance et potentiellement mettent en lumière de manière plus explicite et collaborative des zones de risques à approfondir. »
>
> Jean-David Benassouli

On assiste également au développement de ce que l'on appelle les *process mining*, ou *process intelligence*. Ces audits sont menés dans les entreprises pour mettre la donnée au service des processus. L'idée derrière ces diagnostics est ambitieuse mais relativement simple à comprendre. Il s'agit ni plus ni moins que de se concentrer exclusivement sur les données. Pour l'instant, nous en sommes encore à la première étape, qui consiste à récupérer de la donnée en grande quantité. Ce n'est qu'une fois que cela sera fait que nous pourrons passer à l'étape suivante consistant à travailler sur des simulations et prédictions.

Quels obstacles empêchent encore d'enclencher pleinement cette seconde phase de simulation et prédiction ?

Jean-David Benassouli : Le problème pour nous ? Intervenir au sein d'entreprises dont le pilotage est souvent opéré par un millefeuille de systèmes d'information, issu de fusions, d'acquisitions et de consolidations successives. Si les *process* apparaissent digitalisés, la réalité est en fait bien différente : beaucoup de saisies manuelles, de réconciliations ou consolidations des données issues des différents systèmes… Soit autant de zones de risques pour des données manquantes, des données en doublon : un risque pour la qualité des données. Cela impacte *in fine* la confiance numérique.

94. C'est-à-dire le processus de perfectionnement permettant à un collaborateur de monter en compétences dans la compréhension, la manipulation, l'analyse et la visualisation de données, y compris en quantités importantes, tout en intégrant ces compétences au cœur de l'existant de son métier.

Nathalie Malicet : Grâce à la puissance informatique, on pourrait techniquement regarder toutes les données : mais je ne crois pas que cela suffirait. Je rejoins Jean-David sur ce point, des *process* de qualité n'évitent pas l'entrée de données fausses. C'est pourquoi, j'en suis convaincue, nous devons auditer également tout ce qui se situe autour de l'entreprise si l'on veut apporter une « vérité vraie ». On ne peut, en effet, estimer la qualité des données recueillies que si l'on se pose la question d'auditer aussi la matérialité des éléments qu'elles décrivent.

> « Les tests réalisés par sondages, et non sur une population globale, sont aujourd'hui au cœur de la démarche d'audit dictée par les normes d'exercice professionnel. »
>
> Nathalie Malicet

Il ne faut pas non plus perdre de vue que les tests réalisés par sondages, et non sur une population globale, sont aujourd'hui au cœur de la démarche d'audit dictée par les normes d'exercice professionnel.

Bien sûr, nous possédons tous des outils extracteurs de données qui nous permettent de faire émerger des points de contrôle et de détecter d'éventuelles anomalies sur des bases de données importantes. Or, quand surgissent des anomalies, que la liste soit courte ou longue, se posera toujours la question de savoir si l'on tente de traiter une par une chacune de ces anomalies ou si, au contraire, l'on essaie de déterminer des sous-groupes et de rechercher des indications au travers de sondages réalisés sur ces sous-ensembles. Dans ce cas précis, la data va nous apporter un soutien inestimable. Toujours est-il que l'auditeur ne peut pas s'affranchir des normes qui encadrent strictement son métier, tout comme des contraintes de temps et de budget qui pèsent sur lui. C'est pourquoi nous faisons, *in fine*, le choix de travailler par sondage.

Le problème, c'est que les entreprises attendent beaucoup de nous. Sous prétexte que nous disposons d'outils pour extraire les données, elles s'imaginent que nous voyons tout, que nous traitons tout ! Récemment encore, le directeur administratif et financier d'un grand groupe me confiait rêver d'un commissaire aux comptes « augmenté », c'est-à-dire qui ne se contenterait plus seulement de certifier ses comptes. *« Ce serait encore mieux*, m'a-t-il dit, *s'il pouvait aussi garantir que mon système est sûr et impossible à pirater ! »* Les entreprises espèrent nous voir très bientôt certifier que les systèmes eux-mêmes produisent des données de qualité. C'est un objectif qui semble aujourd'hui inatteignable.

