Enjeux numériques

Faire confiance au temps du numérique

UNE SÉRIE DES
ANNALES DES MINES
FONDÉES EN 1794

N° 13 - MARS 2021

UNE SÉRIE DES
ANNALES DES MINES
FONDÉES EN 1794

ENJEUX NUMÉRIQUES

Série trimestrielle • N°13 - Mars 2021

Photo de couverture :
Alexej von Jawlensky (1864-1941), *Symphony en Rose*, huile sur toile, 1929. Stadelsches Kunstinstitut, Francfort sur le Main.
Photo © Gordon Roberton Photography Archive/ BRIDGEMAN IMAGES

Iconographie
Christine de Coninck

Abonnements et ventes
COM & COM
Bâtiment Copernic - 20, avenue Édouard-Herriot
92350 LE PLESSIS-ROBINSON
Sébastien Rodriguez
Tél. : 01 40 94 22 22 - Fax : 01 40 94 22 32
s.rodriguez@cometcom.fr

Mise en page : Nadine Namer
Impression : EspaceGrafic
N° ISSN : 2607-9984

Éditeur délégué
FFE – 15, rue des Sablons - 75116 PARIS
www.ffe.fr

Régie publicitaire : Belvédère Com
Fabrication : Yaël Sibony
Yaël.Sibony@belvederecom.fr
Tél. : 01 53 36 20 46
Directeur de la publicité : Bruno Slama
Tél. : 01 40 09 66 17
bruno.slama@belvederecom.fr

Faire confiance au temps du numérique

Nouveaux principes d'actions et cas d'usage

Numérique et information

Hors dossier

Ce numéro a été coordonné par Côme BERBAIN et Bertrand PAILHÈS

Introduction

Par **Côme Berbain**
Directeur de l'Innovation du groupe RATP et directeur du programme « Véhicule autonome »
et **Bertrand Pailhès**
Directeur des Technologies et de l'Innovation de la CNIL

« Faire confiance ». Alors que les rapports sociaux semblent se tendre et les repères hérités de la société industrielle disparaître, alors que le numérique constitue un des principaux facteurs de cette transformation des sociétés modernes, « faire confiance » est un *mantra* que peu de responsables politiques ou d'experts pourraient prétendre revendiquer. Et pourtant, le déploiement de la société de l'information depuis 30 ans a permis la constitution d'avancées aussi majeures pour le progrès que l'encyclopédie Wikipédia, bâtie par des milliers d'anonymes sans lien personnel entre eux, de nouvelles technologies fondées sur un *consensus* scientifique global ou le développement d'outils informatiques ouverts, au service de tous.

La confiance dans le monde numérique est une notion mal définie, dans laquelle des intérêts divers se retrouvent, selon que l'on parle de technologies, de contenus ou de contributeurs. Dans de nombreux cas, c'est avant tout une question de règles, de procédures et de standards acceptables par tous et dont le respect conditionne un engagement sincère et sécurisé par chacun. Ces règles sont parfois facilitées par les technologies comme le chiffrement asymétrique, et reposent, dans d'autres cas, sur la pratique des organisations et des individus. Ainsi, à la fin du XX^{e} siècle, alors que la « netiquette » prétendait transposer les standards de la cordialité sociale au monde numérique, ces dernières années ont plutôt mis en lumière les abus, la haine en ligne et le complotisme dans un mouvement de relativisation générale de la vérité par la magie de l'accès instantané, démontrant ainsi la fragilité des mécanismes de confiance dans le numérique.

C'est bien toute l'ambivalence des effets du numérique qui s'exprime à nouveau à travers ce sujet polysémique. Il semble aujourd'hui pertinent de revenir sur les dynamiques qui contribuent ou, au contraire, nuisent à l'émergence d'un numérique de confiance. Avant de plonger dans les dernières technologies ou les régulations qui cherchent à répondre aux défis actuels, il est utile de revenir sur les ressorts de la confiance en s'intéressant au regard que porte la psychologie sur ce sujet ou bien à l'importance de la procédure dans le système judiciaire. Ces points de vue illustrent notamment deux dimensions cardinales de toute relation de confiance : la stabilité et la transparence. En effet, la confiance dans le numérique repose, d'abord, sur une construction patiente, qui se renforce avec le temps et qu'aucune action sur le court terme, aussi décidée et légitime qu'elle soit, ne peut concurrencer. Elle dépend, ensuite, de la visibilité donnée sur le processus, l'algorithme ou l'entité qui prétend la gagner : que ce soit pour les SI (systèmes d'information) de l'État, les réseaux sociaux ou un algorithme de chiffrement, l'opacité n'a jamais pu constituer une approche durable.

Ce numéro de *Enjeux numériques* souhaite ainsi explorer les différentes approches proposées aujourd'hui pour renouer le lien de confiance entre usagers, entreprises et institutions en commençant par les approches technologiques, mises en regard des évolutions réglementaires et du rôle des institutions.

En effet, les avancées du numérique reposant majoritairement sur les possibilités apportées par la technologie, il est particulièrement séduisant d'essayer d'apporter une réponse technique à la question de la confiance. Cette réponse peut se fonder aussi bien sur l'évaluation technique au

travers de méthodes sophistiquées de certification que sur la tentative de l'intégration partielle ou totale de la dimension « confiance » dans la technologie : le développement des technologies de cryptographie homomorphe ou de l'IA de confiance montre que ces pistes sont prometteuses, mais pas encore suffisamment matures pour pouvoir générer de la confiance par leur seule utilisation. Les technologies *blockchain* constituent une autre tentative de générer de la confiance à partir de la seule technologie, en visant à remplacer le tiers de confiance par un protocole technique.

Cependant, comme illustré par l'adage commun en matière de cyberespace « la faille principale se trouve entre le clavier et l'écran », il est probablement illusoire de vouloir faire reposer la confiance à l'ère numérique sur la seule technologie. Élément indispensable, elle ne peut à elle seule capturer l'ensemble des facteurs humains, comme le montrent le succès régulier des attaques par *phishing* ou les détournements de Bitcoins qui ont lieu sans atteinte à la technologie employée mais en jouant sur des ressorts non numériques bien connus de crédulité ou d'appât du gain. Par ailleurs, la technologie qui tente d'intégrer la confiance possède également l'inconvénient d'être plus lourde, plus lente et plus complexe à mettre en œuvre. Dans un monde numérique dans lequel la simplicité pour l'utilisateur et la vitesse d'exécution priment sur les garanties, ces technologies sont *de facto* désavantagées. Qui lit les petites lignes de l'analyse de sécurité d'un produit cyber ? Ou s'intéresse aux détails d'implantation d'un protocole de chiffrement d'une messagerie qui vante de la sécurité de bout en bout ? Ce sont pourtant ces détails qui peuvent créer ou, au contraire, détruire la confiance, qui devient dès lors supposée par l'utilisateur et donc davantage une affaire de *marketing* et d'image qu'une réalité technique.

Les limites d'une approche purement technologique appellent par conséquent à des modes d'action complémentaires pour encadrer le développement de systèmes et de solutions informatiques rapidement perçus comme « complexes ». Dès les années 1970 et le grand débat national sur l'informatisation de la société, il a semblé pertinent de prévoir des garanties juridiques à l'utilisation de l'informatique. La loi Informatique et Libertés de 1978, mais également la loi CADA (qui a créé la Commission d'accès aux documents administratifs) la même année et la loi Archives l'année suivante, ont conclu ce travail de réflexion en posant des principes à respecter, dont les énoncés sont à la portée de tous : finalité du traitement des données, proportionnalité, sécurité, durée de conservation, transparence des décisions automatiques, notamment dans le secteur public. Ainsi, l'ensemble des idées qui restent pertinentes aujourd'hui avaient déjà été identifiées il y a plus de 40 ans.

Évidemment, l'arrivée d'Internet et l'utilisation du numérique dans tous les domaines de l'activité humaine ont accentué l'importance de ces mécanismes de confiance et ont conduit à un renouvellement des pratiques et des moyens : le RGPD (le règlement général sur la protection des données) a consacré le droit à la protection des données en renforçant les moyens de protection ; le mouvement de l'ouverture des données (*open data*) a étendu le principe de l'accès à toutes les données d'intérêt public et mené à de nouvelles approches fondées sur des communautés actives et organisées, avec l'ambition d'appliquer les principes de gouvernance des « communs » aux ressources numériques essentielles pour tous. Ces réflexions s'étendent aujourd'hui à la régulation des algorithmes, combinant preuves mathématiques, garanties procédurales et approches interdisciplinaires pour en capturer la complexité.

Plus récemment et à la faveur de la domination d'une « deuxième génération » de services en ligne fondés à la fois sur d'innombrables contributeurs et le rôle-clé d'un nombre limité de plateformes, la question de la confiance dans les informations diffusées en ligne se pose de manière aiguë. Si l'exemple de Wikipédia a montré la possibilité d'une gouvernance raisonnée de l'information (non exempte de critiques), le cocktail d'autorités publiques en mal de crédibilité, d'acteurs économiques mus par des intérêts économiques fondés sur la vente de publicité et de groupes d'intérêt organisés pour servir certains faits ou théories, est particulièrement dangereux et soulève

de nouvelles questions, techniques, institutionnelles et juridiques. Les développements récents en Europe et aux États-Unis apporteront peut-être des éléments de réponse sur les nouveaux équilibres à trouver sur ce sujet délicat.

Ce questionnement sur la gouvernance de l'information met en particulier en avant la question du rôle des acteurs publics dans la génération de la confiance numérique et celle de la forme de confiance numérique à laquelle ces acteurs peuvent prétendre. La transposition dans l'espace numérique d'un des principaux éléments de la confiance, l'identité des personnes physiques, est également une des problématiques sur lesquelles, dans le même temps, les acteurs publics ont une grande possibilité d'action et rencontrent en France des résistances élevées. Bien que nombre d'autres pays aient réussi le déploiement de solutions d'identité numérique, rares sont ceux pour lesquels cette identité a été déployée largement au-delà de la sphère publique. On assiste aujourd'hui à la gestion de l'identité en ligne autant, si ce n'est plus, par certains acteurs du numérique (Google ou Facebook) que par les États, soupçonnés par ce moyen de vouloir utiliser les possibilités du numérique pour exercer un contrôle étroit de la population. On retrouve cette dualité dans le cas de l'application StopCovid, entre un État qui cherche une souveraineté dans une application maîtrisée, mais qui a des difficultés à déployer un système technique et un accompagnement politique générateur de confiance tandis que Google et Apple déploient très rapidement un système techniquement très performant, mais dont le contrôle démocratique est totalement absent. Il est d'ailleurs intéressant de constater que les autres États européens ne portent pas le même regard que nous sur ces sujets.

S'ils ne peuvent ni créer techniquement les conditions de la confiance, ni réussir à la générer pour leurs propres applications, les pouvoirs publics ont cependant des champs d'action à investir. En rendant accessible le numérique à tous, par une politique ambitieuse d'inclusion numérique, en développant la régulation des espaces de dialogue en ligne, pour tenir un rôle de garant des équilibres entre la liberté d'expression et ses limites, rôle qui est aujourd'hui contesté par les grandes plateformes, les acteurs publics peuvent trouver une place et faire valoir la légitimité et la confiance que procure la démocratie.

Les ressorts de la confiance

Par **Bruno BAGARRY**
Psychologue, psychothérapeute et psychanalyste en libéral et en institution

Se nourrir, se soigner, apprendre des choses, se lier à l'autre ou travailler, quels que soient les domaines de la vie où il est question de subvenir à ses besoins, d'assouvir ses désirs ou d'accomplir un acte, parfois le plus banal, la notion de confiance s'impose. Dans les faits, mais aussi dans les discours, entre amis, dans le couple et jusqu'au cabinet du psychanalyste, la confiance s'interroge comme une clé du lien à l'autre. Qu'en serait-il si le doute s'installait au point de mettre en question le moindre savoir ou la plus banale interaction ?

Le Trésor de la langue française (TLFI) établit que la confiance est une « croyance spontanée ou acquise en la valeur morale, affective, professionnelle... d'une autre personne, qui fait que l'on est incapable d'imaginer de sa part tromperie, trahison ou incompétence ». « Foi en quelque chose, en quelqu'un » (TLFI) caractérise la confiance.

C'est un acte de foi fondé sur des valeurs. Mais est-ce un acte délibéré ? Autrement dit, la confiance est-elle un choix ? Certains auteurs parlent de confiance fondamentale, présente au tout début du développement. D'autres énoncent qu'elle est le résultat du milieu dans lequel le sujet évolue. D'un côté, elle serait une sorte d'état de nature, et de l'autre, selon le contexte de vie, elle s'établirait de façon erratique ou stable.

Si la confiance est au fondement du sujet, qu'advient-il lorsque la désillusion, inévitable et parfois cruelle, bouleverse les représentations ? Le corps social n'est-il pas le garant d'un équilibre des croyances sans lequel la construction du lien, indispensable à chacun et au vivre-ensemble, ne pourrait exister ?

Spontanée ou acquise, édifiée sur des valeurs, la confiance aurait pour origine une croyance que l'existence aurait mauvais jeu de défier. Mais des ressorts intersubjectifs et collectifs existent pour la préserver.

Aux prémices, la dépendance

État de nature ou historicité

Jean-Jacques Rousseau écrivait déjà que l'être humain a « la faculté de se perfectionner […] au lieu qu'un animal est, au bout de quelques mois, ce qu'il sera toute sa vie » (Rousseau, 1755). Et l'homme est si perfectible et non programmé qu'il peut se tuer. Tel est le revers de sa liberté, de son extraction d'un état de nature originel pour accéder à l'historicité. Mais si l'animal peut subvenir à ses premiers besoins dès les tout débuts de son développement, l'humain est pendant des années dépendant de son milieu pour les assouvir. Freud parlera d'« immaturité biologique » concernant le petit de l'homme et son incapacité à subvenir à ses besoins primaires. Aussi, l'infant – l'enfant qui ne parle pas encore – n'a pas d'autre issue que de s'en remettre totalement aux parents nourriciers. Son état de vulnérabilité est si grand que la confiance en ceux qui lui donnent les premiers soins est une nécessité.

La confiance de l'enfant en ses parents est, au départ, inconditionnelle. Il est alors un être totalement crédule, par nécessité. Mais aussi par nature. En effet, il y aurait chez l'être humain, selon Thomas Reid cité par Origgi, une « disposition naturelle, psychologique, à la crédulité » (Origgi, 2008).

Confiance et vulnérabilité

L'état de vulnérabilité de l'enfant fait écho à ce que les adultes traversent dans certaines circonstances de leur vie, même les plus banales. Par exemple, s'en remettre au médecin marque un acte d'abandon à une autorité savante. Cependant, à la différence de l'adulte, « la confiance affective chez l'enfant ne suppose pas qu'il ait préalablement pesé le pour et le contre ; elle est là d'emblée, dans une situation de vulnérabilité maximale » (Origgi, 2008).

Apprentissage

Si l'état de confiance est présent dès l'abord et est une réponse à la condition de vulnérabilité extrême du sujet, il est également à la source de tout l'apprentissage. L'enfant baigne dans le langage dès sa naissance, et c'est dans et par la parole de l'autre qu'il construit son univers mental et symbolique. Wittgenstein note que « l'enfant apprend en croyant l'adulte. Le doute vient après la croyance » (Wittgenstein, 1976).

L'apprentissage requiert un relâchement, un abandon, une « position féminine », diraient certains psychanalystes. Ainsi, apprendre est souvent difficile pour l'adulte. La position de recevoir nécessite de baisser la garde. Et chez certains jeunes hommes, notamment, en bataille avec leur identité masculine, elle est synonyme de féminité, d'un devenir-femme qui les effraie. La rébellion devient la réponse à une menace qu'une construction imaginaire aura instiguée.

Ainsi parle-t-on de confiance fondamentale pour les premiers soins et l'apprentissage. Elle est le résultat d'un état de nature, d'une crédulité originelle.

Mais la confiance est également le produit d'interactions réussies avec le parent nourricier.

Les premières interactions en question

Les premiers soins

L'infant est la proie d'une « angoisse dont nous ne pouvons avoir idée […] : se morceler ; ne pas cesser de tomber ; ne pas avoir de relation avec son corps ; ne pas avoir d'orientation » (Winnicott, 1962*).*

L'une des fonctions du parent est de s'ajuster au vécu chaotique du bébé et d'en favoriser la symbolisation. L'on pourrait parler d'interprétation. Il s'agit de se faire le passeur de ce qu'il ressent et exprime par des cris, des gestes ou des mimiques, faute de mots pour le dire. Se faire l'écho de l'éprouvé infantile conduit le jeune sujet à élaborer son propre langage et, peu à peu, à sortir de son chaos.

Winnicott parle de « la mère suffisamment bonne ». Celle-ci « s'identifie aux besoins de l'enfant, constitue l'étayage pédagogique du travail du moi » (Tyar, 1998). Chez la mère suffisamment bonne, l'on trouve une façon de contenir l'enfant – *holding* – et de lui apporter les premiers soins – *handling* –. Mais ceux-ci ne doivent pas être trop satisfaisants. En cela, ce qui est suffisamment bon ne l'est ni trop ni pas assez. La mauvaise mère est « celle qui satisfait trop bien les désirs de son enfant... celle qui ne prive pas l'enfant de la privation » (Tyar, 1998).

La frustration est un vecteur constitutif du développement et qui engage l'aptitude du sujet à envisager un espace possible entre soi et le monde, ouvrant à la création. Car ce que l'on perdra ou ne pourra pas obtenir sera recréé par le symbole qui substitue un récit à l'absence. Freud illustre cela par le *Fort-Da* (*fort* : parti ; *da* : là), ce mouvement d'aller-retour du jeu de la bobine de son petit-fils (Freud, 1913). L'enfant lance la bobine tenue par un fil, celle-ci disparaît sous son lit – "*Fort*", s'exclame-t-il –, puis réapparaît – "*Da*" –. Par ce mouvement, l'enfant métaphorise les allers-retours de sa mère. Ainsi n'est-il plus sous l'emprise de l'angoisse que générait son absence. Il devient le metteur en scène de la disparition. La confiance naît de cette capacité d'indépendance par la création de son propre monde de représentations.

Confiance en soi, confiance en l'autre

La confiance en soi résulterait ici de l'élaboration d'un récit, celui de l'absence. Une fois symbolisée, la disparition de l'être cher devient une séquence que le sujet a recréée et dont il s'est approprié l'incidence. Il prend ainsi confiance en son indépendance possible et en sa capacité d'élaboration. La confiance en l'autre et la confiance en soi naissent d'un même mouvement. Intériorisés, l'absence de l'autre, et l'autre lui-même, ne sont plus une menace. De plus, l'adulte contribue par ses insuffisances – ne pas pouvoir répondre à tous les besoins ; devoir s'absenter... – à la fabrication du monde intérieur de l'enfant. La défiance cède le pas à la confiance, tout à la fois en l'autre, qui peut s'absenter sans que cela ne provoque l'angoisse, et en soi, parce que le sujet réalise qu'il peut survivre à l'absence.

La désillusion

Selon Ferenczi, la déception de l'enfant a deux origines fondamentales : celle « concernant la capacité des personnes autorisées d'expliquer les choses et les processus, et la déception concernant leur disposition à dire la vérité » (Ferenczi, 1913). Et d'ajouter la « déception quant à la confiance […] accordée aux détenteurs de l'autorité ou plus exactement à la réalité de leur amour » (Ferenczi, 1913).

L'omnipotence des parents est démystifiée. L'enfant intègre, non sans mal, que ceux-ci ne peuvent pas répondre à tous ses désirs. Mais également, la toute-puissance infantile, l'éprouvé que tout besoin devrait trouver une réponse, se dissipe à l'orée « d'exigences qu'il ne peut plus satisfaire par la seule force de son désir mais seulement en modifiant le monde extérieur » (Ferenczi, 1913). Et ce dernier ne manque jamais de résister.

De même, l'illusion d'un amour pur et inconditionnel s'émousse. Elle fait place à la perception de l'ambivalence. Lacan lui donnera un nom : « hainamoration » (Lacan, 1975). Tout amour est teinté de haine et *vice versa*. Là où le chien lèche ou mord, l'homme vit dans la confusion des sentiments. Au point que certains humains optent pour la relation à l'animal afin de ne plus avoir affaire à l'incertitude. Jusqu'à préférer la haine de l'autre dont l'authenticité, le vrai, laisse moins de doute que le meilleur des amours.

Face à la désillusion, tant de la toute-puissance parentale que de celle de l'enfant vis-à-vis de lui-même, et fort du constat de l'ambivalence des sentiments, le sujet est en constante recherche de gages.

Les règles de l'échange, le jeu social ou les institutions luttent sans répit contre le doute, voire la défiance de tout un chacun. Ils établissent des modalités de la confiance afin que les engagements, et, par là même, le vivre-ensemble, restent possibles.

Les mécanismes sociaux de la confiance

La dépendance à l'autre est une conséquence d'un « des besoins fondamentaux de l'humanité, celui de coopérer » (Origgi, 2008).

Si elle est, en premier lieu, l'affaire cruciale des plus vulnérables, elle est présente « dans tout état de l'humanité, son état de nature primordial ainsi que son état social » (Origgi, 2008).

La dépendance affective, économique et sociale de l'homme l'inscrit dans une nécessité de la confiance malgré ses désillusions. Des mécanismes sont à l'œuvre pour favoriser l'adhésion.

La promesse et le renforcement

« L'engagement de la parole donnée est le fruit d'un contrat visant à nous protéger d'une défiance généralisée » (Hobbes, 1977).

Il est attendu que les liens de sang, de provenance ou de parenté soient, par leur nature même, des gages de confiance. La promesse s'établirait avant tout comme substitut du lien naturel. Elle favoriserait l'établissement possible de relations entre inconnus et entre sujets ayant des intérêts divergents.

Tenir ses promesses n'est pas affaire de sentiment, mais de conventions. Et celles-ci connaissent un renforcement dès lors qu'elles se sont avérées fructueuses. Reconnues comme bénéfiques de génération en génération, les conventions se sont confortées, sédimentées, et sont devenues des lois de l'échange.

Intérêts partagés et valeurs communes

Si les conventions régulent l'engagement d'une manière formelle, dénouée d'affect, il n'en demeure pas moins que la confiance s'établit aussi sur des critères intersubjectifs qui mettent en jeu l'intérêt et les valeurs partagés.

« Je fais confiance à quelqu'un si j'ai des raisons de croire qu'il sera dans son intérêt de prendre en compte mes intérêts » (Origgi, 2008).

L'altruisme est suspect dans le rapport social. Connaître l'intérêt de l'autre est, en un sens, rassurant. L'engagement viendra souvent de la révélation mutuelle des profits escomptés. Tant que l'autre n'aura pas abattu les cartes de ce qu'il attend, il demeurera douteux.

Et la considération des valeurs en jeu compte également. Selon Pettit, il est fait le « pari […] que l'autre se conformera aux mêmes valeurs que soi […]. Je fais confiance à un autre si je perçois chez lui des qualités auxquelles j'attache une grande valeur » (Origgi, 2008).

Le code moral peut être contraire à toute éthique publique – code d'honneur de truands par exemple –, il n'en est pas moins indéfectible. En effet, les valeurs personnelles sont ce à quoi le sujet renonce le moins.

Réputation

Un autre facteur de la confiance : le souci de réputation.

Lacan affirme qu'il y a derrière toute demande une infinité de demandes, et, au final, une demande d'amour (Lacan, 1959). Celle-ci se distingue du besoin qui est de nature biologique – la faim – et qui se satisfait d'un objet – la nourriture. À l'inverse, il n'y a aucun objet qui puisse satisfaire une demande, selon Lacan. La réponse donnée n'est jamais la bonne. Elle n'est jamais satisfaisante. Derrière une demande, il y a toujours une autre demande. Et, au final, une demande d'amour. La quête de réputation n'est autre que cela.