> « Les entreprises attendent beaucoup de nous. Elles espèrent nous voir très bientôt certifier que les systèmes eux-mêmes produisent des données de qualité. C'est un objectif qui semble aujourd'hui inatteignable. »
>
> Nathalie Malicet

Notre rôle consiste aussi à alerter les dirigeants sur les risques internes mais, aujourd'hui, je crois que nous devons surtout viser la résilience, c'est-à-dire être capables de détecter les risques, d'en limiter les conséquences et permettre à l'entité de reprendre son activité le plus rapidement possible. Depuis quelques années, je plaide pour la création d'une cotation, une sorte de « nutri-score » des systèmes d'information. Si, en tant que commissaires aux comptes, nous parvenions à attester que telle ou telle entreprise attache un soin tout particulier à la protection des données qu'elle traite, alors nous ferions un pas de géant vers la confiance numérique.

> « Je plaide pour la création d'une sorte de « nutri-score » des systèmes d'information. Si les CAC parvenaient à attester du soin qu'une entreprise attache à la protection de la donnée, nous ferions un pas de géant vers la confiance numérique. »
>
> Nathalie Malicet

Où en sont les entreprises sur ces sujets, les petites comme les grandes ?

> En termes de collecte, de manipulation et visualisation des données, le coût d'entrée reste encore très élevé pour les petites entreprises et donc peu amortissable.
>
> Jean-David Benassouli

Jean-David Benassouli : En termes de collecte, de manipulation ou de visualisation des données, le coût d'entrée reste encore très élevé pour les petites entreprises, et donc peu amortissable. Dans les grandes entreprises, plus matures et équipées de délégués à la protection des données[95], ce que l'on appelle fréquemment la transformation « data driven » est plus souvent très avancée, avec des interlocuteurs dédiés, des responsables des *process*, de la gouvernance, des plateformes, etc.

Nathalie Malicet : La Compagnie Nationale des Commissaires aux Comptes a œuvré pour démocratiser le *process mining* en accompagnant notamment une *startup* qui voulait développer une solution adaptée au monde des TPE. Mais ces *process* restaient longs et coûteux au niveau de la cartographie des données. Nous sommes donc arrivés à la conclusion que ce n'était peut-être pas la meilleure idée, du moins pour les plus petites entreprises.

Cela est d'autant plus frustrant, qu'en raison de systèmes d'information moins complexes, de processus plus « standards », le *process mining* serait paradoxalement plus simple dans ces petites entreprises. Mais, sur ces sujets, elles restent confrontées à des temps d'intervention d'audit colossaux par rapport à leurs moyens. Elles ne voient donc pas l'intérêt d'investir dans un outil qui reste trop cher par rapport au bénéfice qu'elles pourraient en retirer. C'est pourquoi nous attendons beaucoup de la capacité des grandes entreprises à industrialiser les outils et, ce faisant, à les proposer à un coût plus accessible.

Évoquons l'intelligence artificielle. Quelles opportunités pour l'audit ? Quelles en sont, au contraire, les limitations ?

> Vous pouvez disposer des meilleurs algorithmes, si, en amont, vous n'avez pas fait le plein de carburant, c'est-à-dire de données, vous n'irez nulle part…
>
> Jean-David Benassouli

Jean-David Benassouli : La voiture autonome ou les algorithmes de recommandation représentent de véritables cas d'usage d'intelligence artificielle. En revanche, quand on évolue dans le monde de l'audit réglementé, le premier sujet auquel on doit se confronter est tout bêtement celui des données de nos clients. Des données qui n'existent pas toujours, qui ne sont pas toujours exhaustives, et/ou de bonne qualité, etc. Vous pouvez disposer des meilleurs algorithmes, si, en amont, vous n'avez pas fait le plein de carburant, c'est-à-dire de données, vous n'irez nulle part…

Le second sujet concerne la réglementation. On ne peut pas stocker *ad vitam aeternam* les données de nos clients. D'une année sur l'autre, les travaux doivent être certes documentés, mais les données ne peuvent pas

95. Le délégué à la protection des données, connu sous l'acronyme DPO, est chargé de mettre en œuvre la conformité au Règlement européen sur la Protection des Données (RGPD) au sein des entreprises et des organisations. Dans certaines situations, sa désignation est même obligatoire.

être conservées. Les utiliser pour un autre usage s'avère d'ailleurs extrêmement compliqué et/ou interdit par les règlementations. *De facto*, notre champ des possibles en matière d'intelligence artificielle n'est pas très large aujourd'hui par rapport à d'autres métiers et secteurs.

> « Compte tenu de l'impossibilité de conserver des données en raison de la réglementation, notre champ des possibles en matière d'intelligence artificielle n'est pas très large aujourd'hui par rapport à d'autres métiers et secteurs. »
>
> Jean-David Benassouli

Nathalie Malicet : Et ce, quoi qu'en pensent les éditeurs de logiciels qui interagissent avec la profession pour leur vendre des solutions d'intelligence artificielle ! Nombreux sont ceux qui s'imaginent que ces solutions vont faire des miracles… Ils omettent un détail de taille : il faut un grand volume de données pour espérer obtenir de l'apprentissage et donc de l'intelligence artificielle.

Faut-il d'ores et déjà envisager d'auditer les algorithmes ?

Jean-David Benassouli : En tant que consultant, et non en tant qu'auditeur, je constate que ce sont les métiers de la banque qui sont les plus demandeurs en termes d'audit d'algorithmes. Ces professions font notamment face à des problématiques liées au respect de la vie privée. Accorder une assurance, refuser un prêt, cela est nécessairement lié à la vie personnelle des personnes concernées. Sur ces sujets, des missions d'audit d'algorithmes sont de plus en plus fréquentes.

Mais auditer les algorithmes ne saurait suffire. Il nous faut auditer aussi les outils, la gouvernance, les données. Dans les entreprises, cela implique qu'un collaborateur s'occupe précisément de ces questions, que la gouvernance soit incarnée, c'est souvent le rôle d'un *Chief Data Officer* (ou Directeur des données).

Concernant les processus, on ne peut pas non plus se contenter de savoir comment les choses sont faites. Il conviendrait au contraire de déterminer, par exemple, quelle variable influence le plus le *scoring* d'un crédit.

Aucune lacune ne saurait être acceptée non plus du côté de l'auditeur. Ce dernier doit pouvoir se reposer sur une connaissance approfondie du métier, seule à même de lui permettre de comprendre les décisions, mais aussi de repérer, s'il y en a, toute reproduction de biais.

Nathalie Malicet : Dans un futur proche, la masse d'informations produite par les algorithmes sera telle qu'il faudra se poser la question de la transparence et de la loyauté des algorithmes. Demain, si les décisions sont prises en fonction de ces algorithmes, des problèmes apparaîtront nécessairement. C'est à ce moment-là seulement que les audits d'algorithmes se développeront car, pour l'instant, les entreprises ne le demandent pas encore.

> « Dans un futur proche, la masse d'informations produite par les algorithmes sera telle qu'il faudra se poser la question de la transparence et de la loyauté des algorithmes. »
>
> Nathalie Malicet

Jean-David Benassouli : Conceptuellement, on ne voit pas comment ce marché n'existerait pas. Cela ne doit pas occulter d'autres manières d'instaurer une relation avec un algorithme. Il est en effet tout à fait possible d'envisager de le recoder, ou encore d'observer ce qui se passe en entrée et en sortie. Mais ces méthodes ont un coût et nécessitent de nombreuses expertises, ce qui ne les rend accessibles qu'à une minorité d'entreprises seulement.

Quel rôle les auditeurs peuvent-ils encore jouer dans un monde voué à être de plus en plus dominé par l'intelligence artificielle ?

Jean-David Benassouli : Je ne crois pas au scénario d'une disparition de la profession. L'auditeur ne risque pas d'être remplacé par la machine, il sera au contraire « augmenté » grâce aux outils et apports du numérique. Cela suppose en revanche d'apprendre à manipuler les données, d'acquérir de nouvelles compétences, ce qui ne relève d'ailleurs pas de l'âge : c'est une question d'ouverture au changement, de culture et d'état d'esprit.

> « Je ne crois pas au scénario d'une disparition de la profession. »
>
> Jean-David Benassouli

Au-delà, l'esprit critique, le jugement professionnel, l'élaboration de l'opinion et la prévention des risques demeurent des activités résolument humaines. La machine, aussi intelligente soit-elle, ne dispense pas l'auditeur d'être responsable de ce qu'il signe. Que les travaux aient été réalisés grâce à un algorithme rend simplement l'auditeur responsable de cet algorithme, autant que de ses résultats.