Adam Smith « place la réputation au centre de la vie sociale » (Origgi, 2008). « La nature, lorsqu'elle a formé l'homme pour la société, lui a fourni un désir original de plaire et une aversion originale d'offenser son frère » (Smith, 1759). Et Pettit de dire : « J'ai des raisons de faire confiance car je peux parier sur une disposition psychologique chez mes semblables à honorer la confiance afin de garder ou gagner une bonne réputation » (0riggi, 2008).

Inutile d'insister sur la recherche effrénée de réputation sur le net. Elle illustre ce qui s'est observé depuis toujours et à petite échelle dans les coteries. Aujourd'hui, elle se dévoile à tous sur les réseaux sociaux. La réputation donne un gage de crédibilité et augmente les chances de futures connections. Le gain d'une bonne image se traduit par un apport économique. Mais avant tout, les "*likes*" sont bien des mots d'amour.

Conclusion

Pour partie nécessaire et constitutive, la confiance est un trait inhérent au développement d'un sujet. Elle est de plus un garant de l'équilibre social. Mais elle ne survivra qu'au prix de conventions, d'intérêts et de valeurs partagés pour dépasser les désillusions intrinsèques au parcours de vie. L'on pourrait dire qu'elle est le produit d'une lutte sans répit entre les blessures de l'histoire individuelle et l'instauration requise des moyens de la conciliation.

Mais alors, qu'en est-il d'une société de la défiance ? N'observe-t-on pas, en effet, à la faveur de la pandémie actuelle par exemple, une progression manifeste de la suspicion générale ? Et n'a-t-on pas pour coutume de pointer, depuis Jules César, l'esprit querelleur des Français et leur méfiance envers ceux qui les gouvernent, à peine leurs fonctions prises ?

Certains couples tiennent par le soupçon. La menace devient source de vitalité. Elle donne une valeur à ce qui pourrait échapper. Et concernant la collectivité nationale, comme le rappelle Jacques Julliard [(1)], « la défiance à l'égard du pouvoir central est ce en quoi, pour beaucoup de Français, consiste la démocratie. Lorsque tout le monde est d'accord, tout le monde s'inquiète. » Rappelant Marat : « Tout dépositaire de l'autorité est un ennemi potentiel. »

Et si la discorde, tant dans la vie intime qu'au sein d'une collectivité, était un signe de vitalité et devenait elle aussi essentielle à la ferveur du lien…

Bibliographie

FERENCZI S. (1970), *Psychanalyse II*, Paris, Payot.

FREUD S. (1985), *Au-delà du principe de plaisir*, Paris, Payot.

HOBBES T. (1977), *Élément du droit naturel et politique*, Paris, L'Hermès.

LACAN J. (1975), *Le séminaire, Livre XX, Encore*, Paris, Seuil.

LACAN J. (1986), *L'Éthique de la psychanalyse*, *Le Séminaire, Livre VII*, Paris, Seuil.

ORIGGI G. (2008), *Qu'est-ce que la confiance ?*, Paris, Librairie Philosophique J. Vrin.

ROUSSEAU J.-J. (1755), *Discours sur l'origine et les fondements de l'inégalité parmi les hommes*, Amsterdam, Marc Michel Rey.

SMITH A. (1759), *La théorie des sentiments moraux*, Paris, PUF (2000).

Trésor de la langue française informatisé, http://www.atilf.fr/tlfi, ATILF - CNRS & Université de Lorraine.

TYAR A.-F. (1998), *Les aléas de la confiance : gouverner, éduquer, psychanalyser*, Paris, L'Harmattan.

WITGENSTEIN I. (1976), *De la certitude*, Paris, Gallimard.

WINNICOTT D. W. (1962), *Processus de maturation chez l'enfant : développement affectif et environnement*, Paris, Payot.

(1) Entretien sur France Culture (2020), « Penser ce qui nous arrive avec Jacques Julliard », émission *Répliques*, 30 mai, 52 min.

Numérique et confiance

Par **Henri ISAAC**
Université Paris-Dauphine, PSL

Introduction

L'univers numérique s'est développé à une vitesse et une intensité telles que le questionnement de la confiance en cet espace peut paraître incongru. Cependant, dès 2004, la France traduit la directive européenne « E-commerce » en droit français sous le nom « loi pour la confiance dans l'économie numérique » (LCEN), concrétisant l'existence d'enjeux spécifiques de confiance liés à l'espace numérique. Au-delà de la question des transactions marchandes, des enjeux de confiance émergent avec la multiplication des contenus générés par les utilisateurs et, avec ceux-ci, les contenus toxiques (*fake news*). Les comportements des utilisateurs peuvent également amoindrir la confiance en cet espace (fraude en ligne, usurpation d'identité, cyberharcèlement). Par ailleurs, la collecte massive de données personnelles opérée par de nombreux services numériques interpelle. Des risques de nature différente – cybercriminalité, surveillance étatique des communications – entravent également le développement de la confiance en ligne.

Dès lors, un tel espace interroge profondément la question de la confiance ainsi que les mécanismes qui la produisent et l'entretiennent. Univers de confiance pure, l'espace numérique a dû construire de nombreux mécanismes et dispositifs pour créer de la confiance et faciliter le développement des usages. Si ces mécanismes de confiance ont dans un premier temps imité les mécanismes classiques développés dans le monde physique, l'univers numérique a progressivement produit des mécanismes de génération et de gestion de la confiance propres, en s'appuyant sur la nature de ce qui le caractérise, l'organisation réticulaire et le traitement des données.

Dès lors, l'architecture classique du tiers de confiance, quelle qu'en soit sa modalité, pose elle-même question et débouche sur l'idée qu'une architecture de réseau, par conception, par elle-même, peut générer la confiance dans les échanges.

Les multiples défis de la confiance à l'ère numérique

La confiance des individus dans les artefacts technologiques est une problématique ancienne (Taddeo, 2009). Ainsi, la confiance que l'on peut accorder à un robot est une problématique largement étudiée (Coeckelbergh, 2010). Cependant, les enjeux de confiance à l'ère numérique ne se limitent pas à la confiance dans les machines, mais à la confiance envers des dispositifs mêlant des technologies et des comportements humains permis par des infrastructures technologiques distribuées à une échelle mondiale.

L'espace numérique est à la fois un espace informationnel et un espace marchand dans lequel des transactions ont lieu. Dans cet espace, des acteurs malveillants se livrent à de nombreuses attaques, actes de piraterie, et les États eux-mêmes déploient des stratégies de surveillance, qui ont fait l'objet d'un éclairage nouveau après les révélations d'Edward Snowden. Dès lors, la construction de la confiance dans un tel espace fait face à de nombreux défis.

Confiance dans les transactions

Le développement de la sphère marchande sur le *web* a entraîné un questionnement sur la sécurité des transactions dématérialisées. Si cette question a fait l'objet d'une importante réflexion dans

les réseaux professionnels, comme les réseaux utilisant l'EDI [1], force est de constater que la transformation du *web* en espace marchand a rapidement interrogé la confiance que les utilisateurs pouvaient avoir dans les sites et les transactions qui s'y déroulaient. L'impossibilité de déployer des architectures de certificats électroniques auprès du grand public a permis le développement d'une fraude significative dans les transactions en ligne, éloignant pendant de nombreuses années une part substantielle de clients potentiels. Si cette fraude n'a eu de cesse de diminuer depuis une décennie [2], et si 62 % des français effectuent des achats en ligne [3], la question de la sécurité demeure encore un frein au développement des transactions en ligne.

Confiance dans les contenus numériques et l'usage des données collectées

La multiplication des plateformes de médias sociaux a facilité le développement et la propagation de fausses informations. Ces plateformes ont également été utilisées dans de nombreuses campagnes de désinformation initiées par des États. Cette situation conduit les utilisateurs de par le monde à n'accorder qu'une faible confiance à ces espaces informationnels, comparativement à des médias traditionnels. L'étude du Reuters Institute de 2020 met en évidence que 56 % des personnes s'inquiètent de la véracité de l'information publiée sur les réseaux sociaux, cette proportion s'élevant à 84 % au Brésil et 67 % aux États-Unis. Dès lors, seuls 26 % des personnes font confiance aux réseaux sociaux pour s'informer contre 59 % aux médias traditionnels (Reuters Institute, 2020). Mais l'exposition de certains utilisateurs à des contenus dits toxiques (propos haineux, terrorisme, pédopornographie, prostitution) contribue également à amoindrir la confiance que les utilisateurs ont dans les services de réseaux sociaux.

Les services numériques reposent largement sur des traitements de données et particulièrement de données personnelles. Si celles-ci font l'objet d'un cadre juridique renforcé en Europe, force est de constater que certains services en ligne collectent massivement des données personnelles dont la finalité de traitement est opaque et très souvent inconnue des utilisateurs. Les cookies tiers collectés sur des sites éditoriaux à des fins publicitaires sont typiques de ce genre de collecte, qui instille un doute sur la finalité. Ainsi, le questionnement sur les finalités des collectes de données demeure une interrogation très présente pour 76 % des utilisateurs français en 2019 [4]. Cette collecte massive expose également les utilisateurs à un risque de fuite de leurs données par manque de protection et de sécurité du stockage de leurs données. Ces fuites de données sont une réalité qui concerne tout type d'acteurs [5], et elles ont tendance à se multiplier.

Surveillance, cybersécurité et confiance en ligne

La migration progressive et constante des interactions marchandes et non marchandes sur les plateformes numériques conduit plusieurs auteurs à considérer que ces plateformes exercent *de facto* une surveillance de nos comportements et de nos actions. Les plateformes auraient la capacité de manipuler les choix de contenus et par la même nos décisions et comportements individuels (Zuboff, 2019). Une telle vision de l'organisation de la société numérique inspire une partie de la population à se détourner de ces espaces par manque de confiance, de peur d'être traquée par

(1) EDI : Échange de données informatisées ou *Electronic Data Interchange*, échange d'informations structurées par des messages automatiques entre deux entités, de machine à machine. Voir https://fr.wikipedia.org/wiki/Échange_de_données_informatisé

(2) Le taux de fraude pour les paiements en ligne avec une carte bancaire française s'élève à 0,167 % en 2019. Observatoire de la sécurité des paiements (2020), rapport annuel, 82 p., septembre.

(3) Baromètre du Numérique 2019, « Enquête sur la diffusion des technologies de l'information et de la communication dans la société française en 2019 », Credoc, CGE, Arcep, 250 p.

(4) Sondage Odoxa (2019), « Données personnelles. La "*privacy*" comme nouveau cheval de bataille de Google et Facebook », mai.

(5) Voir par exemple : RAHAL A. (2019), "Five data breaches to understand the importance of data security", *Cisomag,* https://cisomag.eccouncil.org/5-data-breaches-to-understand-the-importance-of-data-security/

les dispositifs technologiques de ces plateformes, comme les caméras de leur ordinateur, leur *smartphone* ou encore les enceintes connectées [6].

Cependant la surveillance de l'espace numérique ne se limite pas à l'analyse des comportements d'intention d'achat ou de consommation. Elle est également le fait des États et de leurs services de renseignement. Les révélations de Snowden ont permis de mesurer l'ampleur de cette surveillance étatique des communications électroniques [7]. Ces révélations ont jeté une suspicion généralisée sur l'espace numérique, affaiblissant d'autant la confiance que les utilisateurs pouvaient avoir en cet espace.

Dans ce monde « post-Snowden », l'espace numérique est également devenu un espace d'affrontements géopolitiques qui se caractérise par une escalade et une sophistication croissante des attaques qui visent aussi bien des acteurs économiques pour leur extorquer des fonds que des acteurs publics, comme des hôpitaux, mais aussi des systèmes électoraux. Ces attaques, dans un monde qui a basculé dans le tout-numérique à l'occasion de la pandémie, éprouvent les systèmes de sécurité et leur résilience. Elles questionnent la robustesse de ces systèmes et la confiance que l'on peut y placer.

Construire la confiance en ligne : des tiers de confiance à l'architecture du réseau comme infrastructure de confiance

Pour construire la confiance dans les services numériques, plusieurs dispositifs s'articulent, reprenant des mécanismes classiques de gestion de la confiance. La logique du tiers de confiance a ainsi été rapidement introduite, même si elle a évolué à mesure du développement du *web*, pour intégrer les logiques propres aux échanges virtuels. Plus encore, l'émergence du protocole *blockchain* pousse la logique réticulaire plus loin puisqu'elle définit le réseau lui-même comme tiers de confiance.

S'appuyer sur les logiques classiques de la confiance

Dans le monde des échanges physiques, la confiance s'appuie sur plusieurs dispositifs institutionnels comme les labels, les marques et la réputation. Ces dispositifs ont tous été repris dans l'espace numérique. Le commerce en ligne a dû développer de nombreux mécanismes, dont les labels, afin de rassurer les internautes qui ont été longtemps rétifs aux achats en ligne (Ratnasingham, 1998). De multiples labels ont ainsi été mis en place (Trusted e-shop, charte qualité Fevad, etc.) et ont été complétés par des labels spécifiques pour le paiement (VeriSign Trusted). À ce dispositif est venu s'ajouter la marque comme indicateur de confiance. Si celle-ci joue indéniablement comme un facteur de confiance pour déclencher une commande sur un site de vente en ligne, elle ne peut à elle seule suffire à garantir la confiance, la qualité de l'exécution et la logistique jouant un rôle crucial dans la confiance accordée à un site marchand, ce que certains acteurs ont su parfaitement anticiper pour en faire un puissant moteur de confiance. Cependant de tels mécanismes ne suffisent à eux seuls à garantir la confiance dans les transactions en ligne.

Adapter le tiers de confiance à l'ère numérique

Afin de garantir l'identité des parties et l'intégrité des transactions, et en l'absence d'une identité numérique substantielle, l'introduction d'un tiers de confiance est un mécanisme institutionnel classique qui a été répliqué dans l'espace numérique, sous forme de certificats électroniques

(6) CLAUSER G. (2019), "Amazon's Alexa never stops listening to you. Should you worry?", *New York Times*, 8 août, https://www.nytimes.com/wirecutter/blog/amazons-alexa-never-stops-listening-to-you/
(7) SNOWDEN E. (2019), *Mémoires vives*, Le Seuil, 384 p.

délivrés par une instance aux parties dans une transaction. Si cette logique a pu être déployée dans les transactions B2B (*business to business*), elle a échoué à se développer dans les transactions B2C (*business to customer*) ou C2C (*customer to customer*), du fait de sa complexité technique pour les utilisateurs non professionnels.

Dès lors, plusieurs formes de tiers de confiance ont émergé pour fournir aux utilisateurs un cadre à leurs échanges. Un premier mécanisme est celui de l'évaluation par les pairs d'un produit, d'un service. Les évaluations de la foule et les avis clients, organisés, structurés et mis en valeur, constituent un puissant mécanisme de confiance. Les avis clients deviennent donc en tant que tels un dispositif de la confiance en ligne (Utz & alii, 2012). Cependant, ce mécanisme est lui-même susceptible d'être détourné par des acteurs malintentionnés. Le régulateur a donc introduit des contraintes spécifiques aux acteurs recourant aux avis clients [8]. Des modèles d'affaires se sont bâtis sur les avis clients comme Tripadvisor dans le voyage ou La Fourchette pour les restaurants.

De façon plus générale, les services de l'économie dite collaborative, pour lesquels il faut, par exemple, faire confiance à un chauffeur inconnu pour le covoiturage (Mazzela & alii, 2016), ou encore faire confiance à un inconnu locataire de sa maison (Hawlitschek, 2016). Dès lors, le rôle de la plateforme intermédiaire consiste à être le tiers de confiance, comme dans le modèle des places de marché. La plateforme fournit une infrastructure aux échanges. Elle sélectionne par des mécanismes de référencement les différents acteurs qui vont interagir, vérifie les identités, organise les avis clients et, de la sorte, construit un cadre de confiance plus ou moins élaboré, selon les plateformes (Isaac, 2021). Toutefois, un tel mécanisme centralisé, pour efficace qu'il soit, n'en connaît pas moins plusieurs limites. Il est toujours possible de biaiser les avis clients, d'en publier de faux. Aussi nombreux que puissent être les contrôles, la fraude sera toujours présente sur les plateformes.

Aussi, c'est par un dépassement de l'infrastructure de confiance centralisée, représentée par les plateformes, que d'autres alternatives de gestion de la confiance émergent.

La *blockchain*, ou le réseau comme mécanisme de confiance

Avec la technologie *blockchain*, le tiers de confiance devient le système lui-même (Werbach, 2016) : chaque élément réparti de la *blockchain* contient les éléments nécessaires à garantir l'intégrité des données échangées par un algorithme cryptographique. La chaîne de blocs est une base de données distribuée qui stocke et transmet des informations, envoyées par les utilisateurs. Les liens internes à la base sont vérifiés et groupés à intervalles de temps réguliers en blocs, formant ainsi une chaîne. Une chaîne de blocs gère donc une liste d'enregistrements protégés contre la falsification ou la modification par les nœuds de stockage. À ce titre, c'est un registre distribué et sécurisé de toutes les transactions effectuées depuis le démarrage du système réparti. Ainsi, une telle architecture devient le tiers de confiance, réduisant d'autant les coûts de transaction liés à son existence. Contrairement aux contrats, les chaînes de blocs ne s'appuient pas sur un système juridique pour faire respecter les accords. Contrairement à l'utilisation de normes relationnelles, les chaînes de blocs ne nécessitent pas de confiance ou de relations directes entre les différents acteurs de la chaîne (Lumineau & alii, 2020).

Une telle architecture résout en partie les enjeux de confiance liés aux transactions numériques : elle offre aux transactions une infrastructure d'échange robuste. Elle apporte une traçabilité complète des échanges et une transparence pour les acteurs. Une telle architecture est donc souvent envisagée comme une solution aux nombreuses limites auxquelles la confiance se heurte dans l'espace numérique.

(8) https://www.economie.gouv.fr/dgccrf/Publications/Vie-pratique/Fiches-pratiques/faux-avis-consommateurs-sur-internet

Si l'on perçoit bien l'intérêt pour les transactions marchandes, en revanche, une telle infrastructure ne renforcera en rien la confiance pour les autres contenus numériques, notamment les fausses informations. En effet, une telle infrastructure ne peut infirmer ou confirmer la véracité d'une information. Par ailleurs, elle ne supprime pas les questionnements autour de la surveillance des activités en ligne par les États.

L'espace numérique reste donc un espace où la construction de la confiance est un perpétuel défi, et où la technologie par elle-même semble rarement apporter les éléments suffisants pour bâtir un cadre de confiance robuste.

Références

COECKELBERGH M. (2010), "Humans, animals, and robots: A phenomenological approach to human-robot relations", *International Journal of Social Robotics*, 3(2), pp. 197-204.

HAWLITSCHEK F., TEUBNER T. & WEINHARDT C. (2016), "Trust in the sharing economy", *Die Unternehmung – Swiss Journal of Business Research and Practice*, 70(1), pp. 26-44.

ISAAC H. (2021), *Les business models de plateforme*, Vuibert, Paris, 272 p.

MAZZELLA F., SUNDARARAJAN A., D'ESPOUS V. & MÖHLMANN M. (2016), "How digital trust powers the sharing economy", *IESE Insight*, third quarter (30), pp. 24-30.

MÖHLMANN M. (2016), "Sharing economy: Building trust in P2P online marketplaces", *New York Computer Science and Economics Day*, New York.

LUMINEAU F., WANG W. & SCHILKE O. (2020), "Blockchain governance – A new way of organizing collaborations?", *Organization Science*, https://doi.org/10.1287/orsc.2020.1379

TADDEO M. (2009), "Defining trust and e-trust: Old theories and new problems", *International Journal of Technology and Human Interaction*, 5(2), pp. 23-35.

TADELIS S. (2016), "The economics of reputation and feedback systems in e-commerce marketplaces", http://faculty.haas.berkeley.edu/stadelis/Annual_Review_Tadelis.pdf

UTZ S., KERKHOF P. & VAN DEN BOS J. (2012), "Consumers rule: How consumer reviews influence perceived trustworthiness of online stores", *Electronic Commerce Research and Applications*, Vol. 11, pp. 49-58.

RATNASINGHAM P. (1998), "The importance of trust in electronic commerce", *Internet Research*, 8(4), pp. 313-321.

WERBACH K. D. (2016), "Trustless trust", SSRN: https://ssrn.com/abstract=2844409

ZUBOFF S. (2019), *The age of surveillance capitalism: The fight for a human future at the new frontier of power*, PublicAffairs, 704 p.

La procédure et la confiance des citoyens en la justice à l'épreuve de la dématérialisation

Par **Alain LACABARATS**
Président de chambre honoraire à la Cour de cassation

« Il faut non seulement que justice soit faite, mais aussi qu'elle le soit au vu et au su de tous. Il y va de la confiance que les tribunaux d'une société démocratique se doivent d'inspirer aux justiciables. »

Ce principe est repris de manière constante par la Cour européenne des droits de l'homme dans ses différentes décisions (par exemple : Morice c. France, 23 avril 2015, requête n°29369/10, paragraphe 78). Pourtant, il n'apparaît nullement en tant que tel dans la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (la Convention européenne des droits de l'homme). Comment peut-on alors expliquer la place éminente qu'il tient dans la jurisprudence de la Cour européenne ?

En réalité, ce principe constitue la pierre angulaire de la jurisprudence européenne sur la prééminence du droit (voir ANDRIANTSIMBAZOVINA J. (2018), « La "confiance du public" dans la jurisprudence de la Cour européenne des droits de l'homme », *in* Mélanges en l'honneur de Frédéric Sudre, *Les droits de l'homme à la croisée des droits*, Lexisnexis, pp. 11-19).

La prééminence du droit implique notamment que la justice soit rendue par des juges indépendants et impartiaux.

Comme l'expose la Recommandation [2010]12 du 17 novembre 2010 du comité des ministres du Conseil de l'Europe aux États membres, l'indépendance n'est pas conçue comme un privilège accordé aux juges. Elle ne doit exister que dans le seul intérêt des justiciables, pour garantir le « respect des droits de l'homme et des libertés fondamentales qui permet à toute personne d'avoir confiance dans le système judiciaire ».

La jurisprudence de la Cour européenne des droits de l'homme montre néanmoins que le droit au procès équitable ne se réduit pas à l'existence d'un statut garantissant l'indépendance des juges. Les justiciables ne peuvent avoir confiance en la justice que si celle-ci leur assure l'effectivité et l'efficacité des procédures juridictionnelles. Le droit au procès équitable n'existe pas notamment si l'accès à la justice est entravé de différentes manières ou si les décisions ne sont pas rendues dans un délai raisonnable, compatible avec les attentes des justiciables.

Mais il faut aller plus loin et porter une attention particulière à la qualité des procédures elles-mêmes, telles qu'elle sont mises en œuvre par les tribunaux (1), en s'interrogeant sur le point de savoir si la dématérialisation peut en affecter les caractéristiques (2).

1. La qualité des procédures judiciaires

Indépendamment de l'accès à l'institution judiciaire, qui doit être ouvert également à tous les citoyens, la confiance de ceux-ci dans le bon fonctionnement des tribunaux ne peut exister sans des procédures respectant certains principes précis caractéristiques du procès équitable, tel que l'envisage le droit européen.

Au nombre de ces principes, qui concernent aussi bien les procédures civiles que les instances pénales, figurent ceux de l'égalité des armes et de la contradiction.

En ce qui concerne le premier, la Cour européenne des droits de l'homme énonce que « l'exigence de l'égalité des armes implique l'obligation d'offrir à chaque partie une possibilité raisonnable de présenter sa cause dans des conditions qui ne la placent pas dans une situation de net désavantage par rapport à la partie adverse » (voir, parmi de nombreuses décisions : CEDH, Hôpital local Saint-Pierre d'Oléron et autres c. France, 8 février 2019, requête n°18096/12).

Mais la Cour retient toujours dans ses décisions que doit être corrélativement assuré le respect, entre les parties, du principe de la contradiction (le contradictoire), lequel suppose pour une partie « la faculté de prendre connaissance des observations ou pièces produites par l'autre, ainsi que d'en discuter » (Ruiz Mateos c. Espagne, 23 juin 1993, requête n°12952/87, paragraphe 63).

Autrement dit, en ce qui concerne les procédures juridictionnelles, c'est par la conjonction de ces deux principes que le droit au procès équitable peut devenir une réalité pour les justiciables. La Cour européenne des droits de l'homme ne dit pas autre chose lorsqu'elle énonce que « le principe de l'égalité des armes représente un élément de la notion plus large de procès équitable, qui englobe aussi le droit fondamental au caractère contradictoire de l'instance » (voir décision précédente).

L'égalité des armes et le caractère contradictoire de la procédure se traduisent par des règles différentes, selon la matière civile ou pénale du litige, mais avec le même but de concrétisation du droit au procès équitable.

- Dans la procédure civile française, la réalisation de cet objectif passe par une application stricte des dispositions des articles 14 à 16 du code de procédure civile, desquels il résulte :

- que nulle partie ne peut être jugée sans avoir été entendue ou appelée ;
- que les parties doivent se faire connaître mutuellement en temps utile les moyens de fait sur lesquels elles fondent leurs prétentions, les éléments de preuve qu'elles produisent et les moyens de droit qu'elles invoquent ;
- que le juge doit, en toutes circonstances, faire observer et observer lui-même le principe de la contradiction.

Ces dispositions générales n'excluent pas que des aménagements, justifiés par un intérêt légitime spécifique, soient apportés à leur mise en œuvre. Par exemple, par dérogation à l'obligation d'appeler à la procédure la partie adverse, le code de procédure civile admet que certaines mesures puissent être prononcées par un juge à la demande d'une partie et de manière non contradictoire (articles 493 et suivants, sur la procédure de l'ordonnance sur requête). Mais, outre le caractère provisoire des décisions relevant de cette procédure, les textes prévoient que la partie intéressée peut saisir le juge en rétractation de sa première décision, réintroduisant ainsi le contradictoire dans le déroulement de la procédure.

Un autre exemple peut être tiré du pouvoir donné au juge de relever d'office les moyens de droit qui lui paraissent appropriés : c'est en principe aux parties de préciser les règles de droit susceptibles de justifier leurs prétentions, mais le juge a toujours la possibilité de mettre dans le débat un moyen non invoqué par les parties, et il peut le faire dans toutes les situations procédurales :

- Il le fait, par exemple, dans les procédures civiles sans représentation obligatoire, lorsque l'une des parties se présente en justice sans avocat alors que l'autre partie est représentée ou assistée par un conseil. Le relevé d'office des moyens de droit est alors une façon de rétablir l'équilibre entre les parties, au profit de celle qui ne bénéficie pas des conseils d'un professionnel du droit.
- Il le fait aussi dans toutes les autres procédures, même si les demandes des parties sont

présentées par des avocats, à chaque fois qu'il estime que le débat juridique doit être orienté dans un sens différent de celui invoqué par ces parties.

Il convient néanmoins de souligner que, quel que soit le cas de figure, le juge doit se borner à introduire dans le débat la règle de droit qu'il estime appropriée, sans manifester d'une manière quelconque un parti pris quant à la solution du litige et en laissant aux parties un temps raisonnable de réflexion pour se déterminer sur la question nouvelle ainsi soulevée.

- Le droit au procès équitable est également au cœur des évolutions qu'a connues la procédure pénale française.

Certes, la Cour européenne des droits de l'homme admet que « les impératifs inhérents à la notion de procès équitable ne sont pas nécessairement les mêmes dans les litiges relatifs à des droits et obligations de caractère civil que dans les affaires concernant des accusations en matière pénale » (Dombo Beheer BV c. Pays-Bas, 27 octobre 1993, requête n°14448/88, paragraphe 32), mais la Cour souligne aussi (même décision, paragraphe 33) que certains principes, liés au procès équitable, tels que l'égalité des armes, au sens d'un juste équilibre entre les parties, valent aussi bien au civil qu'au pénal.

Traditionnellement marquée par le caractère inquisitoire et le secret des investigations, la procédure pénale française s'est dégagée progressivement des atteintes les plus manifestes au principe de l'égalité des armes et comporte, depuis une loi du 15 juin 2000, un article préliminaire fondamental.

Après avoir posé en principe que « la procédure pénale doit être équitable et contradictoire et préserver l'équilibre des droits des parties », le texte en décline les conséquences pour les autorités judiciaires et les justiciables, parmi lesquelles :

- La séparation des autorités chargées de l'action publique et des autorités de jugement, principe qui concourt à la sauvegarde de la liberté individuelle (Conseil constitutionnel, 2 février 1995, n°95-360) ;
- L'égalité de tous devant la loi pénale, qui suppose l'absence de discrimination injustifiée entre les justiciables au regard de l'application de la loi (Conseil constitutionnel, 3 septembre 1986, n°86-21) ;
- Le droit au respect de la présomption d'innocence, qui implique notamment que la charge de la preuve de la culpabilité incombe en principe à la partie poursuivante (Cour de cassation, Ch. Crim., 22 avril 1993, n°92-81811) ;
- Le principe du respect des droits de la défense, qui constitue un des principes fondamentaux reconnus par les lois de la République (Conseil constitutionnel, 2 février 1995, précité) et qui implique, notamment, non seulement que la personne poursuivie puisse bénéficier de l'assistance d'un avocat, mais aussi qu'elle soit informée d'une manière détaillée de la nature et de la cause de la prévention dont elle est l'objet, qu'elle puisse se défendre tant sur les divers chefs de poursuite qui lui sont imputés que sur chacune des circonstances aggravantes susceptibles d'être retenues à sa charge (Cour de cassation, Ch. crim., 20 septembre 2000, n°99-82846) ;
- Le juge a en toute hypothèse l'obligation, lorsqu'il envisage de relever d'office un moyen de droit, d'inviter, avant de statuer, les parties à présenter leurs observations (Cour de cassation, Ch. crim., 4 novembre 2008, n°08-80495) ;
- Du droit au procès équitable et du droit de tout accusé à l'assistance d'un défenseur découle également en matière pénale le fait que la juridiction de jugement ne peut juger un prévenu non comparant à l'audience et non excusé sans entendre l'avocat présent à l'audience pour assurer sa défense (Cour de cassation, Ass. plen., 2 mars 2001, n°00-81388).

Au-delà des différences importantes qui subsistent entre les procédures civiles et pénales, la référence commune au droit au procès équitable, à l'égalité des armes et au respect du contradictoire montre le souci d'assurer aux justiciables, par le respect d'un certain nombre de règles essentielles, la qualité de ces procédures. La question qui se pose est de savoir si la dématérialisation des procédures peut avoir des incidences sur ces orientations.

2. La qualité des procédures judiciaires dématérialisées

La dématérialisation ne devrait être qu'un moyen de facilitation de l'accès à la justice et d'amélioration du fonctionnement des tribunaux. Pourtant, les réformes de procédure intervenues en France depuis quelques années montrent que cette dématérialisation n'est pas dépourvue d'incidence sur les dispositions légales ou réglementaires applicables au déroulement des procès.

La justice française est résolument engagée dans la voie de l'informatisation de ses modes d'intervention. Outre les applications numériques destinées à simplifier la gestion des affaires pénales et civiles, de leur enregistrement jusqu'au jugement, les règles de procédure elles-mêmes sont affectées par l'informatisation.

À titre d'exemple, à la Cour de cassation, la quasi-totalité des instances civiles est dématérialisée, du pourvoi lui-même formé et transmis numériquement à la Cour, par l'avocat du demandeur, jusqu'au prononcé des arrêts, en passant par la communication électronique des mémoires des parties et de leurs pièces. Les justiciables peuvent en outre, par un internet sécurisé, avoir accès aux principales informations concernant leur affaire et suivre « en ligne » le déroulement de la procédure.

Pour les procédures civiles ordinaires avec représentation obligatoire par avocat devant le tribunal judiciaire et la cour d'appel, les actes de procédure, notamment l'assignation et les conclusions des parties, doivent également être transmis à la juridiction électroniquement (article 850 du code de procédure civile pour le tribunal judiciaire ; article 930-1 du même code pour la cour d'appel). Le code de procédure civile prévoit aussi, en son article 456, la possibilité d'établir les jugements sur support électronique.

Quant au code de procédure pénale, sans aller aussi loin dans la dématérialisation des procédures, il prend néanmoins bien en considération l'évolution des techniques, notamment en admettant très largement le recours, pour de nombreux actes de procédure, et même dans certains cas pour la comparution du prévenu devant un tribunal correctionnel, aux échanges à distance et à la vidéoconférence (article 706-71 du code de procédure pénale).

Ce dernier point conduit à s'interroger sur la place de l'audience dans la procédure. La publicité est un élément essentiel du droit au procès équitable (FRICERO N. (2017-2018), *Droit et pratique de la procédure civile*, Dalloz Action, n°212-71). Le Conseil constitutionnel l'a rappelé, dans une décision du 19 novembre 2020 (décision n°2020-866 QPC), en énonçant que l'audience est « une garantie légale des exigences constitutionnelles des droits de la défense et du droit à un procès équitable ».

L'audience est un temps important du procès, à double titre :

- L'audience est d'abord le moment où les parties se retrouvent face à leurs juges, et le lieu des échanges contradictoires sur les faits, les éléments de preuve et les moyens de droit. Particulièrement importante en matière pénale, pour les affaires criminelles, en principe aussi pour les affaires délictuelles, et ces procédures étant orales, l'audience ne peut être négligée en matière civile, même pour la procédure écrite de droit commun avec représentation obligatoire par un conseil, dès lors qu'elle peut être l'occasion d'un dialogue de nature à enrichir les données du débat judiciaire.

- Par l'audience la justice « se donne à voir » et contribue, grâce à la transparence des échanges dont elle est l'occasion, à convaincre le public qu'elle a pour seul objectif le respect des attentes des parties et l'application des règles de droit (voir FRICERO N., ouvrage précité, n°212-71).

Malgré les critiques dont elle fait souvent l'objet, la vidéoconférence n'annihile pas le principe même de l'audience, qui, même tenue sous cette forme, conserve ses principales caractéristiques. Le Conseil consultatif de juges européens, organe consultatif du Conseil de l'Europe pour les questions de justice, a néanmoins observé, dans son avis n°(2011)14 sur la justice et les technologies de l'information, que la vidéoconférence peut avoir pour inconvénient « une perception moins directe ou précise par le juge des propos et réactions des parties, des témoins ou des experts ». Le Conseil d'État, dans une décision du 27 novembre 2020 (req. n°446712), a aussi souligné que le recours à la vidéoconférence ne pouvait pas être systématique, et a exclu son application devant la Cour d'assises, l'oralité de la procédure étant un principe essentiel d'examen des procédures criminelles.

Au-delà de cette problématique, on observe depuis quelques années une tendance à réduire la place de l'audience dans les procédures.

C'est le cas dans le domaine pénal, avec notamment la multiplicité des hypothèses où, en matière de délits, le procureur de la République peut mettre en œuvre une procédure simplifiée d'ordonnance pénale. Celle-ci permet au président du tribunal de sanctionner par une peine d'amende et certaines peines complémentaires, sans débat préalable, la commission d'un certain nombre de délits (articles 398-1, 495 et suivants du code de procédure pénale). Certes, cette évolution n'est pas liée à la dématérialisation des procédures, mais il est évident que celle-ci est de nature à favoriser les modalités pratiques de recours à l'ordonnance pénale.

Le domaine civil n'échappe pas à cette évolution puisque a été introduite en procédure civile une possibilité de procès sans audience (article L212-5-1 du code de l'organisation judiciaire, modifié par l'ordonnance n°2019-964 du 18 septembre 2019 et complété par les dispositions du code de procédure civile issues du décret n°2020-1452 du 27 novembre 2020), avec dépôt par les parties de leurs dossiers au greffe de la juridiction. Conçu comme un mécanisme simplificateur destiné à améliorer l'efficacité de l'instance, le procès civil sans audience devrait produire son plein effet lorsque sera applicable l'article L212-5-2 du code de l'organisation judiciaire (non encore applicable en 2020) qui prévoit que certaines demandes en justice pourront être traitées sans audience dans le cadre d'une procédure dématérialisée.

Même si, pour les procédures pénales et civiles précédemment évoquées, des précautions sont prises pour préserver les droits des parties et restaurer, s'il y a lieu, la place de l'audience, le déclin de l'oralité est manifeste et se trouve amplifié par les facilités de traitement liées à l'informatisation.

L'informatisation permet même de s'interroger sur la place du juge dans le règlement des litiges. L'orientation ultime n'est-elle pas celle d'une justice numérique sans juge ? D'une justice soumise aux seuls algorithmes ? C'est la crainte qu'a pu inspirer le décret n°2020-356 du 27 mars 2020. Ce texte prévoit que des données à caractère personnel seront analysées pour développer un algorithme tendant notamment :

- à l'élaboration d'un référentiel indicatif d'indemnisation des préjudices corporels ;
- à l'information des parties et l'aide à l'évaluation du montant de l'indemnisation à laquelle les victimes peuvent prétendre afin de favoriser un règlement amiable des litiges ;
- à l'information ou la documentation des juges appelés à statuer sur des demandes d'indemnisation des préjudices corporels.

À ces fins, l'algorithme recensera les montants demandés et offerts par les parties, les évaluations proposées dans le cadre de procédures de règlement amiable des litiges et les montants alloués aux victimes pour chaque type de préjudice.

En soi, l'objectif d'assurer l'égalité des justiciables devant la loi et la justice est tout à fait légitime : est-il admissible que les victimes de dommages similaires soient indemnisées dans des conditions substantiellement différentes selon la juridiction saisie ?

Même si les règles générales d'élaboration de l'algorithme sont définies par le texte, il conviendra de prêter une attention particulière aux conditions dans lesquelles les données seront recueillies et exploitées, et veiller à laisser aux juges un pouvoir entier d'appréciation. La crainte d'une déshumanisation de la justice est tout aussi compréhensible, et cette déshumanisation serait une réalité si le juge était tenu de se conformer à un barème d'indemnisation, ou si le système aboutissait à des mécanismes d'indemnisation automatique sans possibilité de saisine d'une juridiction.

Conclusion

Dans son avis précité, le Conseil consultatif de juges européens a indiqué que les technologies de l'information « ne doivent jamais porter atteinte aux garanties et aux droits procéduraux tels que ceux assurant un procès équitable devant un juge ».

Il convient à cet égard de souligner que, quels que soient ses risques, la dématérialisation peut aussi être une chance pour les justiciables, spécialement dans le traitement des affaires civiles.

Réparties entre des juridictions civiles, commerciales et sociales, les affaires civiles sont trop souvent l'occasion de contentieux préliminaires portant sur des questions de compétence d'attribution ou de compétence territoriale. Des voies de recours pouvant en outre être formées contre les jugements en matière de compétence, il s'écoule parfois plusieurs années avant que les justiciables sachent réellement quelle est la juridiction compétente pour statuer sur leurs demandes.

Une réforme fondamentale, mais nécessaire et facilitée par la dématérialisation des procédures, consisterait à faire en sorte que le justiciable ait seulement à saisir informatiquement le service de la justice, à charge pour celui-ci de déterminer, par des mesures d'administration judiciaire non susceptibles de recours, la formation, civile, commerciale ou sociale, appelée à statuer sur le fond du litige.

C'est à l'évidence une mesure de simplification propre à améliorer l'efficacité du système judiciaire. Mais, comme l'a également relevé le Conseil consultatif de juges européens dans son avis sur les technologies de l'information, celles-ci requièrent des investissements très importants ainsi que l'allocation aux systèmes judiciaires de moyens financiers adaptés aux besoins des juridictions et des justiciables.

En outre, l'égalité de ces derniers devant l'informatisation doit être préservée, ce qui est loin d'être le cas actuellement compte tenu du pourcentage encore trop important de la population qui n'y a pas accès. Ce n'est que si la justice peut être vraiment accessible à tous et garantit à chacun le respect de ses droits fondamentaux que la confiance du public dans son fonctionnement peut être assurée.

L'engagement dans une pratique collaborative : une question de « confiance » ?

Par **Josette DEBROUX**
Maîtresse de conférences en sociologie à l'Université Lyon 2

Introduction

Omniprésente dans les discours médiatique, politique et économique, la confiance comme « socle à toute vie en société, à toute initiative citoyenne, politique, économique » (Delaye *et al.*, 2016) serait « en crise » : aucun domaine de la vie sociale n'échapperait à l'érosion de la confiance. Les citoyens ont perdu confiance dans les institutions, la défiance se serait généralisée à l'égard des médias, la « confiance des ménages », moteur de l'économie, est au plus bas… Cet « effondrement de la confiance » n'empêche pas le développement d'une « économie collaborative », qui regroupe des activités très diverses relevant aussi bien du secteur associatif et solidaire que du secteur marchand où de parfaits inconnus échangent des biens et des services par l'intermédiaire de plateformes électroniques. Pour accroître leur activité, les plateformes du secteur marchand les plus emblématiques de cette économie collaborative, se développant selon « des dynamiques hyper capitalistes » (Dagnaud, 2015), cherchent à susciter la confiance en permettant aux parties de vérifier les identités et en construisant des indices de réputation.

La confiance constitue le « concept central » du paradigme de l'échange, mobilisé dans de nombreux travaux s'intéressant au développement de « l'économie collaborative ». Elle apparait comme une propriété des individus (des individus qui feraient « par nature » plutôt « confiance ») ou comme le produit d'un raisonnement rationnel, ou encore comme le résultat du travail des plateformes qui, par leur appareillage, susciteraient la « confiance » (Hadrhri *et al.*, 2017).

C'est un autre modèle que nous avons mobilisé pour comprendre l'engagement dans une pratique emblématique de l'économie collaborative, le covoiturage en tant que conducteur par l'intermédiaire de la plateforme BlaBlaCar (Debroux, 2018). Selon le modèle dispositionnaliste et contextualiste, la pratique est toujours « […] le point de rencontre des expériences passées individuelles qui ont été incorporées sous forme de schèmes d'action (schèmes sensori-moteurs, schèmes de perception, d'évaluation, d'appréciation), d'habitudes, de manières (de voir, de sentir, de dire et de faire) et d'une situation sociale présente » (Lahire, 1998).

Quelles sont les dispositions appelées par la pratique du covoiturage sur une plateforme entre inconnus et incorporées par les conducteurs intensifs de BlaBlaCar ? Quelles sont les caractéristiques du contexte déclencheur de la pratique ? Quels sont les ressorts de la pérennisation de la pratique ?

Pour répondre à ces questions, nous nous appuierons sur une enquête par entretiens et observation participante réalisée auprès d'une trentaine de conducteurs réguliers de la plateforme BlaBlaCar. Âgés de 26 à 62 ans, ceux-ci sont tous actifs, quasiment tous diplômés de l'enseignement supérieur.

Des conducteurs prédisposés à pratiquer le covoiturage entre inconnus sur une plateforme

Comme toute pratique sociale non obligatoire, la pratique du covoiturage en tant que conducteur par l'intermédiaire d'une plateforme est socialement sélective. Elle concerne des individus mobiles

(la mobilité s'accroît à mesure qu'on s'élève dans l'espace social) qui utilisent leur voiture pour se déplacer, ayant accès à Internet et qui ont constitué les dispositions ou compétences nécessaires pour s'engager dans le covoiturage : être enclin à être économe, accepter les contraintes de la pratique (se soumettre aux règles de la plateforme comme créer un profil, répondre aux questions des passagers, éventuellement négocier les lieux de rendez-vous ou de dépose, respecter les horaires, contrôler sa manière de conduire…), avoir des compétences relationnelles permettant de jouer le jeu de la « convivialité » ou le double-jeu de la relation marchande et amicale (Jacquet, 2015), voire avoir le goût de l'altérité. Bien sûr, à ces dispositions peuvent s'en ajouter d'autres comme aimer « rendre service ».

Les conducteurs de BlaBlaCar appartiennent très majoritairement aux catégories moyenne et supérieure (ADEME, 2015). La prise en compte de leur trajectoire sociale permet de différencier les conducteurs enquêtés les plus âgés (ils ont plus de 40 ans), qui ont très souvent connu une mobilité sociale ascendante, des plus jeunes, plus souvent en situation d'immobilité ou de déclassement. Tous ont cependant vécu dans des familles accordant une grande importance à la gestion de l'argent.

Les plus âgés, d'origine populaire, sont souvent issus des strates les plus stables (les pères ont dans de nombreux cas connu une petite mobilité professionnelle), perméables aux normes dominantes (vacances, accession à la propriété) et mobilisées autour des enjeux scolaires. Ils ont appris très tôt l'importance de la gestion de l'argent (tous évoquent les cahiers de compte tenus par un de leurs parents), la retenue dans la dépense (distinguer l'utile et le superflu), le sens de l'économie (le goût de l'épargne). L'attention portée aux dépenses se relâche au cours de leur vie d'adulte : leur mobilité sociale ascendante, souvent renforcée par l'hypergamie (choix d'un conjoint d'une origine sociale et/ou d'un statut social plus élevés), leur donne une plus grande confiance dans l'avenir.

Les plus jeunes sont, quant à eux, fréquemment d'origine sociale plus favorisée. L'aisance économique du milieu d'origine, parfois relative, est toujours récente. On retrouve toujours, au sein du couple parental, un rapport différencié à l'argent ou l'existence de tensions autour de sa gestion. Clara, 27 ans, professeur de lettres, a vécu dans une famille aisée avec un père médecin et une mère professeur des écoles qui ont divorcé lorsqu'elle avait 6 ans. Ses deux parents sont issus de familles de petits indépendants. Alors que sa mère était très dépensière, « elle était tout le temps à découvert, toutes les fins de mois », elle a le souvenir d'un père très soucieux de gérer ses comptes et son patrimoine : « Moi, j'ai des souvenirs, il faisait ses comptes sur l'ordinateur, sur ses tableaux Excel là, avec le code fiscal, il sait tout comment payer moins d'impôts […] il est beaucoup dans le "faut gagner de l'argent", "faut capitaliser", "faut enrichir le patrimoine" ». Clara met de l'argent de côté tous les mois pour « voir venir » : « […] je dirais que je suis attentive, je suis toujours dans la peur de manquer, voilà donc, je vois pas d'où elle vient cette peur, parce que j'ai jamais manqué de quoi que ce soit quand j'étais enfant, donc du coup, je fais toujours attention à ça, mes économies ».

Quelle que soit leur origine sociale, les enquêtés ont tous forgé une disposition ascétique « comme contrôle de soi et substitution du devoir au plaisir ou à l'envie comme guides explicites ou implicites des pratiques » (Darmon, 2010), comme en témoigne leur trajectoire scolaire. Lorsqu'ils sont d'origine populaire, ils disent avoir travaillé « dur » pour poursuivre des études supérieures après avoir été souvent orientés vers le secondaire technique. La reprise d'études en cours de carrière est fréquente quand le niveau scolaire atteint ne correspond pas à celui espéré par les parents. Sylvie, fille d'un directeur commercial et d'une secrétaire, après avoir échoué en première année de langues à l'université, s'est orientée vers un BTS de bureautique sans appétence particulière. Ses parents avaient d'autres ambitions pour elle : « Ils auraient préféré que je fasse des études plus longues, mais comme ils étaient un peu stricts à mon goût eh […] ils auraient aimé que je fasse plus et mieux ». Après avoir exercé le métier d'agent immobilier pendant plusieurs années, elle reprend des études, obtient un master et développe une activité d'*e-learning* en tant qu'indépendante.

Ouvrir son véhicule à un inconnu suppose d'être familiarisé à l'altérité sociale, de posséder les codes pour établir une relation avec autrui. Les enquêtés les plus âgés ont développé une sensibilité à l'environnement international (parmi eux, nombreux ont vécu à l'étranger au cours de leur carrière professionnelle), aux voyages, aux expériences d'arrachement à l'ordre ordinaire des choses et ils manifestent souvent un véritable goût pour les échanges avec des inconnus. *A contrario*, les plus jeunes, de par leur capital culturel, disposent des compétences relationnelles minimales pour échanger avec autrui sans en avoir le goût. Ils se décrivent comme solitaires, peu intéressés par la vie des autres, et s'ils cherchent à engager la conversation avec les passagers, c'est pour remplir le « contrat » : « Quand je parle avec eux, la plupart disent que c'est un peu le principe… » (Clara, 27 ans, professeur de lettres, Capes, père médecin et mère professeur des écoles).