> « L'automatisation de certaines tâches de l'audit va permettre aux auditeurs de se concentrer sur des activités à très forte valeur ajoutée. »
>
> Jean-David Benassouli

La technologie va en revanche nous aider à rendre plus pertinent, et attractif, le travail de l'auditeur, en supprimant tout un ensemble de tâches répétitives et basiques. On assiste déjà à une automatisation de certaines tâches de l'audit. Une grande partie des tâches de manipulation de données va pouvoir, à terme, être industrialisée de façon à préparer le travail des auditeurs financiers et IT. Ceux-ci pourront ainsi concentrer leur temps sur des activités à très forte valeur ajoutée, des activités essentiellement humaines et inaccessibles aux machines.

Nathalie Malicet : Demain, les auditeurs devront plus que jamais mettre en œuvre leur jugement professionnel pour évaluer les informations qui leur sont transmises. On évolue vers des tâches plus intéressantes, qui remettent l'humain au cœur du système.

Le recours massif au* cloud *est-il une solution pour sécuriser les accès et les échanges de données ?

Nathalie Malicet : Je porte un regard réservé, presque sévère, sur ce sujet. Le *cloud* apporte certes des moyens et des ressources dont ne disposent peut-être pas les entreprises en interne. Mais on ne peut pas ignorer non plus les questions de souveraineté numérique qu'il soulève. Attention, donc, à ne pas faire confiance à n'importe quel *cloud* les yeux fermés !

> « Le *cloud* apporte certes des moyens et des ressources mais, on ne peut pas ignorer les questions de souveraineté numérique qu'il soulève. »
>
> Nathalie Malicet

Jean-David Benassouli : Pour ma part, je suis beaucoup plus optimiste. Je conseille même à mes clients d'embrasser cette technologie, rapidement mais pas n'importe comment. Les sujets évoqués tout au long de cet entretien ont mis vingt ans à évoluer. Une telle lenteur s'explique aisément au regard du cadre réglementaire qui régit la profession ! On doit pouvoir trouver un moyen de la rendre plus technophile…

Le *cloud* nous offre la possibilité, sans investissement en termes d'infrastructure ni vraiment de moyens humains complémentaires, de traiter l'ensemble des données, et ce peu importe la volumétrie. Cette capacité

de traitement et cette productivité maximale pourront s'avérer très utiles, entre décembre et février notamment, période de l'année où, en raison de la clôture des comptes, l'on a plus que jamais besoin de telles capacités d'élasticité.

L'expérience que nous avons pu acquérir collectivement autour de la nécessaire gouvernance des données nous instruit quant à la façon d'aborder la transition vers le *cloud* : avec raison, organisation, et en articulant l'activité quotidienne de tous les acteurs de l'entreprise avec l'introduction de cette technologie. Faute de quoi, les chances de créer de nouvelles zones de risque et d'opacité seront grandes.

Les autres publications de l'Institut Messine

- ***Éclipse ou crépuscule ? Pourquoi les Bourses n'ont plus la cote***
  Février 2021, *Note* – par Catherine Lubochinsky (Économiste, Professeur en sciences économiques à l'Université Paris 2 Panthéon-Assas), avec Philippe Manière (Président de Vae Solis Communications)

- ***Comment l'État se défausse sur les entreprises : Neuf regards***
  Juin 2020, *Recueil* – sous la direction d'Anne de Guigné (Journaliste)

- ***Les patrons des PME et d'ETI françaises vendent-ils trop tôt et pourquoi ?***
  Mars 2019, *Rapport* – sous la présidence de Baudouin d'Hérouville (Capital Investisseur)

- ***Le lanceur d'alerte dans tous ses états – Guide pratique et théorique***
  Novembre 2018, *Rapport* – sous la présidence de Pascale Lagesse (Avocat, spécialiste du droit social, Associée, cabinet Bredin Prat)

- ***Repenser le travail et faire converger les protections pour réconcilier tous les actifs***
  Novembre 2017, *Rapport* – sous la présidence d'Emmanuelle Barbara (Avocat, Associé-Gérant d'August Debouzy, Spécialiste en droit du travail, de la sécurité sociale et de la protection sociale)

- ***Comprendre et évaluer les entreprises du numérique***
  Octobre 2017, *Livre* co-édité avec Eyrolles – par François Meunier (Économiste, auteur et chroniqueur)

- ***Les chiffres dans le débat public : vérités et mensonges***
  Décembre 2016, *Note* – par Jean-Marc Daniel (Statisticien, Professeur d'économie à ESCP-Europe-Paris)

- ***Taux d'intérêt négatifs – Douze regards***
  Janvier 2016, *Recueil* – sous la direction de Natacha Valla (Économiste)