Le contexte déclencheur de la pratique

Avoir incorporé des dispositions ascétiques, acquis des compétences relationnelles, voire développer un goût pour échanger avec des inconnus ne déterminent pas mécaniquement la pratique. L'entrée dans la pratique s'inscrit toujours dans un contexte d'incertitude ou de fragilisation du statut social : il s'agit de difficultés à trouver un emploi à la fin des études, d'une perte d'emploi, d'un déclassement professionnel, d'une séparation qui modifient les ressources disponibles, tant économiques que relationnelles. Après plusieurs mois de chômage, Noria, 27 ans, titulaire d'un master 2, accepte un emploi à 100 kilomètres de la maison qu'elle vient d'acheter avec son conjoint « en CDI ». Elle est surqualifiée pour l'emploi qu'elle occupe et, si rapidement elle obtient une promotion, elle n'est pas sûre d'être faite pour son métier : « Je commence à craquer […] y en a (des fournisseurs) qui sont là en train de pleurer devant moi, y en a certains, c'est du cinéma, c'est pour ça j'arrive à être un peu dure, mais y en a d'autres, c'est pas du cinéma, ils m'expliquent "je vais devoir licencier", je sais […] y a une semaine, j'arrivais à pas y penser le soir, à pas y penser le week-end, et là ça a pris le dessus en fait ». Dans ce contexte d'incertitudes, l'idée de se rapprocher de son travail est hypothétique : « Eh on a acheté une maison ici, c'est acheté, et puis il a un CDI ici, éventuellement oui peut-être déménager sur V., mais on est bien ici ». Elle cherche un moyen économique pour réaliser un trajet qui lui pèse.

La perte d'emploi peut réactiver une forte disposition à être économe mise en veille au cours d'une trajectoire ascendante. Corinne, 46 ans, en ascension sociale (son père, ouvrier, est devenu agent de maîtrise), a occupé des postes à responsabilités très bien rémunérés lui permettant de vivre confortablement. À la suite d'un *burn out* et en arrêt maladie longue durée, elle a peur « de manquer d'argent » : « […] je me suis dit "faut que je réduise mes frais", ce qui était économiquement pas du tout justifié […] en plus, c'est pas 5 ou 6 euros qui vont changer quelque chose », réactivant sa disposition à être économe construite au sein de sa famille : « Ma mère faisait très attention à tout, tout le temps… »

L'engagement dans la pratique suppose enfin l'existence d'un « passeur », familier du covoiturage. Il s'agit, le plus fréquemment, d'un proche ou d'un « autrui significatif », quelqu'un d'intime en qui la confiance est totale et qui fait, très souvent, partie de la famille. Aucun des enquêtés ne fait état de doutes, de réflexions, d'hésitations qui témoigneraient de la mise en œuvre d'un calcul rationnel en termes de coûts/avantages comme le montre, par exemple, le récit d'Aline, 55 ans, hôtesse de l'air : « Ben, ce sont mes neveux qui habitent dans la région parisienne qui viennent voir leurs parents qui m'en ont parlé "oh mais tu devrais faire ça, c'est bien, c'est sympa, tu rencontres des gens", donc je me suis décidée à le faire ».

Des dispositions inégalement constituées à l'épreuve de la pratique

Les dispositions ascétiques ainsi que les dispositions relationnelles sont inégalement constituées chez les usagers intensifs de la plateforme. Une forte inclination à faire des économies peut compenser de

faibles compétences relationnelles, voire la crainte de la confrontation avec un inconnu. Guillaume, ingénieur, 32 ans, fils d'un contrôleur SNCF et d'une mère responsable de service, est depuis toujours attentif à ses dépenses comme ses parents le sont : « En fait, ils m'ont toujours appris à bien gérer l'argent dans le sens où ils ont pu acheter une maison, après, ils ont acheté un appartement puis un deuxième pour mon frère et moi, [qu']on ait un appartement ». À la suite du déménagement de son entreprise en périphérie de la ville, le temps de trajet qu'il réalisait auparavant en train pour se rendre à son travail à 100 kilomètres de son domicile est fortement augmenté. Sur les conseils de sa conjointe, il s'inscrit sur toutes les plateformes de covoiturage et reçoit une demande de BlaBlaCar. Pour avoir de « bons avis » et, selon la plateforme, davantage de demandes de trajets, Guillaume doit faire constamment des efforts pour se montrer « convivial » et surmonter sa grande timidité et la peur du regard des autres. À l'inverse, le goût de l'altérité, des échanges avec des inconnus peut « travailler » une disposition ascétique faiblement incorporée. Charles, 42 ans, formateur, se définit comme un « tchatcheur » altruiste, aimant rendre service et rencontrer de nouvelles personnes, mais ayant des difficultés à respecter les horaires, voire ses engagements. Après plusieurs avis négatifs qui l'ont beaucoup affecté alors qu'il est en quête de profits symboliques, « je me plie en quatre et quand je tombe sur des gens comme ça qui mettent des avis eh, à la légère, pour du retard », il s'efforce d'être à l'heure, « d'être plus structuré ».

L'approche dispositionnaliste montre que l'engagement dans le covoiturage ne se limite pas à une « question de confiance », qu'il résulte à la fois de dispositions ascétiques (avoir une inclination à faire des économies, accepter les contraintes liées à la pratique), de compétences relationnelles ou d'un goût pour l'altérité, et d'un contexte biographique qui favorise leur activation.

Bibliographie

ADEME-6t-bureau de recherche (2015), « Enquête auprès des utilisateurs du covoiturage longue distance », rapport final, Paris, ADEME.

DAGNAUD M. (2015), « L'économie collaborative ou la confiance à tous les étages », *Telos,* https://www.telos-eu.com/fr/societe/entreprise/leconomie-collaborative-ou-la-confiance-a-tous-les.html

DARMON M. (2010), « Des jeunesses singulières. Sociologie de l'ascétisme juvénile », *Agora. Débats/jeunesses*, 56(3), pp. 49-62.

DEBROUX J. (2018), « Les ressorts de l'engagement dans une pratique de consommation collaborative. Le cas des conducteurs d'une plateforme de covoiturage », *L'homme et la société,* 207(2), L'Harmattan, pp. 187-217.

DELAYE R. & LARDELLIER R. (2016), « Introduction. Panser la confiance… Radiographie d'une valeur en souffrance », *in* DELAYE R., *La confiance. Relations, organisations, capital humain*, EMS Éditions, pp. 21-27.

HADRHRI W., DRAC L. & LEMOINE L. (2017), « La confiance au cœur des modèles de l'économie collaborative », XXVI[e] conférence internationale de management stratégique, Lyon, https://www.strategie-aims.com/events/conferences/28-xxvieme-conference-de-l-aims/communications/4824-la-confiance-au-cur-des-modeles-de-l-economie-collaborative/download

JACQUET É. (2015), « Le "prêt payant". Les paradoxes de l'économie collaborative », *Réseaux*, 190-191(2), pp. 99-120.

LAHIRE B. (1998), *L'homme pluriel*, Paris, Nathan.

Le numérique à l'école : la crise sanitaire, une opportunité pour développer une culture numérique

Par **Jean-Marc MERRIAUX**
Directeur du numérique pour l'éducation (DNE) au ministère de l'Éducation nationale, de la Jeunesse et des Sports

Tous les systèmes éducatifs sont engagés dans des transformations pédagogiques et organisationnelles profondes, à tous les niveaux de la scolarité, qui nécessitent de mobiliser fortement et de façon très volontariste les potentialités du numérique. Le numérique est un agent de transformation puissant pour accompagner les politiques étatiques dans toutes leurs dimensions : la modernisation de l'État avec un changement des outils liés au pilotage du système éducatif, le déploiement de nouveaux services numériques pour les enseignants dans le but de renforcer leur professionnalisation, de nouvelles modalités de transmission des connaissances pour les élèves… Mais nous savons aussi à quel point le recours à l'usage du numérique dans nos systèmes éducatifs est un sujet complexe tant il doit être appréhendé avec ambition et discernement.

À la suite de la fermeture de toutes les écoles le 16 mars 2020, l'ensemble de la communauté éducative a dû répondre à cette situation exceptionnelle, qui a touché 12 millions d'élèves, plus de 20 millions de parents, 800 000 enseignants et 400 000 agents du ministère chargé de l'Éducation nationale, en ayant recours massivement au numérique. Les outils institutionnels proposés par le ministère, ses opérateurs et ses partenaires tels que les outils « ma classe à la maison » du CNED, les ENT (espaces numériques de travail) et les ressources numériques ont permis de répondre à l'urgence et aux attentes des différents acteurs. La spécificité française qui repose sur la capacité à articuler les politiques publiques en matière de numérique avec le soutien d'une multitude d'acteurs a su montrer une certaine efficacité, soulignée par l'OCDE qui a cité la France comme l'un des pays ayant le mieux réussi à organiser cette continuité pédagogique.

Cette période de crise sanitaire offre une occasion unique de prolonger la dynamique d'amélioration continue de notre École. Jamais l'éducation n'a utilisé aussi massivement le numérique en si peu de temps, avec une adaptation en temps réel pour garantir la continuité pédagogique. Cette crise, en accélérant l'utilisation du numérique dans notre système éducatif, en aura révélé fortement tout à la fois les atouts et les limites. Il y a nécessité à comprendre et à analyser. Les résultats des états généraux du numérique pour l'éducation qui se sont déroulés les 4 et 5 novembre 2020 sont une formidable manne, et ils doivent nous aider à apprendre collectivement de cette période. Ces travaux se sont nourris des témoignages recueillis, des retours d'expérience, des résultats des enquêtes conduites au niveau national comme international et de l'analyse des données d'utilisation des services, au final un ensemble de matériau collecté d'avril à novembre 2020, partagé avec les représentants de la communauté éducative, les enseignants et les élèves, les parents, mais aussi tous les partenaires de l'école, en premier lieu les collectivités territoriales qui jouent un rôle primordial puisqu'elles partagent la responsabilité du « numérique éducatif » avec l'État [(1)]. La force de ces résultats tient à la démarche participative et décentralisée, développée pour

(1) Loi de refondation de l'école de 2013, où est défini le service public du numérique pour l'éducation, dans lequel les collectivités territoriales jouent un rôle essentiel à travers, entre autres, l'acquisition des équipements numériques…

structurer les états généraux, tant il est évident que l'expérience du quotidien a souvent force de loi en matière de numérique. C'est ainsi par l'analyse des cas concrets, problèmes et solutions, qu'une liste de propositions [2] a vu le jour.

Ces premiers axes qui sont présentés doivent être appréhendés sous la forme d'une constante invitation à améliorer notre système éducatif. Ils ne peuvent être figés, mais, bien au contraire, s'intégrer dans un processus permettant un continuel aller-retour, fait de tests et de perfectionnements itératifs de l'existant. Il est évident que, pour construire des politiques publiques dans le champ du numérique éducatif, l'échange, le partage et l'écoute sont un gage essentiel de la confiance en notre système éducatif, et nous savons aussi à quel point en matière de numérique, la confiance est un élément de structure fondamental.

Il s'agit dans cet article d'effectuer une synthèse intégrant un grand nombre de retours d'expériences observés pendant la crise sanitaire.

Garantir un égal accès au numérique pour tous / Fracture numérique

La période du premier confinement a montré que la **fracture numérique est toujours d'actualité**. Il est estimé que plus de 500 000 jeunes n'ont pas eu les moyens de pouvoir se connecter et travailler à distance.

Les outils et ressources numériques à visée éducative disponibles par le *web* (ENT, classes virtuelles proposées par le CNED, ressources privées, etc.) ont parfois constitué un facteur d'inégalité, car ils n'étaient pas toujours accessibles ou maîtrisés par tous et partout. Ainsi, les dispositifs de scolarité à distance mis en place dans le cadre du premier confinement pourraient même accroître les inégalités scolaires existantes. Ces inégalités d'accès et d'appropriation préexistaient à la crise, qui les a davantage révélées.

Dans le même temps, le travail à distance, puis hybride (à distance et en présence), a mis en évidence les besoins d'adaptation des outils et services à toute la communauté éducative.

La continuité pédagogique mise en place lors du premier confinement a fortement mobilisé les professeurs et demandé une implication importante et accrue des parents (responsables légaux), les plaçant plus fortement que d'ordinaire aux côtés des professeurs pour accompagner les apprentissages des enfants. La mise en œuvre de l'enseignement à distance a démontré le besoin particulier d'accompagnement des familles aux usages du numérique.

Il a fallu adapter les outils et les services à toutes les populations : prise en compte des besoins particuliers des agents, des enseignants et des élèves, mais aussi accompagnement des parents, notamment allophones [3].

À l'École, le recours au numérique (ordinateurs portables, tablettes, logiciels, applications, plateformes, sites Internet, etc.) permet de compenser les différents troubles moteurs, sensoriels, cognitifs, ... que présentent certains élèves sous réserve que les équipements et ressources numériques utilisés soient handi-accessibles.

La prise en compte de l'accessibilité est utile pour tous les élèves et facilite l'accès aux savoirs.

(2) https://www.education.gouv.fr/les-etats-generaux-du-numerique-pour-l-education-304117
(3) Personne ayant une autre langue maternelle que celle du pays où il se trouve.

Travailler ensemble autrement / Culture numérique professionnelle commune

Les dernières études de l'OCDE mettent en évidence que, dans les pays qui ont la plus grande efficience de leur modèle éducatif, la **capacité des enseignants à travailler ensemble, à mieux collaborer, à mieux se coordonner** est un facteur déterminant. Ce point ressort aussi fortement de l'analyse des outils qui peuvent être déployés à l'étranger (voir les tendances du dernier BETT [4]). Il s'agit donc de **construire les « communs numériques »** pour l'ensemble des praticiens de l'éducation.

Si les enseignants utilisent déjà le numérique éducatif pour collaborer entre eux, les possibilités d'échange entre les élèves sont moins exploitées et moins généralisées. Le premier confinement a suscité des modalités de travail variées avec la nécessité de coopérer à différentes échelles. Par ailleurs, l'état de la recherche montre qu'à l'égard de ces pratiques il n'y a « aucune opposition globale et monolithique des enseignants », et que les pratiques collaboratives et l'organisation de collectifs accompagnent « les mutations sociétales liées notamment à la transformation numérique » [5]. Le travail à distance, puis hybride (à distance et en présence), interroge, par conséquent, le choix et la disponibilité des outils mis à disposition, ainsi que leur fiabilité, leur pérennité et leur adéquation aux besoins des différents personnels de l'éducation.

En outre, le premier confinement a imposé une adaptation des modèles habituels de pilotage des établissements. Ces nouveaux processus doivent permettre aux enseignants et aux agents d'acquérir de nouvelles compétences, grâce à un environnement de travail proposant des contenus diversifiés (webinaires, communautés, etc.), à l'intégration des besoins de chacun, ainsi qu'à un accompagnement bienveillant et cohérent.

Enseigner et apprendre avec le numérique

Le numérique vient modifier aussi bien les pratiques pédagogiques que le développement professionnel de l'enseignant. Il implique une **évolution de la forme scolaire**, **tant dans la manière d'enseigner que dans l'aménagement spatial et l'organisation temporelle**. Pour ce faire, il faut repenser les organisations, les lieux et les espaces pour répondre aux **nouveaux besoins pédagogiques induits par le numérique**. Des actions sont à mener sur **l'hybridation des enseignements et du travail**.

La recherche sur les modalités d'appropriation professionnelle constate que « la majorité des technologies ne sont pratiquées quotidiennement que par une minorité d'enseignants et [que] la pratique des technologies à visée éducative en classe, par les élèves, est très limitée » [6].

La période du premier confinement, en modifiant l'espace-temps pédagogique, a nécessité et permis l'intégration de nouvelles modalités d'enseignement à distance, mobilisant le numérique. Les enseignants ont dû trouver comment susciter l'engagement personnel de l'élève dans sa démarche d'apprentissage, en stimulant son intérêt et sa créativité dans le *continuum*, en présence ou à distance, tout en prenant en compte son degré d'autonomie.

Les enseignants ont mis en place de nouvelles modalités de travail avec les élèves. Ceux-ci ont alors dû utiliser le numérique pour suivre les cours, conforter les acquis ou acquérir de nouvelles compétences. Ils ont parfois transposé dans l'apprentissage des outils ou des pratiques développés dans d'autres cadres (celui du jeu notamment) et ont développé de nouvelles formes d'entraide.

(4) *British Education and Training Technology* : le marché international des services et ressources pédagogiques.
(5) Source : DNE-TN2 & CREAD-M@rsouin, 2020.
(6) DNE-TN2 & CREAD-M@rsouin, 2020.

Certains élèves ont décroché faute de compétences suffisantes, de connectivité, d'équipement ou de motivation.

Avant le premier confinement, les études disponibles n'avaient pas établi si l'utilisation du numérique améliorait les résultats scolaires des élèves, sachant que la recherche nuance souvent cette approche en encourageant une prise en compte multifactorielle, écosystémique et non déterministe des pratiques numériques en contexte scolaire [7]. Pour autant, certains apprentissages sont plus efficaces avec le numérique qui permet de varier et d'adapter les supports aux besoins des élèves, de leur proposer un retour immédiat des réussites ou difficultés ainsi que des recommandations. Par ailleurs, au niveau international « dans les pays ayant les meilleurs résultats, les échanges professionnels et la formation entre groupes de pairs sont prépondérants et permettent une évolutivité des systèmes éducatifs » [8].

Il est indispensable que les élèves acquièrent une culture numérique partagée, permettant d'utiliser les outils et services proposés de manière efficace, responsable et sécurisée, et que l'on puisse tirer parti des nouvelles compétences de coopération et de collaboration développées entre pairs.

Les enquêtes internationales, comme TALIS [9] réalisée par l'OCDE, soulignent dans la durée le fort besoin de formation des enseignants français dans le domaine de l'utilisation pédagogique du numérique, tant dans la formation initiale que dans la formation continue. Le premier confinement et l'enseignement à distance, qui mobilisent toutes sortes de services numériques, ont suscité un besoin et une nouvelle demande de formation.

Les premières études menées par les laboratoires de recherche en éducation ont montré que le premier confinement a exhorté, voire contraint les enseignants à s'emparer des outils numériques – et de fait à se former – dans des délais extrêmement courts sans pouvoir, dès lors, bénéficier d'une prise de recul pourtant nécessaire sur leurs pratiques parfois très disparates. Ainsi, la formation continue est nécessaire pour consolider les acquis et permettre une montée en compétences.

Ces enjeux mettent en avant la nécessité de renforcer l'acculturation à de nouvelles modalités de formation (auto-formation, libre accès à des outils de formation…).

Au-delà, l'ambition est de changer la manière dont les professeurs vont enseigner et les élèves apprendre l'usage du numérique, et changer dans le même temps l'enseignement et l'apprentissage avec l'usage du numérique. En intégrant les apports de la recherche, il faut aussi souligner « l'importance de construire des formations sur l'intégration pédagogique [des outils] dans des situations d'enseignement et d'apprentissage », et non de se contenter de « l'apprentissage des outils technologiques » [10].

Favoriser le développement d'un numérique responsable et souverain

La mise en œuvre de la continuité pédagogique et administrative a engendré une **utilisation accrue d'équipements, de services et de ressources numériques**. Cette augmentation des usages a des impacts environnementaux, d'une part. Elle suscite, d'autre part, des interrogations sur les **conditions du traitement des données d'éducation ainsi que la qualité et la disponibilité des outils et des services numériques**.

(7) Voir notamment FLUCKIGER C. (2017), "Les technologies numériques à l'école, quel bilan ?," http://hal.univ-lille3.fr/hal-01613680 et les productions des groupes thématiques numériques de la DNE (2020), DNE-TN2, 3 juillet. Voir également les productions des groupes thématiques numériques de la DNE (Billet), "Éducation, numérique et recherche", https://edunumrech.hypotheses.org/1948

(8) Gibert, 2018 cité par DNE-TN2 & CREAD-M@rsouin, 2020.

(9) Source : http://www.oecd.org/education/talis/TALIS2018_CN_FRA.pdf

(10) DNE-TN2 & CREAD-M@rsouin, 2020.

Assurer la continuité pédagogique au travers de l'usage accru des outils et des services numériques pose de fait la question de la souveraineté numérique de l'École.

Cette souveraineté est garante de la continuité pédagogique elle-même en favorisant, par exemple, la pérennité des outils, services et contenus mis à la disposition des élèves et des enseignants. Elle permet également de garantir le respect des conditions du traitement et du stockage des données d'éducation et de leur réutilisation par le ministère à des fins pédagogiques.

La période du premier confinement et la mise en œuvre de l'enseignement à distance ont montré que de nombreux acteurs, aux côtés de l'État et des collectivités, ont eu un rôle essentiel dans la mise en place de solutions pour assurer la continuité pédagogique, en particulier des entreprises des technologies de l'éducation (EdTech) qui contribuent fortement à l'écosystème du numérique pour l'éducation.

La stratégie numérique de l'État doit favoriser l'émergence d'une filière publique (offres des opérateurs) et privée (offres des EdTech et des éditeurs de l'éducation) soutenable et économiquement viable, en abordant les questions d'interopérabilité, de réversibilité des données vers les élèves et leurs parents, de transfert avec la recherche et d'une stratégie d'achats de ressources et de services numériques par l'ensemble des acteurs de la communauté éducative.

Mettre en place de nouvelles formes de gouvernance et de nouveaux outils d'anticipation

Le service public du numérique pour l'éducation est une compétence partagée entre l'État et les collectivités territoriales, partenaires avec lesquels il est nécessaire d'approfondir et de fluidifier les échanges pour co-construire des politiques publiques plus efficaces et coordonnées.

Il faut renforcer les mécanismes de coordination et de coopération pour s'adapter et anticiper d'éventuelles crises à venir, avec des plans de continuité numérique (prévoir des jours de télétravail, des heures d'enseignement à distance, etc.).

La gouvernance du numérique pour l'éducation en interministériel, ministériel et région académique doit être revue, y compris au sein des écoles et des établissements. Le modèle de partenariat autour de l'École doit inclure, plus largement, tous les acteurs autour du numérique (collectivités, société civile, associations, acteurs culturels, filière industrielle, etc.).

Une mutualisation des initiatives et des propositions nationales et locales est nécessaire afin d'analyser leur généralisation potentielle, anticiper les adaptations, l'ouverture et l'accélération de chantiers en cours, pour construire et préparer l'avenir de toutes et tous.

Face au défi d'un monde où les repères structurants de la République sont attaqués, où la science est remise en question par le bruit des réseaux sociaux, il est plus que jamais important de permettre aux acteurs de l'éducation de sécuriser un socle de savoirs fondamentaux et une culture numérique indispensables au développement de l'esprit critique et à la défense de nos droits et de nos libertés.

C'est bien tout l'enjeu de saisir l'opportunité de la crise sanitaire et de savoir capitaliser sur le déploiement du numérique dans notre École.

La certification de produits fonctionne-t-elle ?

Par **Renaud LABELLE**
et **Sylvain LEROY**
Agence nationale de la sécurité des systèmes d'information (ANSSI)

Les services numériques que nous utilisons au quotidien reposent sur de nombreux mécanismes de sécurité (contrôle d'accès, chiffrement, intégrité, etc.) qui sont pour la plupart installés dans des produits disponibles sur le marché (pare-feu, VPN, composants de sécurité).

Or, si les descriptifs se ressemblent souvent, tous les produits ne se valent pas, et il est très difficile de reconnaître ceux qui apportent un réel niveau de sécurité. Pour se faire un avis sur un produit, il n'existe pas d'autre solution que de vérifier en profondeur que les fonctions de sécurité qu'il prétend apporter sont bien présentes et remplissent leur rôle. Cette vérification nécessite, compte tenu de la complexité des technologies en jeu, des experts de haut niveau dans de nombreux domaines (cryptographie, architecture matérielle, systèmes d'exploitation, développement logiciel sécurisé, etc.) qui doivent en permanence se tenir à jour des nouvelles méthodes utilisées par les attaquants et des mécanismes qui permettent de s'en protéger.