- ***Norme et Jugement sont-ils compatibles ?***
  Juin 2015, *Rapport* – sous la présidence d'Hervé Philippe (Directeur Financier et membre du Directoire de Vivendi)

- ***L'excès d'information financière nuit-il à l'information financière ?***
  Juillet 2015, *Note* – par Sophie Chassat

- ***Fiscalité et politiques publiques : Peut-on vraiment orienter le comportement des entreprises par l'impôt ?***
  Mars 2015, *Rapport* – sous la présidence de Gauthier Blanluet (Avocat associé de Sullivan & Cromwell)

Toutes nos publications sont téléchargeables sur notre site internet : **www.institutmessine.fr**

Dépôt légal : Mars 2022 – N° d'Imprimeur : 83747
Imprimerie Compédit-Beauregard, Z.I., La Ferté-Macé 61600 – Tél. 02 33 37 08 33

Gouvernance

Les opinions exprimées dans le présent Recueil n'engagent ni les personnes citées, ni les organisations qu'elles représentent.

Président

Michel LÉGER	Commissaire aux comptes, Président du Conseil de surveillance de BDO France.

Comité Directeur

Philippe AUDOUIN	Directeur Général Finances, Membre du Directoire d'Eurazeo.
Jean BOUQUOT	Commissaire aux comptes, Président d'honneur de la CNCC.
Dominique CARLAC'H	Présidente de D&C ; Vice-Présidente et Porte-parole du MEDEF.
Jean-Marc ESPALIOUX	Senior Advisor de Montefiore Investment.
François HUREL	Président et Fondateur de l'Union des Auto-Entrepreneurs.
Denis LESPRIT	Commissaire aux comptes, Associé fondateur d'AEC ; Président d'honneur de la CNCC.
Monique MILLOT-PERNIN	Commissaire aux comptes, Ancien Membre du Comité Monétaire de la Banque de France.
Yves NICOLAS	Commissaire aux comptes, ancien Associé de PwC ; Président d'honneur de la CNCC.
Yannick OLLIVIER	Commissaire aux comptes, Président de la CNCC ; Directeur général du groupe Fiteco.
Pascale PARQUET	Directeur au sein du Secrétariat Général du Groupe BPCE ; Membre de la Commission nationale des sanctions.
Helman LE PAS DE SÉCHEVAL	Secrétaire général et Membre du Comité exécutif de Veolia ; Membre du Collège de l'Autorité des marchés financiers.
Didier-Yves RACAPÉ	Commissaire aux comptes, Associé fondateur du Groupe Volentis ; Ancien Président de la Compagnie Régionale des Commissaires aux Comptes de Paris.

Conseil d'Orientation

Philippe BILGER	Magistrat honoraire ; Président de l'Institut de la parole.
Gauthier BLANLUET	Avocat Managing Partner de Sullivan & Cromwell en France ; Professeur de droit fiscal des affaires à l'Université de Paris II.
Francis CHARHON	Directeur général de Scala Mécénat ; ancien Directeur Général de la Fondation de France.
Geneviève FÉRONE-CREUZET	Fondatrice et Présidente de Casabee ; Cofondatrice et Associée de Prophil.
Yves GÉRARD	Médiateur auprès de Société Générale et du groupe Crédit du Nord ; Président du Cercle des médiateurs bancaires.
Antoine GOSSET-GRAINVILLE	Avocat, Co-fondateur et Associé de BDGS Associés.
Anne-Marie IDRAC	Présidente de France Logistique ; ancienne Secrétaire d'État au Commerce extérieur et aux Transports ; Administratrice de sociétés.
Henri NALLET	Président de la Fondation Jean Jaurès ; ancien ministre de la Justice.
Marie-Pierre PEILLON	Directrice de la Recherche et de la Stratégie ESG de Groupama Asset Management ; Présidente de la commission Finance durable de l'Association Française de la Gestion financière ; ancienne Présidente de la Société Française des Analystes Financiers.
Guylaine SAUCIER	Administratrice de sociétés ; Fellow de l'Ordre des Comptables Agréés du Québec ; ancienne PDG du groupe Gérard Saucier Ltée.
Natacha VALLA	Présidente du Conseil national de productivité ; Doyenne de l'école du management et de l'innovation de Sciences-Po.
Jean-Marc VITTORI	Éditorialiste, *Les Échos*.

Institut Messine

www.institutmessine.fr