La certification de sécurité est une réponse à cette problématique : effectuée par un tiers indépendant du fabricant, c'est une méthode normalisée d'évaluation de la sécurité des produits, qui permet d'attester qu'ils exécutent correctement les fonctions de sécurité qu'ils prétendent offrir.

L'évaluation de sécurité s'est développée en même temps qu'Internet

L'évaluation des produits de sécurité est née aux États-Unis à la fin des années 1960 dans le monde de la défense, pour maîtriser l'accès distant aux informations militaires classifiées dans les réseaux ancêtres d'Internet. Elle aboutit en 1986 à la publication des "Trusted Computer System Evaluation Criteria" (TCSEC), qui eurent un impact considérable dans le monde naissant de la sécurité informatique, mais qui se révélèrent inapplicables, tant les évaluations préconisées étaient longues et coûteuses.

Rapidement, la communauté économique européenne décida de se doter de ses propres critères : quatre pays avancés dans le domaine, le Royaume-Uni, l'Allemagne, les Pays-Bas et la France, publièrent conjointement en 1990 les "Information Technology Security Evaluation Criteria" (ITSEC), plus orientés vers les produits commerciaux civils. Les autres pays européens, moins avancés, reconnaissaient les évaluations effectuées par ces quatre pays, dans le cadre d'un accord appelé SOG-IS.

En parallèle, d'autres pays non européens développèrent leurs propres critères. Rapidement, il devint nécessaire d'unifier toutes ces initiatives, notamment pour permettre une reconnaissance mutuelle des évaluations. Ainsi émergèrent les « critères communs », initiés par l'ISO en 1999, qui furent reconnus par 17 pays dans le cadre de l'accord international CCRA. Toujours en vigueur aujourd'hui, ils sont utilisés dans le cadre des « certifications critères communs ».

Dans la foulée, la DCSSI (ancêtre de l'ANSSI) fit publier le décret 2002-535 du 18 avril 2002 qui instaura le schéma de certification français actuel, conforme aux « critères communs ». En 2008,

elle créa un autre type de certification, dite « certification de sécurité de premier niveau » (CSPN), plus simple et mieux adaptée aux produits logiciels.

La certification de sécurité en détail

La certification de sécurité est l'attestation de la robustesse d'un produit, basée sur une analyse de conformité et des tests de pénétration. Elle est réalisée sous l'autorité de l'ANSSI par des entreprises privées que celle-ci agrée, les « centres d'évaluation de la sécurité des technologies de l'information » (CESTI).

L'industriel souhaitant faire certifier un produit doit d'abord avoir établi une « cible de sécurité », c'est-à-dire la liste des propriétés de sécurité que son produit prétend satisfaire. La cible de sécurité trace en particulier la frontière entre ce qui est de la responsabilité du produit et ce qui est supposé acquis dans son environnement. Après vérification de la cohérence de cette cible de sécurité par l'ANSSI, l'évaluation est effectuée aux frais de l'industriel par un CESTI de son choix.

À la suite de cette évaluation, un rapport est rédigé par le CESTI et envoyé à l'ANSSI qui, au vu de son contenu, décide la certification ou non du produit, éventuellement en y ajoutant des conditions particulières d'emploi.

Dans le cas d'une certification effectuée selon les critères communs, le CESTI réalise deux grands types de travaux :

- d'une part, il vérifie la conformité des fonctions de sécurité du produit avec celles décrites dans la cible de sécurité, ainsi que sa conformité aux référentiels et critères d'évaluation (qui définissent, en fonction du niveau de certification souhaité, un niveau d'exigence et la puissance de l'attaquant considéré) ;
- d'autre part, il réalise une analyse de vulnérabilités pour s'assurer qu'il n'est pas possible pour un attaquant de contourner les fonctions de sécurité, en regardant le code source du produit, son architecture, la manière dont il doit être mis en œuvre, et en réalisant des tests de pénétration ciblés. En fonction des types de produits et des niveaux visés, ce type de certification peut durer entre 6 et 18 mois et est très coûteux. Il est particulièrement adapté aux composants de sécurité et aux puces des cartes bancaires.

La certification de sécurité de premier niveau française est réalisée en temps limité (25 jours si le produit ne contient pas de fonctions cryptographiques, 35 jours s'il en contient), en boîte noire (sans examen du code source) et est essentiellement un « avis d'expert » sur les fonctions de sécurité apportées par un produit, en prenant en compte un attaquant de niveau modéré. Cette certification n'est pas réalisée selon la méthodologie des critères communs et n'est donc pas reconnue au niveau international.

Les forces et les faiblesses de la certification

La certification offre à un industriel la possibilité unique de faire évaluer son produit en profondeur à un instant donné par un tiers réalisant des attaques de niveau élevé, selon un cadre reconnu internationalement.

Des évaluations coûteuses

Pour atteindre ce niveau d'exigence, des moyens importants sont mobilisés : les CESTI sont régulièrement audités par les meilleurs experts de l'ANSSI afin de s'assurer qu'ils sont bien en mesure de mettre en œuvre le niveau d'attaque attendu. Chaque évaluation est vérifiée par un certificateur de l'ANSSI, qui s'assure que tous les chemins d'attaque possibles ont été effectivement

testés ; en cas de doute, les experts de l'ANSSI et du CESTI engagent un dialogue de pair à pair. Tout ceci permet de garantir que les produits ont été évalués de manière très sérieuse, et que ceux qui obtiennent la certification sont de qualité. Mais, en contrepartie, les évaluations sont coûteuses, et elles ne restent compétitives que parce que l'État accepte d'entretenir à ses frais un centre de certification et des experts de haut niveau à l'ANSSI.

De plus, réaliser des attaques de niveau élevé nécessite des investissements conséquents en équipements et en ressources humaines, qui reflètent les moyens de plus en plus importants mobilisés par les attaquants (entre autres, des groupes criminels). À titre d'exemple, le niveau usuel de certification des cartes à puce requiert de mettre en œuvre des lasers ou des logiciels complexes d'analyse de code.

Une reconnaissance mutuelle difficile à atteindre en pratique

Si les critères communs fournissent une définition commune du niveau de l'attaquant, leur interprétation est difficile, et les évaluations opérées par les différents pays ne sont pas toujours équivalentes. Ainsi, pour les cartes à puce et les composants, des travaux sont menés en permanence par l'ensemble des parties prenantes européennes (industriels, centres de certification, CESTI) pour atteindre une interprétation uniforme de ces critères. Malgré ces travaux, des différences subsistent entre les pays, et l'assurance que chaque évaluation sera effectuée de la même façon dans chaque laboratoire reste illusoire.

Forts de ce constat, les États-Unis aujourd'hui ne réalisent plus que des tests de conformité pour les produits commerciaux. De même, au niveau mondial, seules les évaluations de simple conformité sont reconnues.

Un processus qui n'est pas adapté aux produits complexes ou aux systèmes

Pour être exhaustive, l'évaluation d'un produit selon les critères communs nécessite l'étude de sa documentation, de ses processus de développement, l'audit de ses sites de développement et de production, de ses processus de gestion de vulnérabilité, l'analyse de son code, la réalisation d'attaques physiques, et ce sur l'intégralité du périmètre du produit. Pour les produits complexes, les coûts deviennent rapidement prohibitifs.

De plus, cette certification n'est pas du tout adaptée aux produits modernes, qui sont souvent très connectés et composés d'applications fonctionnant sur des terminaux mobiles et des serveurs distants.

En limitant le nombre de jours utilisables par l'évaluation, la CSPN limite les coûts. Cependant, en temps limité, elle ne peut prétendre à l'exhaustivité, et elle n'est, par conséquent, adaptée qu'aux produits simples.

C'est aussi parce que la certification n'est pas adaptée à tous les cas qu'apparaissent de nouveaux modèles d'évaluation, comme les *bugs bounties*, qui promettent d'être plus agiles, ou les *pentests* mis en œuvre par des prestataires d'audits qui, bénéficiant d'un cadre moins strict, peuvent évaluer des systèmes complexes, voire des systèmes d'information dans leur intégralité (et se révèlent très utiles pour les applications modernes).

Une gestion des vulnérabilités perfectible

Si la certification permet de se faire une bonne idée de la sécurité apportée par un produit, il est fort probable que des vulnérabilités soient découvertes pendant sa durée de vie, remettant potentiellement en cause la valeur du certificat délivré. Pour en tenir compte, certains produits sont réexaminés périodiquement, et les certificats sont depuis peu archivés au bout de cinq ans (ce qui indique qu'un produit ne peut plus être considéré de confiance au-delà de cette durée sans réévaluation).

Cependant, il n'existe pas de moyen simple de réévaluer un produit déjà évalué lorsque celui-ci a été modifié (par exemple en cas de correction d'un *bug* ou d'une vulnérabilité). Selon la procédure, sauf pour quelques cas très simples, il faudrait effectuer à nouveau la plupart des tâches.

De ce fait, ces mécanismes n'incitent pas les industriels à corriger leurs produits certifiés, et on peut encore aujourd'hui trouver des produits certifiés vulnérables, alors que des produits non certifiés sont à jour.

La certification ne vaut pas recommandation

Lorsque l'ANSSI certifie un produit, elle vérifie qu'il offre bien les fonctionnalités de sécurité qu'il prétend apporter, mais elle ne donne pas d'avis sur l'utilité ou la pertinence du produit. Ceci est une source de grande confusion chez les acquéreurs, qui pensent qu'une certification vaut recommandation.

Par contre, lorsque l'agence souhaite recommander l'utilisation d'un produit, notamment par les administrations et les opérateurs d'importance vitale (les entreprises les plus critiques de la nation), elle utilise un autre processus nommé « qualification », qui est basé sur une ou plusieurs certifications, dont les cibles de sécurité jugées pertinentes, mais aussi sur d'autres éléments comme les processus de gestion des vulnérabilités.

Cependant, la qualification est critiquée par ses utilisateurs, car elle recommande parfois des produits dont la sécurité a été évaluée en profondeur, mais qui sont bien moins performants que leurs concurrents. Prenant cette problématique très au sérieux, l'ANSSI réfléchit à l'inclusion dans ce processus de tests fonctionnels et ergonomiques, réalisés en partenariat avec les utilisateurs.

L'avenir : la certification européenne

Faisant le constat que plusieurs schémas de certification existaient, ou étaient en cours de création, dans divers pays de l'Union européenne, créant de ce fait des barrières au sein du marché intérieur et un manque de lisibilité pour les clients, la Commission européenne a proposé la mise en place d'un cadre de certification européen pour les produits, services et processus numériques, qui s'est concrétisé par la publication du "Cybersecurity Act" en juin 2019 (et qui doit entrer en vigueur en juin 2021).

La certification européenne définit trois niveaux de certification : « élevé », « substantiel » et « élémentaire » :

- Dans le cadre d'une évaluation de niveau élevé, des tests de pénétration sont menés par un tiers de confiance comme pour la majorité des évaluations critères communs effectuées en France. La certification est dans ce cas opérée préférentiellement par un organisme public.
- Le niveau substantiel repose lui sur des tests de conformité, dans un esprit similaire à l'approche américaine, qui incluent la prise en compte des vulnérabilités connues. Dans ce cas, la certification est réalisée par un tiers de confiance privé accrédité.
- Enfin, le niveau élémentaire laisse ouvert la voie à l'auto-évaluation du produit par son développeur, se rapprochant ainsi du marquage CE.

L'existence d'un niveau plus faible avec des tests plus simples, donc plus rapides, ouvre ainsi la voie à la certification d'un nombre bien plus important de produits, par exemple les objets connectés.

Cette nouvelle certification européenne va, assez naturellement, donner un cadre européen officiel au SOG-IS, mais aussi chercher à certifier de nouveaux objets, tels que les services d'informatique « nuagique » (*cloud computing*), l'IoT (*Internet of Things*), les équipements 5G ou des processus comme la certification ISO 27001 qui concerne le management de la sécurité des systèmes

d'information. Dans un second temps, des schémas dits sectoriels, adaptés spécifiquement à un secteur de l'industrie comme l'automobile ou la santé, pourraient être étudiés.

Cette certification introduit aussi des améliorations méthodologiques, comme la possibilité d'utiliser des processus analogues à la CSPN pour le niveau élevé. Enfin, elle imposera une meilleure gestion des vulnérabilités : un produit vulnérable perdra certes sa certification, mais la version corrigée pourra la récupérer plus rapidement par l'application d'une méthode sûre et rapide reposant, notamment, sur un processus audité de gestion des correctifs.

Conclusion

La certification est un processus complexe et potentiellement coûteux, qui est perfectible, mais qui reste néanmoins une manière objective et largement reconnue d'évaluer un produit de sécurité : c'est pour l'ANSSI la manière standard de se faire un avis sur un produit. La certification française, globalement de très haut niveau, est reconnue internationalement comme étant de qualité.

La certification européenne, qui est toujours en cours de négociation, est porteuse d'un grand nombre d'améliorations visant à rendre les processus plus performants. Mais au travers de l'élargissement de son champ d'action à de nouveaux types d'objets et à des niveaux plus faibles, elle devrait surtout contribuer à renforcer, pour les entreprises, mais aussi, et c'est une nouveauté, pour les citoyens, la confiance dans le numérique.

Vers la confiance, voire la certification, des systèmes à base d'intelligence artificielle

Par **Julien CHIARONI**
Directeur du grand défi sur « la sécurisation, la fiabilisation et la certification des systèmes à base d'intelligence artificielle », secrétariat général pour l'investissement (SGPI)

Le fonctionnement sûr des logiciels est depuis longtemps au cœur de nombreuses applications. Toutefois, la question reste ouverte lorsque les systèmes intègrent de l'intelligence artificielle (IA). Que l'on pense à la sûreté d'une prise de décision « autonome » en temps réel, à des domaines ne tolérant pas l'erreur de décision ou encore à des attentes d'équité des traitements qui exigent la garantie que ceux-ci ne sont pas biaisés, la confiance placée dans les systèmes intégrant de l'IA doit impérativement être développée.

Les enjeux de l'intelligence artificielle de confiance, voire de sa certification pour les applications qui le requièrent

Un fonctionnement de type « boîte noire » des algorithmes d'apprentissage profond impliquant que l'on ne sache ni les expliquer, ni les garantir

Les récents progrès en IA résultent des avancées dans un domaine numérique particulier, celui de l'apprentissage profond ou *deep learning*, associées à l'augmentation de la performance des architectures électroniques (essentiellement les *Graphics Processing Unit* ou GPU) et à la disponibilité de grandes quantités de données (ou *big data*).

Néanmoins, cette méthode présente un inconvénient majeur. Son fonctionnement est opaque et souvent qualifié de « boîte noire », « dans le sens où l'on peut juger des données qui entrent dans la boîte et des résultats qui en sortent, mais sans savoir ce qui se passe à l'intérieur » [(1)]. Cela implique que l'utilisateur final ne sait en général pas comment elle fonctionne et le concepteur comment en garantir le « bon » fonctionnement.

Un frein majeur à la diffusion de l'IA dans de futurs produits « industriels »

Aujourd'hui, l'intelligence artificielle occupe une place de plus en plus prépondérante dans notre quotidien, au travers par exemple des moteurs de recherche et de recommandations, ou des assistants vocaux. Nous mobilisons ainsi des algorithmes d'une complexité croissante pour produire des services de plus en plus personnalisés. Ces usages requièrent des garanties éthiques et de transparence, notamment inscrites dans la loi en 2016 [(2)]. Ils ne sont toutefois pas, pour la plupart, critiques au sens où elles ne présentent pas ou peu de risques pour les biens et les personnes. « Lorsqu'il s'agit de battre un champion de go ou bien de recommander le film du dimanche soir, la machine peut se tromper, ça n'est pas très grave, votre soirée peut en être gâchée, mais guère plus. » [(3)]

(1) « Les boîtes noires du "deep learning" », *Les Échos*, Benoit Georges, le 27 août 2018.
(2) Loi pour une République numérique (2016) : « Une décision individuelle prise sur le fondement d'un traitement algorithmique comporte une mention explicite en informant l'intéressé. Les règles définissant ce traitement ainsi que les principales caractéristiques de sa mise en œuvre sont communiquées par l'administration à l'intéressé s'il en fait la demande. »
(3) Discours sur l'intelligence artificielle de la ministre des Armées le 5 avril 2019 à Saclay.

Ce n'est pas le cas pour de futurs produits industriels mobilisant des algorithmes d'IA : véhicule autonome, assistant au pilotage, aide au diagnostic médical, contrôle commande industriel, etc. Prenons l'exemple du véhicule autonome : une erreur de décision du système peut potentiellement entrainer un accident grave, dont les conséquences seraient dramatiques pour le conducteur et les usagers ; ceci d'autant plus que des modifications de la perception réussissent parfois à tromper le guidage autonome, provoquant, par exemple, une circulation en sens inverse du véhicule [4]. Pour toutes ces applications dites « critiques », apporter des garanties de fonctionnement (fiabilité, sécurité, disponibilité), voire certifier quand cela s'avère nécessaire, est ainsi un impératif sociétal et économique majeur, mais aussi une véritable opportunité économique, en jetant les bases d'une « IA de confiance pour l'industrie ».

L'impératif d'adopter une approche « système », et pas uniquement algorithmique

Un système à base d'IA est un assemblage de briques logicielles et matérielles permettant de réaliser une fonction ou un service, soit « purement » numérique, soit produisant un actionnement sur le monde physique.

Ce système est un « objet » réalisant une fonction plus ou moins complexe et résultant de l'intégration de trois principales composantes :

- Des données en quantité très importante ou *big data* servant non pas à programmer, mais à estimer un modèle à partir d'« observations » fournies ainsi que des connaissances. La fonction réalisée en est fortement dépendante ce qui implique que ces données et connaissances soient intégrées au système.
- Un algorithme ou une somme d'algorithmes d'IA qui peuvent être de « natures » ou de typologies variables. Par exemple, dans le cas d'un système d'aide à la décision, le concepteur peut avoir recours à des algorithmes d'apprentissage machine, ceux-ci générant des règles à partir de bases de données importantes, ces dernières servant ensuite à alimenter un moteur de règles.
- Un composant ou une architecture électronique sur lesquels sont implémentés les algorithmes avec des contraintes et spécifications associées à l'application visée.

L'algorithme s'intègre ainsi dans un système pour lui conférer de nouvelles fonctions ou propriétés. Il ne doit donc pas être considéré indépendamment de cet ensemble plus large, sans quoi tous les éléments nécessaires ne pourront être pris en compte. C'est pourquoi la confiance, et à terme la certification, ne peut être menée qu'au travers d'une approche « systémique » et pas seulement algorithmique, qui va considérer l'ensemble des composantes, à la fois techniques et fonctionnelles donc dépendantes du contexte d'utilisation et du cycle de vie du produit ; ce dernier point est particulièrement essentiel, dans la mesure où le contexte dans lequel évolue le produit doit être qualifié, mais aussi qu'il peut évoluer sans pour autant que son fonctionnement ne soit impacté.

Un système à base d'intelligence artificielle doit respecter un ensemble d'exigences pour garantir la confiance des utilisateurs et prétendre, suivant les applications, à une certification.

Les terminologies pouvant être amenées à varier, ainsi nous proposons de retenir le regroupement d'exigences suivant, bien qu'il existe évidemment des liens, voire des recoupements entre eux :

(4) Tesla.

- Responsable (éthique, valeurs) : « L'emploi de l'IA, comme l'utilisation de toutes les autres technologies, doit toujours être aligné sur nos valeurs fondamentales et respecter les droits fondamentaux. L'objectif des lignes directrices en matière d'éthique est de s'en assurer dans la pratique [5]. » Citons l'exemple des « biais » par lesquels l'algorithme peut discriminer un groupe de personnes en particulier. Plusieurs initiatives ont proposé des principes permettant de garantir une IA responsable ; parmi ces initiatives figurent les lignes directrices posant le « cadre d'une IA digne de confiance » par la France (GPAI), les travaux de l'Union européenne au travers du High Level Expert Group [6] (HLEG AI) ou encore la déclaration de Montréal [7].
- Fiable et explicable (ou auditable) : le système est capable d'expliquer et d'informer les utilisateurs (ou les concepteurs) de propriétés ou limites de fonctionnement, de ses choix ou raisonnements relatifs à la décision. À cela s'ajoute l'instauration d'un mode de communication entre l'individu et l'IA, afin de permettre une assistance à l'opérateur, à l'utilisateur ou au concepteur de systèmes. Notons que l'« auditabilité » est aussi une notion centrale, notamment pour les systèmes autonomes, qui permettent de comprendre et corriger *a posteriori* une erreur de décision. Enfin, d'autres propriétés techniques doivent également être prises en compte comme la fiabilité, dans laquelle nous inclurons notamment les concepts de robustesse (à savoir l'évaluation de l'aptitude du système à fournir des réponses correctes y compris face à des situations inconnues ou à des malveillances), la contrôlabilité (à savoir la garantie que le système ne fait que ce que l'on attend de lui et rien d'autre, notamment le maintien dans son domaine d'emploi), etc.
- Certification : le produit, service ou système doit être conforme à des exigences spécifiques. Pour ce faire, il faut garantir le fonctionnement du système (fiabilité, robustesse, reproductibilité ou sécurité, soit un ensemble d'éléments qui fournissent des informations sur le système et qui permettent donc en partie de l'expliquer) avec un niveau d'exigence et de criticité définis dans le cahier des charges. Enfin, des normes et standards doivent être édictés. Cela dépend évidemment des secteurs, applications et risques afférents, qui ne concernent donc pas tous les produits, services ou systèmes. À ce titre, le livre blanc de la Commission européenne sur l'IA [8] souligne notamment ce qu'elle considère comme des applications à « haut risque », selon deux critères : le secteur de marché (santé, mobilité, etc.) et le risque pour les bien et les personnes. Citons aussi la publication de l'European Union Aviation Safety Agency [9] (EASA) qui présente une première feuille de route proposant un schéma qui repose sur des *trustworthy AI building blocks*.

Revisiter l'ensemble de la chaîne de conception et d'évaluation des systèmes à base d'intelligence artificielle en vue d'apporter les garanties de confiance nécessaires à leur déploiement

Pour parvenir à développer « une IA de confiance pour l'industrie », il est essentiel de répondre aux problématiques suivantes : concevoir de manière sûre les systèmes, savoir les évaluer pour en garantir le fonctionnement et créer l'environnement normatif adéquat pour, à terme, les certifier.

(5) Discours de Mariya Gabriel, commissaire chargée de la politique numérique, à la Commission européenne.
(6) Lignes directrices en matière éthique pour une intelligence artificielle de confiance, groupe d'experts de haut niveau, avril 2019.
(7) « Déclaration de Montréal pour un développement responsable de l'intelligence artificielle », initiative de l'Université de Montréal lancée en décembre 2018.
(8) Livre blanc (2020), « Intelligence artificielle : une approche européenne axée sur l'excellence et la confiance », commission européenne, février.
(9) EASA (2020), "Artificial Intelligence Roadmap 1.0", février.

Un impératif de conception « systémique » pour le déploiement sûr, voire certifiable, des produits à base d'intelligence artificielle

La réalisation de systèmes critiques à base d'IA nécessite de revisiter les ingénieries classiques (ingénierie de la donnée et de la connaissance, ingénierie algorithmique et ingénierie système) et de les enrichir. Il faut être en mesure de s'assurer de la conformité du système aux besoins et aux contraintes du client, définir des méthodes et outils pour sécuriser l'ensemble des phases de conception, mais aussi garantir des propriétés de type fiabilité, sécurité et cybersécurité, et « maintenabilité » du système ; et cela, tout au long de son cycle de vie. L'enjeu industriel est alors d'outiller de bout en bout toute la démarche de « génie de l'IA », en prenant en compte les dimensions algorithmiques, logicielles et systèmes, mais aussi celles de la donnée et des connaissances, afin de faire émerger les bases d'« une IA de confiance pour l'industrie ».

Il s'agit ainsi d'outiller la chaîne de conception en vue de respecter les exigences et spécifications, d'apporter le maximum d'éléments de preuve et d'expliciter le processus, pour au final réduire la quantité de tests nécessaires à la qualification, voire à la certification, du ou des systèmes. Il est indispensable de disposer ou de revisiter, afin de tenir compte de l'introduction de l'IA, de plusieurs sous-ensembles de la chaîne de conception : les outils d'ingénierie de la donnée et de la connaissance permettant de maitriser l'ensemble des étapes nécessaires à l'obtention d'une base de données qualifiée et représentative du domaine d'emploi concerné par le système, les outils d'ingénierie algorithmique tels que définis par Peter Sanders [10] et d'autres [11] au début des années 2000, et incluant la validation et la vérification des algorithmes, les outils d'ingénierie système, sans oublier la prise en compte au besoin des contraintes d'« embarquabilité » et d'interface entre l'homme et la machine.

L'évaluation de la conformité des algorithmes et des systèmes à base d'IA au cœur du processus de certification

La confiance dans les systèmes à base d'intelligence artificielle requiert également le développement de plateformes d'évaluation aux besoins des applications et services. En effet, en se focalisant sur l'évaluation des « performances » d'une IA à base de données, celle-ci peut se résumer à évaluer la « qualité » d'une fonction dont l'apprentissage est statistique. se pose ainsi la question de la représentativité des données utilisées, de leur couverture par rapport au domaine d'emploi, mais aussi de possibles problèmes de surreprésentation pouvant induire un biais dans le système. À cela s'ajoutent deux questions centrales : quelles sont les métriques les plus adaptées pour réaliser les évaluations ? Comment réaliser une quantité suffisante de tests ?

Pour ce faire, revisiter nos approches techniques est fondamental, notamment en ayant davantage recours à des chaînes de simulation générique, interopérables et évolutives, associées à des schémas de tests (ou *scenarii*) représentatifs du contexte et du domaine d'emploi, voire même des potentielles évolutions de ces derniers. Toutefois, se pose alors la question de la qualification des outils et des modèles eux-mêmes, mais aussi de la reproductibilité des tests. Cela constitue un élément central pour que la simulation puisse être utilisée comme une preuve « acceptable » dans le cadre d'un processus règlementaire d'évaluation et de pré-certification. La définition d'exigences, l'injection de données réelles, voire la réalisation de tests réels comparés constituent des pistes pour permettre de valider cette conformité et par là-même les résultats.

(10) SANDERS P. (2010), "Algorithm engineering: an attempt at a definition using sorting as an example", *Proceedings* of the Twelfth Workshop on Algorithm Engineering and Experiments (ALENEX), *Society for Industrial and Applied Mathematics* – SIAM, pp. 55-61.

(11) ZHANG H., WENG T. W., CHEN P. Y., HSIEH C. J. & DANIEL L. (2018), "Efficient neural network robustness certification with general activation functions", Advances in neural information processing systems (NIPS), pp. 4939-4948.

L'importance de normes et de standards pour le monde numérique, et tout particulièrement l'intelligence artificielle

Développer des normes volontaires est l'une des actions essentielles pour accompagner le développement de l'IA de confiance, qui prennent en considération les enjeux socio-économiques et certains enjeux spécifiques tels que l'éthique (transparence des plateformes, égalité de traitement, etc.), la sureté et la sécurité des biens et des personnes, ceci dans l'objectif d'assurer la souveraineté numérique et de préparer un cadre répondant aux besoins industriels sectoriels comme la santé, l'industrie du futur ou la mobilité, notamment en termes de responsabilité. Certaines normes essentielles sont en cours de réflexion à l'International Organization for Standardization (ISO) (concepts et terminologie ISO/IEC 22989 sur l'éthique, ISO/IEC 24372 ou le management du risque, ISO/IEC 23894), en parallèle de la publication par certains pays de feuilles de route, comme récemment par le German Institute for Standardization (DIN) en Allemagne [12].

Conclusion

La confiance est un élément central pour la diffusion de l'IA dans de nombreux produits et services. À cette fin, une approche règlementaire et la définition de « grands principes » (biais, robustesse, etc.) sont essentielles, mais leur « application » directement dans les systèmes se doit d'être démontrée et prouvée, afin que cette exigence soit effectivement respectée et implémentée, comme cela a pu être fait dans d'autres secteurs. Il nous faut donc développer un cadre « technique », au travers de la revisite des chaînes d'ingénierie ou au travers d'approches outillées plus adaptées pour l'évaluation, permettant l'introduction de l'IA dans les systèmes critiques, et, plus largement, d'une IA pour l'industrie. L'ensemble de ces briques logicielles contribueront ainsi à un « socle » plus large, celui de la confiance numérique, incluant les infrastructures, les données ou l'électronique.

Remerciements

Je tiens à remercier toutes les équipes impliquées dans le grand défi du conseil de l'innovation, tout particulièrement le consortium « Confiance.ai », initiative du grand défi sur la conception d'outils logiciels et des méthodologies associées.

(12) "The German Standardization Roadmap on Artificial Intelligence", novembre 2020.

Blockchain : quelle confiance, pour quels usages ?

Par **Clément JEANNEAU**
Cofondateur de Blockchain Partner, *leader* français du conseil sur les *blockchains* et actifs numériques

En octobre 2015, la revue *The Economist* consacra sa une à une technologie encore inconnue du grand public, la *blockchain*, alors désignée comme une « machine à créer de la confiance ». Cette couverture sonna le top départ d'une frénésie autour d'une innovation dont les possibilités et les limites ont, depuis, souvent été mal perçues. Vue comme complexe, voire obscure, la *blockchain* est devenue l'archétype du "*buzzword*", suscitant emballement chez les uns, agacement chez les autres.

L'économiste Nouriel Roubini, qui se range dans la deuxième catégorie, parle même d'une « escroquerie » et de « la technologie la plus surfaite et la moins utile de toute l'histoire humaine » (1) – rien que ça ! Cet avis très tranché symbolise les réactions disproportionnées, les plus laudatives comme les plus sévères, autour de la *blockchain*. Plus de dix ans après sa création et cinq ans après son entrée sur le terrain médiatique, cette technologie mérite des analyses plus dépassionnées. Peut-on avoir confiance en la *blockchain*, elle qui permettrait justement, dit-on, de se passer de tiers de confiance ? Et si oui, pour quels usages concrets ? C'est tout l'objet de cet article.

Un malentendu originel

Si la *blockchain* a suscité autant de controverses, c'est notamment parce que le ver était dans le fruit dès le départ : aucune définition de la *blockchain* ne fait *consensus*. L'enjeu n'est pas seulement le choix des termes pour décrire cette technologie, mais bien le périmètre qui entoure celle-ci. Ainsi, si une *blockchain* est une base de données décentralisée (partagée entre tous ses utilisateurs, et fonctionnant sans organe central de contrôle), toute base de données décentralisée n'est pas une *blockchain* : il lui faudrait pour cela des caractéristiques supplémentaires, dont la liste peut faire débat.

Exemple typique : si les droits d'écriture et de lecture des données qui y sont inscrites sont réservés à certains acteurs spécifiques, une base de données décentralisée peut-elle être une *blockchain* ? Oui, potentiellement, répondront la plupart des acteurs du secteur, pour qui il faut alors parler de « *blockchain* privée ». Non, répondront certains puristes, pour qui une *blockchain* n'a de sens qu'en version publique, lorsque ces droits sont ouverts à tous.

Au cœur de la confiance, le protocole de *consensus*

L'enjeu n'est pas anecdotique. La confiance envers une *blockchain* tient à la façon dont les informations y sont inscrites et gérées. C'est toute la question de ce qui est appelé « le protocole de *consensus* » : la façon dont les acteurs d'une *blockchain* se mettent d'accord sur l'inscription et la gestion des données, et notamment leur authenticité. On touche là au cœur de la *blockchain* comme « machine à générer (ou non) de la confiance ». Pour schématiser : si le protocole de *consensus* est jugé faible, la confiance générée envers les données ne peut qu'être fragile ; s'il est robuste, la confiance est alors (plus) forte.

(1) « La grande escroquerie de la blockchain », tribune dans Les Échos, 30/10/2018

La *blockchain* dont le protocole de *consensus* est jugé généralement le plus robuste est la première *blockchain* à avoir vu le jour : celle de Bitcoin, née en 2009, justement en écho à la crise de confiance engendrée par la crise financière. Son protocole de *consensus* repose sur un algorithme, appelé le *Proof of Work* (preuve de travail), qui, en quelques mots, repose sur le travail d'acteurs, d'entités et d'individus, appelés « mineurs » : ceux-ci sont en compétition pour résoudre le plus rapidement possible un problème mathématique complexe dans l'objectif de confirmer une transaction sur le réseau, ce qui leur permet alors de toucher une récompense financière. La transaction vient ensuite valider l'inscription d'une donnée sur la chaîne, c'est-à-dire sur le registre : à chaque transaction peut en effet être associé un (petit) ensemble de données.

Pourquoi l'invention de la *blockchain* Bitcoin était inédite

La confiance envers la *blockchain* Bitcoin tient à un assemblage inédit, qui mêle une couche technologique (algorithme de *consensus*, cryptographie asymétrique, réseau pair à pair et registre distribué) avec une deuxième couche, composée d'incitations économiques. En très bref : il est plus rentable, pour un acteur qui dispose d'une forte puissance de calcul, de participer à l'activité du réseau (en tentant de valider des transactions) que de l'attaquer (en tentant de le pirater, ce qui n'est de toute façon à la portée de quasiment aucune entité). En effet, plus l'on dispose d'une forte puissance de calcul, plus l'on a de chances de résoudre en premier le problème mathématique en question et ainsi de remporter la récompense qui vient avec la validation d'une transaction.

Si le terme – assez galvaudé – de « révolution » devait être appliqué aux *blockchains*, ce serait pour qualifier cet assemblage qu'il serait le moins illégitime. La *blockchain* Bitcoin n'est pas infaillible : aucun système informatique ne l'est. Cependant, pour reprendre les mots du grand informaticien français Gérard Berry, « un système est sûr non pas quand il est inattaquable – ce qui est théoriquement impossible –, mais quand cela coûte trop cher de l'attaquer » [(2)]. Or ce principe est au cœur de la *blockchain* Bitcoin, aujourd'hui la plus sûre de toutes les *blockchains* publiques.

Cela ne signifie pas pour autant que la *blockchain* Bitcoin est idéale en tout point : sa forte consommation énergétique est fréquemment désignée comme l'un de ses grands inconvénients, de même que sa vitesse pour valider des données, plus limitée que sur d'autres *blockchains* par mesure de sécurité. En réalité, il n'existe pas de « meilleure » *blockchain* dans l'absolu : tout dépend des critères qui comptent le plus pour les utilisateurs d'un protocole par rapport à leurs besoins.

Cela ne signifie pas non plus que la *blockchain* Bitcoin est totalement novatrice : son inventeur anonyme, se cachant derrière le pseudonyme Satoshi Nakamoto, est venu piocher dans des décennies de recherche académique. La quasi-totalité des composants techniques de Bitcoin proviennent en effet de travaux de recherche publiés dans les années 1980 et 1990.

La première application ouverte par la *blockchain* : la rareté numérique

En réalité, l'originalité de la *blockchain* Bitcoin tient à la combinaison d'éléments qui n'avaient jamais été imbriqués les uns avec les autres. Ainsi, si Bitcoin ne fut pas la première monnaie digitale, elle fut la première à incorporer l'idée d'un algorithme de *consensus* empêchant le problème de la double dépense (le fait d'émettre deux transactions dépensant le même avoir) – ce sans quoi il ne peut y avoir de confiance envers une monnaie.

Ce faisant, la *blockchain* Bitcoin, qui s'appuie sur un croisement inédit d'innovations en théorie

(2) Entretien publié par Rue89 le 21/11/2016

des jeux, en cryptographie, en informatique, entre autres domaines, a permis ce qui n'avait jamais été possible jusqu'à présent : envoyer en ligne une unité de valeur d'un acteur A à un acteur B sans duplication ni passage par un tiers de confiance. En d'autres termes, la *blockchain* Bitcoin a rendu possible la rareté numérique. Lorsqu'un internaute A envoie un fichier (document texte, image, son, vidéo…) à un internaute B, il envoie en réalité une copie, et conserve le premier fichier sur son terminal ; avec Bitcoin, il est devenu possible de s'envoyer de la rareté numérique de pair à pair, c'est-à-dire sans passer par une autorité centrale comme une banque.

La *blockchain* est à la valeur ce qu'Internet a été à l'information

Pourquoi est-ce important ? Parce que ce qui est valable pour le Bitcoin l'est également pour de multiples autres actifs numériques échangeables *via* une *blockchain* (qu'il s'agisse de celle de la *blockchain* Bitcoin ou d'une autre, la principale alternative s'appelant Ethereum). Ces actifs, pouvant être créés par tout internaute, sont appelés « jetons », ou *tokens* en anglais – de là la notion de « tokenisation », qui consiste à créer sur une *blockchain* la représentation numérique d'actifs existants (actions, obligations, actifs immobiliers, etc.).

En définitive, la *blockchain* est à la valeur ce qu'Internet a été à l'information. Internet a permis de décentraliser l'information, en donnant à chaque internaute un pouvoir inédit : celui de publier et d'échanger toute information qui soit, instantanément, auprès du monde entier, sans devoir en demander la permission. La *blockchain* permet de décentraliser la valeur. Avec la *blockchain*, tout internaute s'empare d'un nouveau pouvoir : créer et échanger tout actif de valeur qui soit, avec l'internaute de son choix, (quasi) instantanément, sans nécessiter la permission d'un quelconque tiers.

Une confiance pour quels usages ?

L'intérêt que l'on peut porter aux *blockchains* comme génératrices de confiance dépend étroitement de l'intérêt que l'on porte à ses usages. Comme nous venons de l'expliquer, le premier usage historique des *blockchains* est la création et l'échange d'actifs numériques sans intermédiaire. C'est ce que le grand public connaît sous le terme de « cryptomonnaies », et ce que les entreprises expérimentent depuis quelques années pour des applications financières et immobilières, notamment sous le terme de « tokenisation » présenté plus haut. La banque Santander et la Société générale ont ainsi commencé à expérimenter en 2019 la « tokenisation » d'obligations sur la *blockchain* Ethereum.

Gérer des actifs numériques sur une *blockchain* peut permettre, en particulier, de se passer d'intermédiaires lors des échanges, avec l'automatisation des processus d'émission et d'échange d'actifs. Ce faisant, les entreprises peuvent bénéficier de réductions de coûts, de contraintes et de temps, et limiter le risque de contrepartie pour certaines opérations. Ces applications relèvent d'une logique d'optimisation pour les acteurs financiers existants, mais peuvent également ouvrir de nouvelles possibilités, par exemple l'accès facilité aux marchés de capitaux à des structures plus petites, ou l'apparition de nouveaux produits et services financiers.

Au-delà de la finance

La finance et l'immobilier ne sont pas les seuls secteurs concernés. Le concept de « rareté numérique », qui rend possible la propriété, la portabilité et la traçabilité d'actifs nativement numériques, ouvre de nouveaux champs que commencent à explorer un nombre croissant d'acteurs du sport (autour de l'idée de cartes de collection numériques liées à des sportifs professionnels, comme le propose la prometteuse *start-up* française SoRare, qui a signé des accords avec les plus grands clubs de

football européens), du luxe (autour du concept de « vêtements digitaux »), de l'art ou encore du jeu vidéo.

De façon plus traditionnelle, loin des questions d'actifs numériques, une *blockchain* peut également être utilisée en tant que registre. Elle peut alors servir à prouver l'existence à un temps T d'une donnée ou d'un document numérique (ce qui a des applications en propriété intellectuelle au travers de l'« enveloppe Soleau numérique », comme le propose la solution Datatrust), ou à prouver l'intégrité de données ou documents numériques. C'est ce qui explique, entre autres usages, pourquoi la *blockchain* est aujourd'hui utilisée pour lutter contre les faux documents.

Exemples d'applications réelles

Les exemples d'applications dans le tissu économique, bien que méconnus, sont variés. Rien qu'en France, pensons aux différents établissements d'enseignement supérieur français qui l'utilisent pour certifier leurs diplômes (par exemple, l'ESCP et l'EM Lyon *via* la *start-up* BCDiploma) ; aux nombreux groupes du CAC 40 qui se servent de la *blockchain* Ethereum pour garantir l'authenticité de leurs communiqués de presse et lutter ainsi contre les *fake news* en communication financière (dont Renault, Natixis, Bouygues, Crédit agricole, *via* la plateforme Wiztrust qui s'appuie sur Datatrust) ; au groupe Kering qui utilise depuis l'an dernier la *blockchain* Bitcoin pour enregistrer les certificats d'authenticité numériques des montres de sa marque Ulysse Nardin ; ou encore aux bailleurs sociaux comme Immobilière 3F et acteurs du BTP comme Léon Grosse qui ont recours à la *blockchain* Bitcoin (*via* la plateforme ContractChain), pour garantir la bonne conformité des documents des contrats.

La *blockchain* peut également s'avérer intéressante en version privée, pour s'organiser collectivement entre acteurs qui ne se font pas confiance *a priori* et/ou qui rencontrent des difficultés à collaborer : entreprises concurrentes ou (lointaines) partenaires, entreprises d'une même chaîne de valeur, entités d'un même groupe, etc. Grâce à la décentralisation du registre, le problème politique de la propriété de ce registre est réglé, puisque celui-ci devient techniquement réparti entre tous ses acteurs.

Le cas de la Banque de France

Ce dernier usage correspond par exemple au projet « Madre » développé par la Banque de France, dont la *blockchain* privée a été mise en production en 2018. Jusqu'alors, la Banque de France collectait elle-même les requêtes d'identifiants créanciers SEPA – envoyées par les banques commerciales pour le compte de leurs clients – et gérait elle-même l'attribution de ces identifiants. La Banque de France a choisi de décentraliser le registre : celui-ci est aujourd'hui une *blockchain* répartie entre les banques commerciales et la Banque de France. Chaque acteur dispose ainsi d'une transparence sur la base de données, sans qu'aucun ne la contrôle plus qu'un autre.

En outre, la Banque de France a utilisé des *smart contracts* – des programmes autonomes qui s'appuient sur la *blockchain* et sur des référentiels de confiance (liste des SIREN à jour, etc.) – pour automatiser le processus d'attribution des identifiants et l'inscription de ceux-ci sur le registre. Ce nouveau système a permis de réduire les délais de traitement, de plusieurs jours à quelques minutes.

Une nouvelle économie numérique… en devenir

Dans l'immense majorité des cas cependant, une *blockchain* a peu d'intérêt par rapport à une base de données traditionnelle : cette technologie n'a pas vocation à devenir la règle pour gérer des

données. Son usage ne correspond qu'à certains besoins très spécifiques, cités ci-dessus. Au-delà, il faut bien percevoir que l'essentiel ne se joue pas dans les blockchains privées, ou fermées : bien que celles-ci puissent être parfois intéressantes pour les organisations, elles sont l'équivalent des intranets par rapport au réseau ouvert qu'est Internet. À partir des concepts de « rareté numérique » et de « tokenisation », la *blockchain* ouvre la voie à une nouvelle économie numérique, dont les applications n'ont de sens que sur des *blockchains* ouvertes.

Malgré des avancées réelles ces dernières années, les besoins de facilité d'utilisation, de confidentialité et de rapidité restent encore à satisfaire pour que cette économie numérique prenne son essor massivement. Ce chemin prendra encore plusieurs années et ne doit pas être précipité au détriment des impératifs de fiabilité ; ce sera à ce prix que les utilisateurs grand public pourront accorder véritablement leur confiance aux *blockchains*.

RGPD, trois ans après, où en est-on ?

Par **Marie-Laure DENIS**
Conseiller d'État, présidente de la CNIL

Alors que le règlement général sur la protection des données (RGPD) fêtera son troisième anniversaire le 25 mai 2021, force est de constater que ce texte reste très mobilisateur à tous les niveaux, ainsi que très présent dans l'agenda politique et médiatique mondial.

Afin d'évaluer le chemin parcouru, rappelons brièvement **en quoi consiste le RGPD et les enjeux de son succès opérationnel**.

Le RGPD, un texte au service de la confiance dans le numérique

Rappel de ses principes

Depuis la création de l'informatique, la société s'est numérisée dans toutes ses sphères. Les données personnelles sont devenues le pilier de l'activité commerciale des entreprises, qui tendent à en collecter toujours plus pour affiner la connaissance de leurs clients, et personnaliser en conséquence leurs produits et services. Le développement des objets connectés, des techniques de profilage, des outils de contrôle et algorithmes en tous genres, l'augmentation des cyberattaques, ainsi que les révélations d'Edward Snowden en 2013, ont nourri une prise de conscience collective sur la nécessité de revoir à la hausse le niveau de protection accordé aux données personnelles.

Au-delà des risques pour la vie privée liés à une mauvaise gestion et à une sécurisation insuffisante des données personnelles, certains traitements informatiques présentent aussi de réels risques pour les libertés individuelles et publiques. Par exemple, un recours disproportionné à la vidéosurveillance ou à la cybersurveillance peut placer les personnes dans une situation de contrôle quasi-permanent et peut générer des réflexes d'auto-censure.

Le RGPD n'est pas né d'un droit hors-sol. L'Europe, riche de sa tradition philosophique héritée des Lumières, a consacré une nouvelle génération de droits de l'Homme, celle des « droits-système » afin d'organiser l'univers sous-jacent du numérique, après avoir conceptualisé les droits et libertés, les droits patrimoniaux et les droits sociaux afin de garantir un niveau de protection maximal à la vie privée et aux libertés des personnes.

Le RGPD a ainsi été élaboré autour de trois axes majeurs :

- le renforcement des droits des citoyens européens, tant sur le plan qualitatif, avec la possibilité de mieux comprendre et contrôler l'usage qui est fait de leurs données, que quantitatif, avec l'apparition de nouveaux droits comme le droit à la portabilité ;
- une nouvelle logique de responsabilisation de l'ensemble des acteurs de traitement de données des citoyens européens, quelle que soit leur localisation, remettant sur un pied d'égalité l'ensemble des acteurs européens et internationaux au regard du droit applicable ;
- et le renforcement du pouvoir de sanction des CNIL européennes (Commission nationale de l'informatique et des libertés), avec une hausse des seuils à 20 millions d'euros ou 4 % du chiffre d'affaires mondial des entreprises.

De cette manière, l'Europe a fourni une réponse moderne et innovante aux problématiques d'utilisation des données personnelles, faisant des valeurs de la confiance et de la transparence la clé de voûte de la régulation économique et d'un déploiement durable du numérique dans tous les aspects de l'activité humaine.

Nouveaux mécanismes de régulation à l'échelle européenne

Pour éviter le risque de *forum shopping* qui a pu affaiblir les réglementations du numérique des années 2000, le RGPD a mis en place une mécanique inédite de coopération en réseau d'autorités nationales, une sorte d'intégration décentralisée impliquant de profonds changements dans les méthodes de travail des autorités nationales. Autrement dit, il y a désormais un guichet unique pour les entreprises, à savoir l'autorité de protection des données de son établissement principal, et un guichet unique pour les citoyens, l'autorité de protection des données de son pays. Si l'entreprise n'a qu'un seul interlocuteur parmi les autorités, les décisions qui la concernent sont prises en commun, afin de prononcer une décision applicable à l'échelle de l'Union européenne. En cas de désaccord entre autorités, c'est le comité européen à la protection des données (CEPD), nouvel organe de l'Union européenne, qui arbitre.

Les conséquences pour les entreprises

Bien sûr, pour les entreprises, le RGPD représente un défi de taille : celui de la mise en conformité, pour laquelle il n'existe pas de solution passe-partout. Chaque secteur d'activité et chaque métier appellent des réponses adaptées. C'est là le tout nouveau rôle d'« évangélisation » du délégué à la protection des données, chargé d'aider l'entreprise à procéder à un changement général de posture, en application du principe de responsabilité, pour constamment avoir l'assurance que les politiques et les procédures encadrant l'innovation technologique restent valides sur la durée et à tous les niveaux. Un des nouveaux leviers prônés par le RGPD est le principe de protection des données dès la conception et par défaut (*data protection by design and by default*). Il implique la prise en compte de la vie privée très en amont des projets, par des mesures préventives ou des choix technologiques limitant les risques éventuels de violation de données personnelles.

Cette exigence éthique de mise en conformité dynamique et globale peut nécessiter des investissements importants sur le plan financier et humain. Mais, d'une part, ces principes sont en réalité connus depuis plus de 40 ans avec la loi Informatique et Libertés (loi du 6 janvier 1978) ; d'autre part, ils peuvent également être un vecteur de croissance pour les entreprises, qui sécuriseront leurs consommateurs sur l'utilisation, la qualité et la pertinence des données collectées. En tout état de cause, la protection des données est désormais un sujet de gouvernance interne des entreprises, à la croisée des compétences informatique, juridique, commerciale et de communication.

Ces fondements posés, la responsabilité collective d'être à la hauteur de ces enjeux, de concrétiser les promesses du RGPD et de le faire mieux rayonner se dégage. **Quel a été le bilan de ces trois ans d'effectivité ?**

Bilan à trois ans

À l'échelle de la France

A l'échelle de la France tout d'abord, les chiffres montrent que la mise en œuvre de ce nouveau modèle est plus qu'enclenchée.

L'effet RGPD s'est ressenti du côté des professionnels : plus de 24 000 délégués à la protection des données, représentant plus de 72 000 organismes, étaient déclarés en France fin 2020. Près de 6 000 notifications de violation de données personnelles ont été reçues depuis 2018, avec près de 1 200 dossiers en 2018, 2 300 en 2019 et plus de 2 500 en 2020, ce qui a permis à la CNIL de mieux orienter son action de conseil et de répression, et de mieux jouer son rôle dans l'écosystème de la cybersécurité.

Du côté des particuliers également, le nombre cumulé de visites du site de la CNIL, d'appels et de consultations des questions/réponses disponibles en ligne a enregistré une hausse très importante,

de 60 % depuis 2018, donnant un bon indicateur du besoin d'information sur le RGPD. En 2019, la CNIL a reçu un nombre record de 14 137 plaintes, en augmentation de 27 % par rapport à 2018 et en augmentation de 79 % sur les cinq dernières années. À ce stade, si les chiffres consolidés de 2020 ne sont pas encore connus, on peut tout de même dire que le nombre de plaintes a continué d'augmenter, avec une évolution sensible des demandes d'informations liées à la crise sanitaire.

Ces augmentations apportent un éclairage essentiel sur la structure des problématiques quotidiennes des Français et reflètent leurs trois préoccupations majeures :

- conserver la maîtrise de leurs données et éviter qu'elles soient traitées à leur insu, ce qui est illustré par les 13 % d'augmentation des plaintes relatives au déréférencement ;
- ne pas être dérangé, être entendu et considéré, avec 15 % des plaintes relatives à la réception de prospection commerciale, associative ou politique ;
- et faire prendre en compte leurs droits, tant auprès des employeurs que des services publics, avec notamment 42 % d'augmentation des plaintes liées à l'accès au dossier médical.

En ce qui concerne les sanctions, la CNIL conduit en moyenne 300 contrôles formels par an. Le nombre de mesures correctrices est quant à lui en hausse chaque année, puisque, dans un premier temps, la CNIL a concentré ses efforts sur son action pédagogique auprès des acteurs économiques, en entretenant un dialogue étroit avec les têtes de réseau pour démultiplier son accompagnement, et en produisant de nombreux outils facilitant la mise en conformité, comme le MOOC RGPD, le guide à destination des TPE et PME, et les outils d'analyse d'impact qui sont disponibles sur son site Internet. Cette période de transition étant désormais terminée, la CNIL a prononcé une quinzaine de sanctions en 2020 pour un montant cumulé d'environ 139 millions d'euros, contre 8 sanctions en 2019, ce qui a activé ainsi les nouveaux montants permis par le RGPD.

À l'échelle de l'Europe

Au niveau européen, la coopération est également devenue une réalité quotidienne pour les autorités de régulation. Plus de 1 300 cas transfrontaliers ont été identifiés, 450 procédures dites de « guichet unique » ont été lancées et plus de 150 décisions finales ont été adoptées en application des mécanismes de coopération et de cohérence. Fin 2020, le CEPD a également adopté sa première décision contraignante afin d'arbitrer un différend entre l'autorité irlandaise et les autres autorités européennes concernant Twitter ; il a aussi adopté une vingtaine de lignes directrices, sur différents sujets relatifs à l'application du RGPD, comme notamment son champ d'application territorial, le ciblage des utilisations sur les réseaux sociaux ou le *Privacy by design*, contribuant à une véritable doctrine européenne en matière de protection des données.

S'il n'y a pas de statistiques officielles tenues par le CEPD sur le nombre de sanctions à l'échelle européenne, certains sites privés indiquent qu'à la fin de novembre 2020 environ 420 sanctions avaient été émises, représentant plus de 260 millions d'euros d'amende.

À l'échelle mondiale

Enfin, même au niveau mondial, nous constatons qu'il y a eu un avant et un après 25 mai 2018. Le caractère extraterritorial du RGPD remettant les acteurs internationaux et européens sur un même plan, ainsi que la libre-circulation des données permise sur le territoire sont autant de signaux forts affirmant la volonté de souveraineté numérique européenne. Il ne s'agit pas ici de protectionnisme, mais bien d'affirmer un modèle de régulation basé sur la défense du droit des personnes, notamment par rapport aux GAFAM (acronyme pour Google, Apple, Facebook, Amazon et Microsoft) et en matière de cybersécurité. S'il faut se garder de tout triomphalisme, le RGPD est véritablement devenu une source d'inspiration mondiale.

Certains pays ont procédé à une mise à jour de leur cadre national en matière de protection des données, afin de continuer à commercer avec l'Europe. C'est le cas notamment du Japon, de la Corée du Sud, du Bénin ou encore de l'Australie. Un processus législatif en ce sens est également en cours en Suisse, en Tunisie et au Burkina Faso.

D'autres États ont aussi, pour la première fois, adopté un cadre juridique général encadrant les traitements de données personnelles, dont les principales dispositions peuvent se rapprocher de celles du RGPD. C'est le cas de la Californie avec le "California Consumer Privacy Act" adopté en octobre 2018 et entré en application au 1er janvier 2020, mais aussi du Brésil avec la "Lei Geral de Proteçao de Dados" adoptée en 2019. En Inde, où la Cour suprême a consacré en 2017 le droit à la vie privée comme droit fondamental, un projet de loi est actuellement en discussion au Parlement. Le RGPD est donc devenu un instrument de *soft power* dans la diplomatie actuelle de la donnée.

Focus sur les enjeux de 2020, année de la mise à l'épreuve

De nombreuses études de cas réels ont eu lieu en 2020, testant de fait l'application d'une grande quantité des dispositions du RGPD, qui auraient pu être durement mises à l'épreuve durant l'année qui vient de se terminer.

Les leçons de la crise du COVID

Une des conséquences de la pandémie, tout d'abord, aura été de placer les enjeux de protection des libertés fondamentales et des données à caractère personnel au cœur des débats publics, et de faire émerger d'importants points de tension, susceptibles de déplacer les perceptions et les préoccupations concernant la protection de la vie privée. La CNIL en tire plusieurs leçons.

La première : la grande robustesse des principes posés par le RGPD, qui ont permis d'éviter le détournement de l'encadrement de l'usage des données sensibles et se sont révélés suffisamment souples pour permettre aux États membres de prendre en compte la nécessité de traiter et partager des informations dans un contexte exceptionnel.

Concrètement, les principes de finalité (est-ce que le but de la collecte est clair et précis ?), de nécessité (quelle utilité ?), de proportionnalité (existe-t-il un moyen moins intrusif ?), de minimisation des données (seules les données nécessaires sont-elles collectées ?) et de limitation de la conservation des données (est-ce que les données seront effacées quand le traitement aura atteint son but ?) ont constitué des éléments essentiels de la confiance dans les traitements de données en situation d'urgence, et ils continueront de servir de fil rouge aux décisions dans un monde post-Covid. La crise aura également particulièrement bien montré l'intérêt des approches *by design* préventives que les différents porteurs de projet se sont efforcés d'intégrer dans leurs protocoles de gestion de données.

La deuxième leçon concerne la fonction d'accompagnement et de contrôle du régulateur, indispensable au principe de responsabilisation des acteurs. Le rôle de la CNIL comme guide des administrations et des entreprises privées, mais aussi comme garante des libertés et de la vie privée, est apparu essentiel pour accompagner les pouvoirs publics et les acteurs privés. Cela confirme l'utilité pour la CNIL de communiquer de manière régulière sur sa doctrine afin que les acteurs puissent s'en saisir le plus en amont possible dans le cadre de leurs projets.

Les défis à l'échelle européenne

2020 aura également été marquée par d'autres rebondissements majeurs rebattant les cartes économiques : l'arrêt Schrems II rendu par la Cour de justice européenne, annulant le "Privacy Shield" qui permettait le transfert de données entre l'Europe et les États-Unis ; l'engagement de transférer l'hébergement par Microsoft du Health Data Hub vers une plateforme européenne

dans un délai de deux ans ; les initiatives législatives européennes en matière de marché unique européen avec le "Digital Governance Act", le "Digital Services Act" et le "Digital Markets Act", prochainement suivis du "Data Act" ; et le plan de relance économique volontariste en France.

Ce contexte exceptionnel offre un alignement assez inédit des intérêts entre notre régulation et notre politique industrielle. Il est de notre responsabilité de parvenir à nous en saisir collectivement en vue de mener une politique ambitieuse en matière de souveraineté numérique européenne, pour laquelle le respect du RGPD sera un facteur essentiel de succès.

L'atout confiance
Maîtriser le risque numérique pour construire la cyber-résilience

Par **Fabien CAPARROS**
Agence nationale de la sécurité des systèmes d'information (ANSSI)

Figure 1 : Extrait de "Risk in focus 2021", enquête annuelle IFACI & ECCIA

Avoir confiance en son activité numérique

Précisons les termes. Pour une organisation, un risque stratégique peut être défini au travers de trois caractéristiques : elle ne peut y échapper ; l'impact est potentiellement mortel ; et elle ne peut le transférer totalement. Son caractère systémique signifie pour l'organisation que sa propre cybersécurité est aussi importante que celle de son écosystème.

Étant donné la nature à la fois stratégique et systémique du risque numérique pour une organisation, sa gestion est de la responsabilité du dirigeant. Elle ne peut être ni déléguée ni externalisée. Pour bien comprendre la nature du risque numérique en 2020, reprenons l'analogie développée par Knake et Clarke dans leur dernier livre *The Fifth Domain* (2019). Au cours de la décennie 2000, dans un cyberespace encore juvénile, la menace était principalement un virus ou un ver informatique. La probabilité pour une organisation d'être touchée grandissait mais restait supportable : le risque était technique. Dès lors, **2000 a été la décennie de la protection** et a vu la création de solutions techniques, tels les *firewalls* et autres antivirus. Puis, la décennie 2010 a

vu l'importance du cyberespace croître et de nouvelles menaces surgir, capables de contourner les protections pour viser des cibles stratégiques, comme les infrastructures. Ces menaces, dénommées *advanced persistent threats* (APT), ont fait évoluer le risque pour les organisations les plus essentielles à une nation. Il a donc fallu de nouvelles capacités pour les détecter et les contrer, avec leur lot d'acronymes : SOC, SIEM, CERT [1]... **2010 fut ainsi la décennie de la défense**. En 2020, avec le développement de la cybercriminalité, d'une part, et l'importance prise par le cyberespace, d'autre part, qui plonge les organisations dans des écosystèmes numériques profondément interconnectés et interdépendants, toutes les organisations sont concernées, quels que soient leur taille ou leur secteur. Le risque est devenu à la fois stratégique et systémique, et aucune organisation ne pourra vraisemblablement franchir cette décennie sans subir une attaque sérieuse, directe ou indirecte. **2020 sera donc la décennie de la résilience.**

Pour gérer un tel risque, le dirigeant d'une organisation aura besoin d'analyses de risque dédiées à la décision stratégique, de mettre en place une gouvernance adaptée, et de s'appuyer sur de nouvelles compétences. Le management du risque numérique consiste à éclairer la décision pour trouver le bon compromis entre exposition au danger, coût, et gains opérationnels espérés. Le domaine étant très technique, tant que le risque était également technique, cette décision était déléguée à l'expert qui pouvait garder la complexité à son niveau. Mais, dès lors que le risque est devenu stratégique, la responsabilité est revenue au décideur. Celui-ci doit, certes, monter personnellement en compétence, mais il ne va pas devenir pour autant un ingénieur en cybersécurité. L'analyse de risque qui permettait jusqu'alors à l'ingénieur de créer un système sécurisé au bon niveau doit, aujourd'hui, être un outil d'aide à la décision stratégique pour un décideur. Par ailleurs, la mise en œuvre des mesures de réduction du risque n'est plus limitée à l'utilisateur final, mais implique toutes les ressources de l'organisation, les trois lignes de défense chères aux managers des risques [2]. En conséquence, la gouvernance du risque et l'expertise évoluent au sein de l'organisation pour éclairer à la fois les fonctions techniques transverses en charge des technologies de l'information, les fonctions opérationnelles au cœur des différents métiers et les fonctions de direction.

Face à ce constat, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) s'est engagée avec ses partenaires dans une profonde refonte de sa doctrine de management du risque numérique. Dans un premier temps, le moteur a été repensé **:** la méthode d'analyse des risques numériques de l'ANSSI, EBIOS, avait été créée au début des années 2000, à l'instar des autres méthodes du domaine. Elle avait été régulièrement améliorée, mais restait inaccessible pour un non-expert. Sa nouvelle version, **EBIOS Risk Manager**, élaborée conjointement avec le club EBIOS [3], est ainsi pensée comme un outil d'aide à la décision stratégique, qui offre une vision partagée des risques pour les décideurs et les métiers. Puis, fruit d'une collaboration avec l'AMRAE [4], le guide « Maîtrise du risque numérique, l'atout confiance » propose une démarche progressive pour mettre en place une gouvernance du risque cyber au sein de l'organisation. Enfin, ces publications sont complétées par une collection de guides dédiés à la gestion des crises cyber et à un panorama des nouveaux métiers de la sécurité du numérique.

À l'heure de l'informatique en nuage, des services numériques et des attaques informatiques *via* la *supply chain*, la confiance en ses propres capacités à gérer les risques ne suffit plus. La confiance en ses partenaires numériques est tout aussi importante.

(1) *security operation center* (SOC) ; *security information and event management* (SIEM) ; *computer emergency response team* (CERT).
(2) Le modèle de la maîtrise des risques autour de trois lignes de défense est promu par les associations françaises AMRAE et IFACI depuis 2013. Il fait référence dans le domaine.
(3) Le club EBIOS est une association à but non lucratif qui regroupe les praticiens et les amateurs de la méthode EBIOS.
(4) L'AMRAE (Association pour le management des risques et des assurances de l'entreprise) est l'association professionnelle de référence des métiers du risque et des assurances en entreprise.

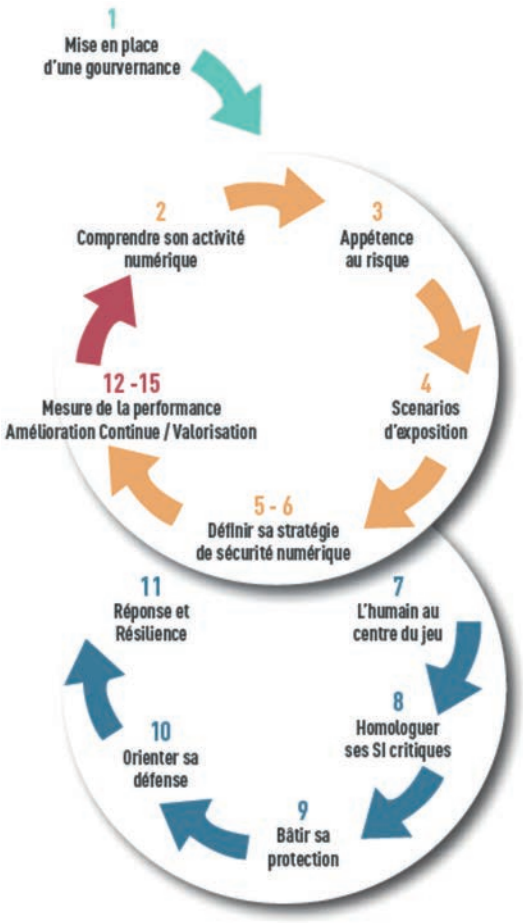


Figure 2 : démarche progressive de construction d'une gouvernance des risques cyber, extrait du guide « Maîtrise du risque numérique, l'atout confiance »

Avoir confiance en ses partenaires numériques

La question n'est pas d'avoir confiance dans le sérieux de ses partenaires numériques, mais de connaître, de renforcer et de surveiller la solidité des liens qui nous unissent à eux et les risques que cela induit. J'ai réalisé ma première analyse de risque EBIOS Risk Manager une année avant la parution de la méthode, en 2018, auprès d'une PME qui opère une plateforme informatique chargée de gérer les flux logistiques d'un grand port de France. Elle interconnecte ainsi toutes les parties prenantes publiques et privées du port. Lorsqu'on a évoqué la confiance qu'ils pouvaient avoir envers leurs partenaires numériques, à l'aune de l'attaque qui a frappé le port d'Anvers en 2011 [5], certains transitaires ont été qualifiés avec humour de « truands-sitaires »… De la même manière, l'attaque NotPetya [6], en 2017, a utilisé comme vecteur d'infection un logiciel de comptabilité imposé par les services administratifs ukrainiens aux entreprises commerçant en Ukraine. Pourtant, dans ces deux situations, il n'est pas question de se passer de ces liens numériques qui unissent les organisations à des partenaires privés ou publics. Il convient donc d'évaluer les risques, de prendre les mesures adéquates et de gérer les risques résiduels. Nous sommes bien dans le champ du management du risque.

Néanmoins, l'évaluation de son écosystème numérique n'est pas chose aisée. Après presque deux années depuis le lancement d'EBIOS Risk Manager, il ressort que les organisations sont encore peu matures dans ce domaine. Prenons l'exemple d'une analyse de risque dans un aéroport. Naturellement, la question du risque terroriste vient en premier. Mais quand vous creusez les aspects métiers, il ressort que le chiffre d'affaires dépend en grande partie de l'exploitation des parkings. Or, ces parkings sont opérés par des partenaires externes, comme Q-Park ou Vinci, entre autres. Si le service venait à être indisponible, les pertes d'activité seraient rapidement très importantes. Quel est le niveau de dépendance vis-à-vis du service numérique fourni par le partenaire (prend-il en charge la perte d'activité éventuelle, l'atteinte à l'image…) ? Quel est son

(5) Le port d'Anvers a été victime d'une attaque particulièrement sophistiquée en juin 2011. Une *mafia* était parvenue à prendre le contrôle du système informatique dédié à la gestion des conteneurs pour pouvoir importer illégalement de la drogue.

(6) L'attaque informatique NotPetya a frappé en 2017 un grand nombre d'entreprises ayant des activités en Ukraine. Particulièrement destructrice, elle a paralysé les activités de nombreuses entreprises dont des multinationales pendant plusieurs jours, voire semaines, et a entraîné des dommages estimés par les autorités américaines à plus de 10 milliards de dollars.

niveau de pénétration dans les systèmes de l'aéroport lui-même s'il était le vecteur d'une attaque (souvenez-vous de NotPetya) ? Quel est son niveau de maturité en cybersécurité ? Peut-on avoir confiance en lui (souvenez-vous des « truands-sitaires ») ? À travers ces quatre questions, EBIOS Risk Manager propose, d'une part, d'évaluer pour chaque partenaire la criticité de la relation afin de doser l'effort que l'on va consentir dans la sécurisation de la relation, et, d'autre part, de faire une cartographie des risques sous forme de radar pour définir une stratégie dédiée à la gestion globale des partenaires numériques. Cette cartographie permet à la fois d'orienter l'effort de sécurité là où il est nécessaire et de diffuser largement la démarche au sein de toute l'organisation. Mais si les questions semblent simples, il ressort que les organisations sont aujourd'hui rarement en mesure d'y répondre. La confiance est donc donnée *a priori*, sur la base d'éléments fragiles, sans réaliser les risques pris, ce qui explique pour partie l'inquiétude des décideurs face au risque numérique (voir Figure 1).

En outre, le partage des responsabilités et des coûts liés à la cybersécurité est souvent mal maîtrisé par les organisations. Il est clair aujourd'hui que la sécurité est perçue comme un coût. Or, entre deux partenaires, la question du partage des coûts mérite d'être posée. Si nous caricaturons un peu : un responsable de la sécurité des systèmes d'information aura tendance à vouloir maîtriser au maximum sa propre sécurité. Il sera donc tenté de l'internaliser de manière à utiliser un système d'information capable d'évoluer dans un environnement extérieur en lequel il n'aura pas confiance *a priori*. *A contrario*, un acheteur voudra reporter l'effort sur le partenaire, quitte à faire jouer la concurrence pour que celui-ci prenne au maximum sa part. En attendant l'avènement éventuel du *Zero Trust Network* [7], la solution se situe entre les deux options.

Se pose alors la question de la responsabilité en cas d'attaque. Il suffit de regarder les clauses de limite de responsabilité imposées par certains *cloud providers* pour se convaincre que cette question est loin d'être anodine. Vient alors la couverture assurantielle. Là aussi, l'âge de la confiance sans

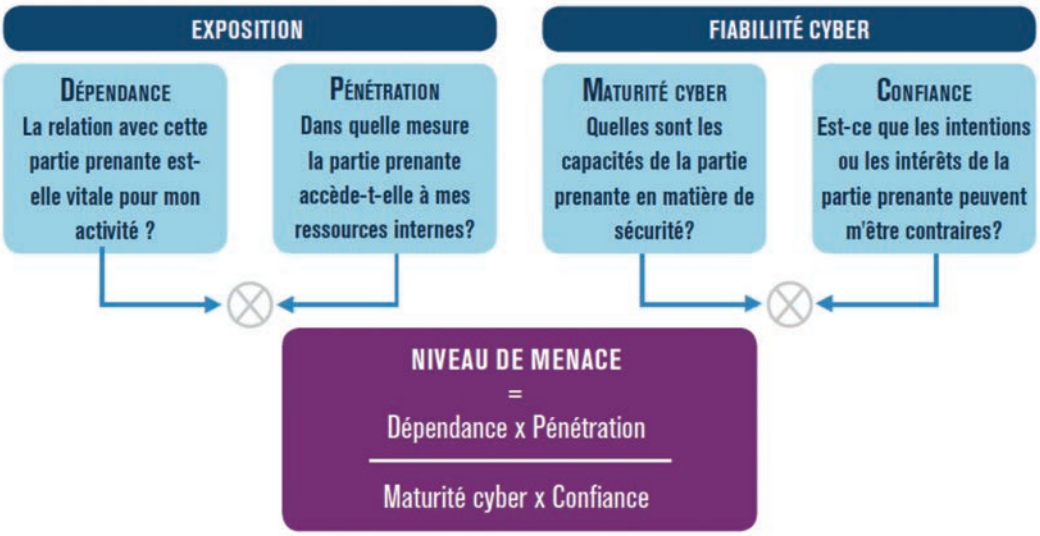


Figure 3 : évaluation du risque lié à une relation numérique avec un partenaire, d'après la méthode EBIOS Risk Manager

(7) Les modèles *Zero Trust* font l'hypothèse que le système d'information d'une organisation, même contrôlé, peut être compromis ou peut abriter une menace intérieure. Ils préconisent donc de considérer l'ensemble de la chaîne de connexion depuis l'usager, de segmenter les ressources, de développer les contrôles et de cesser de faire dépendre l'accès aux ressources de la présence ou non au sein du périmètre du SI.

réelle maîtrise est terminé. Les régulateurs ayant imposé aux assureurs de faire une revue de leurs couvertures dites « silencieuses », le marché s'est durci, et les assureurs sont très regardants face à leur propre exposition à un risque systémique.

Après la confiance dans son activité et la confiance dans ses relations avec ses partenaires numériques, vient la question de la confiance dans son environnement. Comment structurellement mettre en place des mécanismes vertueux pour renforcer la cyber-résilience de son écosystème numérique ?

Avoir confiance en son environnement numérique

Alors que les écosystèmes numériques sont de plus en plus imbriqués, interconnectés et interdépendants, utiliser le management des risques pour améliorer la transparence des offres au sein des chaines de valeur permettrait de bâtir des chaines de confiance. La crise sanitaire en cours a donné un nouvel éclairage sur la question de la confiance entre un offreur et un acheteur au sein d'une chaine de valeur, et a montré les insuffisances du modèle actuel. Au moment de choisir les bons prestataires de visioconférence, le débat autour de la sécurité numérique a été vif comme en témoigne le cas révélateur des offres de la société Zoom [8]. Dans ce contexte, le système actuel de certification de sécurité n'a pas apporté un éclairage suffisant. L'idée d'une meilleure transparence dans les offres est alors apparue et est actuellement étudiée au sein de l'OCDE. Ainsi, au travers d'une démarche d'analyse de risque pertinente et adoptée à la fois par les acheteurs et les offreurs, il pourrait être possible pour les acheteurs de définir les bonnes mesures de sécurité nécessaires dans leur contexte d'emploi et pour les offreurs de se différencier. En complément ou au travers des certifications de sécurité, cette transparence dans les offres pourrait permettre de construire des chaines de confiance au sein des écosystèmes numériques.

Dès à présent, les parties prenantes d'un même écosystème numérique réclament des gages de confiance, notamment les clients des entreprises et les usagers des administrations. Plutôt que d'être considéré comme un coût, l'effort de sécurité peut donc être valorisé au sein des offres de valeur privées ou des missions de service public. Si l'analyse semble évidente, la mise en œuvre est plus difficile. Faire travailler ensemble les responsables de la sécurité du numérique et les responsables métiers ne va pas de soi. Cela a amené l'ANSSI et l'AMRAE à proposer dans le guide « l'atout confiance » une gouvernance mixte, qui intègre le métier dans les comités de management du risque cyber. Ainsi, il devient possible de bâtir des stratégies qui allient sécurité du risque numérique et valorisation des efforts de sécurité. Un euro dépensé pour la sécurité peut alors être un euro valorisé pour répondre à la demande d'une relation de confiance de la part des clients ou des usagers.

Enfin, le plus grand moteur de la résilience d'un écosystème numérique est le système assurantiel. Or aujourd'hui il n'est pas encore en mesure de remplir son office. Pour pouvoir être pleinement efficace, un système assurantiel doit partager un état de l'art à peu près stabilisé et ainsi agir à la fois sur la réduction du risque individuel et du risque systémique. En premier lieu, cela concerne les mesures de sécurité pour réduire le risque, ce que nous appelons « le socle de sécurité » dans EBIOS Risk Manager. C'est sans doute le domaine le plus mature aujourd'hui. À ces mesures de sécurité doit être associé un système d'inspection et d'évaluation de référence, en lequel les différentes parties ont confiance. Ce système peut être transversal ou sectoriel, comme les certifications des navires marchands pour le secteur du transport maritime. Puis vient la connaissance de la menace pour, d'une part, connaître les modes d'action actuels, les cibles, mais

(8) Durant les premiers mois de la crise sanitaire, la société Zoom qui offre des solutions de visioconférence a fait l'objet de sévères critiques mettant en cause la sécurité de ses solutions.

également anticiper les tendances. D'autre part, cette connaissance doit être statistique pour bâtir des modèles agrégés de prédiction des impacts financiers. Enfin, se pose la question de l'aspect systémique du risque qui doit être couvert par des mécanismes dédiés, comme la réassurance ou les systèmes de type « catastrophe naturelle » qui impliquent davantage l'État. Dans tous ces domaines, l'état de l'art n'est pas encore suffisamment stabilisé, mais les acteurs du système assurantiel innovent et progressent, sous le regard attentif de leurs régulateurs.

Conclusion

Pour une organisation, publique comme privée, le management du risque numérique permet de mieux appréhender la question de la confiance dans son activité numérique. Devant la complexité du risque, ses aspects stratégiques et systémiques, ce management nécessite de bâtir la confiance dans son organisation et ses capacités propres autant que dans ses liens avec ses différents partenaires. Il requiert également d'œuvrer à la construction de mécanismes vertueux de cyber-résilience, qui amèneront la confiance au cœur de l'écosystème numérique.

Si l'on peut légitimement ne pas partager l'optimisme excessif de Clarke et Knake, qui annoncent la victoire inéluctable de la sécurité des organisations contre les cyberattaquants, nous les rejoindrons bien volontiers sur le fait que 2020 sera la décennie de la cyber-résilience.

Bibliographie

IFACI & ECIIA (2020), "Risk in focus 2021", rapport.

CLARKE R. & KNAKE R. (2019), *The fifth domain,* New York, Penguin press.

ANSSI (2018), « La méthode EBIOS Risk Manager ».

ANSSI (2019), « Maîtrise du risque numérique, l'atout confiance ».

ANSSI (2020), « Organiser un exercice de gestion de crise cyber ».

ANSSI (2020), « Panorama des métiers de la cybersécurité, édition 2020 ».

ANSSI (à paraître), « Gérer une crise cyber ; La communication de crise face à une crise cyber ».

Qualité, équité, transparence, vérification et explicabilité des décisions algorithmiques

Par **Serge ABITEBOUL**
Autorité de régulation des communications électroniques et de la poste (Arcep), Institut national de recherche en sciences du numérique (Inria)

Introduction

L'informatique accélère les découvertes scientifiques et l'innovation, transforme nos vies et la société. De plus en plus, les logiciels sont amenés à prendre des décisions qui influencent nos vies [(1)] dans les domaines de la santé, la justice, la banque, etc. Ils choisissent les informations auxquelles nous sommes exposés sur les réseaux sociaux et les moteurs de recherche. Les algorithmes ont ainsi pris une forme d'autorité. En « assumant » ou pas la responsabilité qui devrait accompagner cette autorité, les algorithmes vont gagner la confiance des utilisateurs, ou leur défiance. Le triangle « autorité, responsabilité, confiance » est typiquement inhérent aux décisions algorithmiques. Par exemple, dans le cadre des réseaux sociaux :

- **Autorité**. Devant les comportements nocifs de certains de leurs utilisateurs et parfois d'États, certains réseaux sociaux bloquent des contenus, ferment des pages ou des groupes, bannissent des utilisateurs de la plateforme. Doit-on leur laisser ainsi la responsabilité de définir de fait des valeurs de notre société ? Quelle légitimité ont-ils à le faire ?
- **Responsabilité**. Les réseaux sociaux nous informent, nous permettent d'échanger, de tisser de nouveaux liens. Pourtant, entre pédopornographie, bobards (*fake news*), messages de haine, harcèlements, etc., la liste de leurs dérives est longue. Comme participants à la vie de la cité, ne pouvons-nous exiger d'eux des comportements responsables ?
- **Confiance**. De plus en plus, les citoyens mettent en cause les réseaux sociaux. Comment faire pour qu'ils puissent en jouir sans avoir à en supporter les nuisances, et pour rétablir leur confiance dans ces réseaux ?

Ce triangle soulève des questions de qualité, d'équité, de transparence, de vérification, d'explicabilité des décisions algorithmiques, que nous considérons ici.

- **Éducation.** Le problème avec les algorithmes, c'est que nous ignorons souvent ce qu'ils sont réellement et comment ils fonctionnent. Un minimum de compétences pour entrouvrir les boîtes noires est un point de passage obligé pour établir la confiance dans les décisions algorithmiques. Cet aspect, bien qu'essentiel, ne sera pas considéré dans cet article.

La qualité des décisions

Nous sommes régulièrement confrontés à des erreurs de logiciels. Comment pourrait-il en être autrement ? Un correcteur professionnel laisse encore des fautes d'orthographe dans un roman de quelques dizaines de milliers de caractères. Comment espérer la perfection d'un logiciel comme Windows XP contenant 40 millions de lignes de code, coécrites par une armée de programmeurs ?

(1) ABITEBOUL S. & DOWEK G. (2017), *Le temps des algorithmes*, Paris, Le Pommier.

De plus, même si les résultats d'un logiciel sont le fruit de raisonnements logiques, celui-ci peut se tromper, parce que son raisonnement (son algorithme) est incorrect, que les données, sur lesquelles il se base, sont incomplètes, erronées, biaisées, qu'il est mal utilisé, ou que le problème est trop complexe, insuffisamment analysé.

Quand un logiciel est proposé pour prendre une décision importante à la place d'humains, la question de sa qualité se pose de façon aiguë. On est tenté de placer la barre très haut. Par exemple, aux yeux de certaines personnes, il serait inacceptable d'accorder à un véhicule autonome le droit d'emprunter nos routes s'il court le risque de causer un accident mortel. Comme les logiciels sont plus simples à analyser que les humains, plus simples à « corriger », il est légitime d'exiger que le risque soit statistiquement plus faible si le véhicule est autonome. Mais ne serait-il pas disproportionné d'exiger la perfection d'un véhicule autonome, quand nous acceptons de partager la route avec des conducteurs en état d'ébriété, avec d'autres à la vue déficiente, etc. ?

Enfin, les logiciels sont de plus en plus utilisés dans des domaines (typiquement de sciences humaines et sociales) où les concepts sont complexes et difficiles à spécifier de façon précise, des domaines où les meilleurs experts humains peuvent hésiter, ne pas être d'accord. Dans de tels cadres, on a recours à des techniques [(2)] comme l'analyse massive de données (*big data*) ou l'apprentissage automatique (*machine learning*) qui sont souvent les seules capables aujourd'hui d'apporter des réponses. La qualité des décisions ne dépend plus alors uniquement du code informatique, mais aussi des données qui vont guider ce code. Par exemple, les analyses du logiciel COMPAS, utilisé pour aider les juges états-uniens à décider de mises en liberté sous condition, ont mis en évidence la très piètre qualité de ses résultats [(3)].

L'équité

Les logiciels, quand ils proposent des décisions, doivent évidemment respecter nos lois. Mais, au-delà, nous attendons d'eux que, participant à la vie en société, ils respectent aussi nos valeurs éthiques, ainsi qu'ils se montrent « équitables », qu'ils ne présentent pas de biais. Dans *Weapons of Math Destruction* [(4)], Cathy O'Neil explique parfaitement les mécanismes qui peuvent introduire des biais dans l'analyse de données.

La tentation d'introduire discrètement des biais est forte pour ceux qui contrôlent la conception des algorithmes [(5)]. Mais des biais peuvent aussi être introduits involontairement. Sans que l'entreprise en soit consciente, les tarifs des agrafeuses de Stapples.com étaient plus élevés dans les quartiers défavorisés [(6)], parce que le logiciel corrélait le prix avec la distance à un magasin vendant des agrafeuses, et que de tels magasins sont rares dans les quartiers défavorisés.

L'apprentissage automatique peut en particulier conduire à introduire des biais. De tels biais sont parfois causés par des insuffisances dans les données utilisées pour « entraîner » le logiciel, comme cela a été observé pour la reconnaissance faciale [(7)]. Ils proviennent quelquefois aussi du fait qu'un monde numérique peut se contenter d'être le miroir d'une certaine réalité : il a été démontré que le

(2) ABITEBOUL S. & PEUGEOT V. (2017), *Terra data : qu'allons-nous faire des données numériques ?* Paris, Le Pommier.
(3) YONG E. (2018), "A popular algorithm is no better at predicting crimes than random people", *The Atlantic*.
(4) O'NEIL C. (2016), *Weapons of math destruction: How big data increases inequality and threatens democracy*, Crown Books.
(5) DUCOURTIEUX C. & PIQUARD A. (2019), « Concurrence : l'Europe inflige à Google une troisième amende, d'un montant de 1,49 milliard d'euros », *Le Monde*.
(6) VALENTINO-DEVRIES J. (2012), "Websites vary prices, deal based on users' information", *The Wall Street Journal*.
(7) SIGNORET P. (2018), « Une étude démontre les biais de la reconnaissance faciale, plus efficace sur les hommes blancs », *Le Monde*.

logiciel COMPAS [8] (pour la remise en liberté conditionnelle) défavorisait des minorités ethniques, en reproduisant les biais de certains juges états-uniens. Il faudrait aussi parler des algorithmes de classement [9], basés sur la popularité, que l'on trouve dans des applications de rencontre comme Match.com ou de financement comme Kickstarter. Le biais introduit par la mise en avant selon la popularité résulte, suivant les cas, en l'absence de diversité, la discrimination, voire l'exclusion de certains. *The rich get richer, the poor get poorer*.

Si l'équité aborde le rapport entre un individu et un groupe social, on peut aussi s'intéresser au rapport entre un individu et le logiciel lui-même. Un logiciel est typiquement proposé avec des fonctionnalités, des promesses envers ses utilisateurs. On s'attend à ce que le logiciel obéisse aux règles telles qu'elles ont été édictées pour lui-même. Si une plateforme de recommandation de restaurants annonce que les notes qu'elle décerne ne s'appuient que sur les avis de ses utilisateurs, il serait déloyal de sa part de favoriser des restaurants qui seraient clients de certains de ses services.

Nous n'avons fait ici qu'esquisser les grandes lignes de la responsabilité des décisions algorithmiques. Cette responsabilité est un composant essentiel pour construire la confiance. Elle doit s'accompagner de transparence et de vérification.

Transparence et vérification

La confiance dans les algorithmes peut se construire à partir de la compréhension de ce qu'ils font, de leur transparence. Forcés à rendre leurs algorithmes transparents, les entreprises ou les États sont contraints à rendre visibles leurs choix, peut-être à révéler leurs erreurs, leurs errements. Prenons le cas de l'affectation des futurs étudiants de l'enseignement supérieur français dans les formations disponibles. Pendant longtemps, cette affectation a été réalisée en toute opacité par des humains. Ces humains ont été remplacés par des logiciels, d'abord APB puis Parcoursup, ce qui a introduit davantage de justice dans l'affectation. De plus, quand le code de ces logiciels a été mis en accès libre, la procédure est devenue transparente. Un avantage considérable est qu'il devient alors possible d'étudier les règles qui guident ses choix d'affectation, et de les contester. La transparence ouvre la porte au débat.

La transparence des algorithmes gagne du terrain en Europe. Elle devrait se trouver affirmée notamment par les futurs "Digital Service Act" et "Digital Market Act". Il est d'ailleurs intéressant d'observer le contraste entre la transparence attendue de plus en plus de la part des grandes entreprises du *web* ou des États, et une forme d'opacité de la vie privée des citoyens prônée par des règlements comme le RGPD (règlement général sur la protection des données, règlement de l'Union européenne). Ce traitement différencié est destiné à corriger, au moins en partie, la dissymétrie d'information actuelle entre ces acteurs, et pourrait participer au rétablissement de la confiance des citoyens.

Pourtant, la transparence seule ne suffit pas. Par exemple, la « librairie » SSL de Debian (service d'encodage et de certification SSL) comportait une erreur qui affaiblissait son système cryptographique. La transparence (le logiciel était ouvert donc le code en accès libre) a permis à quelqu'un de vérifier le code et de trouver l'erreur, mais il a fallu attendre deux ans que quelqu'un se penche sur le code et trouve le *bug*. La transparence facilite la vérification, mais ne la remplace pas. Ceux qui proposent des algorithmes peuvent toujours déclarer leurs bonnes intentions. Mais, seule la vérification de ces algorithmes permet de se convaincre de la qualité de leurs réponses, de leur respect des valeurs éthiques et de leur loyauté.

(8) LARSON J. et al. (2016), "How we analyzed the COMPAS recidivism algorithm", *Pro Publica*.
(9) YANG K, GKATZELIS V. & STOYANOVICH J. (2019), "Balanced ranking with diversity constraints", *Proceedings* of the Twenty-Eighth International Joint Conference on Artificial Intelligence.

Dans de nombreux cas, la spécification formelle de propriétés, faisant intervenir des humains, est souvent déjà une barrière. Dans le cas du logiciel COMPAS pour la remise en liberté conditionnelle, il a pu être montré que ce logiciel était équitable s'agissant d'une spécification particulière d'« équitable », injuste pour une autre, et que ces deux spécifications (toutes deux pourtant apparemment convaincantes) ne pouvaient être en même temps satisfaites [10].

Pour vérifier le comportement d'un traitement algorithmique, on peut :

- analyser son code et les données qu'il utilise, ce qui s'apparente à faire la preuve d'un théorème mathématique, ou
- analyser ses effets, ce qui tient plutôt à l'étude d'un phénomène physique comme le climat ou biologique comme le cœur humain.

La première approche nécessite d'avoir accès au code et aux données (par exemple, d'entrainement) qui guident ce code. Cela peut être le cas s'ils sont en accès ouvert. Sinon, on doit recourir à des mécanismes lourds d'audit. Il faut bien insister sur la complexité de ce problème de vérification. Si de nombreux résultats ont déjà été obtenus sur la vérification de logiciels dans des domaines tels que la sûreté (*e.g.,* la garantie d'absence de panne pour un logiciel de pilotage de métro automatique), la vérification de propriétés liées à l'équité de décisions a encore été peu étudiée.

L'analyse des effets s'appuie sur des observations, souvent statistiques, du comportement du logiciel. Le logiciel est alors vu comme une boîte noire, ce qui ne simplifie pas le problème. Le logiciel AdFisher [11] a ainsi permis de détecter que les publicités de Google Ads s'appuyaient sur le genre, un attribut protégé : les hommes voyaient des annonces pour des emplois mieux rémunérés beaucoup plus souvent que les femmes. Pour arriver à discerner ce biais, AdFisher a construit des profils d'internautes identiques si ce n'était pour leur genre, et analysé les publicités qu'ils recevaient.

Explicabilité et contestation

La transparence des algorithmes donne des indications sur leur comportement « en général ». Un individu confronté au choix d'un algorithme peut vouloir une explication pour « son cas particulier ».

La loi du 7 octobre 2016 pour une République numérique, comme le RGPD en avril de la même année, a commencé à introduire des exigences d'explicabilité. Cela semble naturel : quand des décisions sont prises qui nous concernent, nous voulons savoir pourquoi. Pour des décisions prises par des humains, on doit se satisfaire de peu d'explications souvent impossibles à vérifier. Pour des décisions algorithmiques, il est techniquement possible d'exiger bien davantage d'explications.

Si un médecin s'appuie sur un système informatique pour le diagnostic général d'un patient, il ne peut se contenter d'obtenir comme réponse : « appendicite ». Le médecin a besoin de la justification du diagnostic proposé, du raisonnement qui conduit à faire ce diagnostic, des statistiques sur lesquelles ce raisonnement s'appuie, etc. Le médecin a besoin de telles explications, pour adopter ce diagnostic, informer le patient, proposer éventuellement d'autres examens, demander l'avis d'un confrère, etc.

On retrouve dans de nombreux cas de décisions algorithmiques ce même besoin de rendre compréhensible une décision, et de la rendre ainsi acceptable. Il n'est pas toujours simple d'obtenir de telles explications, en particulier, les résultats d'algorithmes d'apprentissage automatique,

(10) KLEINBERG J. (2018), "On algorithms and fairness", Collège de France (site web).
(11) DATTA A., TSCHANTZ M. C. & DATTA A. (2015), "Automated experiments on ad privacy settings", *Proceedings on Privacy Enhancing Technologies*.

qui résultent d'énormes volumes d'opérations et sont le fruit de la mise au point de nombreux paramètres, sont souvent difficilement explicables. Cette technique est utilisée en médecine, par exemple, pour détecter des tumeurs. Mais dans des cas comme le diagnostic général, des techniques à bases de règles qui proposent des explications sont préférées.

Comme on peut contester la décision d'un juge, « faire appel », on doit pouvoir contester celle d'un algorithme, car lui aussi peut se tromper. C'est ce que l'on trouve sur certains réseaux sociaux : on peut contester le rejet d'un contenu, bloqué par la modération. Une possibilité qu'offre par exemple Facebook. Devant la critique du fait que cette contestation était traitée en interne, ce réseau social est allé jusqu'à créer un « comité de supervision » indépendant doté des moyens de changer les grandes lignes de la modération. Ce comité agit comme une « Cour suprême », ce qui tend à réduire un peu plus la distance entre un réseau social et un État.

Conclusion

Les réticences envers la prise de décision par les algorithmes s'expliquent parfois par le manque de robustesse et de transparence de ces derniers, par leurs biais, par de nombreuses raisons qui tiennent souvent de la relative jeunesse de l'informatique et de ses usages. Nous avons vu que la transparence, la vérification, l'explication peuvent ouvrir la voie **à** une instauration de plus de confiance en ces algorithmes. Mais il ne faut pas être naïf : les intérêts en jeu sont tels qu'on imagine mal les citoyens seuls pouvoir imposer des comportements éthiques de leurs logiciels aux entreprises toutes puissantes, qui les proposent parfois. L'État doit apporter sa contribution par les lois et la régulation. Pour ce qui est des réseaux sociaux, la régulation proposée par la « Mission Facebook » [12,13] illustre ce que pourraient être de telles lois.

Tant vis-à-vis l'individu que de la société, le contrôle des algorithmes pose de façon concrète, pour chaque contexte, la question de l'autorité que nous voulons leur accorder, celle de leur responsabilité. Mais aucune transparence, aucune perfection des algorithmes, ne pourraient seules éteindre les réticences des humains envers eux. Ces questions se rapportent aussi au pré carré décisionnel que les humains veulent conserver.

Nous disposerons bientôt de voitures autonomes qui se passeront de conducteurs humains. Certaines personnes refusent cette éventualité, voyant dans le fait de ne plus conduire sa voiture une perte de liberté (la personne devient dépendante de la machine), une forme d'infantilisation (les enfants ne savent pas conduire). Toutefois, pour des personnes incapables de conduire en toute sécurité, pour des questions d'âge ou autres, cela représentera surtout un progrès, une forme de mobilité en toute indépendance. Les avis sont contrastés.

Voulons-nous de robots-aide-soignants ? De robots-juges ? De robots-policiers… ? Dans chaque cas, les réponses ne sont pas simples, car c'est notre humanité qui est mise en question. Et les réponses évoluent dans le temps, en même temps que nous apprenons à vivre avec des logiciels de plus en plus sophistiqués. Dans ce cadre, il est important de répéter que nous ne pouvons céder de prises de décision à des algorithmes par commodité ou par paresse, que cet acte doit résulter de choix qu'il nous faut prendre collectivement.

(12) ABITEBOUL S. & POTIER F. *et al.* (2019), « Créer un cadre français de responsabilisation des réseaux sociaux : agir en France avec une ambition européenne », www.economie.gouv.fr
(13) ABITEBOUL S. & CATTAN J. (2020), « Nos réseaux sociaux, notre régulation », *Le Grand Continent*.

Prouver son identité en ligne : l'enjeu d'une solution régalienne de confiance

Par **Valérie PÉNEAU**
Programme interministériel « France Identité Numérique »

Dans un environnement de dématérialisation croissante des démarches, la garantie de l'identité de son interlocuteur sur Internet – personne physique ou morale – est un facteur clé de confiance.

Être en capacité de prouver son identité en ligne, de façon simple mais sécurisée, est par conséquent devenu un enjeu tant pour les fournisseurs de service, victimes de fraudes croissantes, que pour les usagers qui souhaitent maîtriser leurs données personnelles et se prémunir contre l'usurpation d'identité.

Depuis 2014, le règlement européen dit eIDAS précise les différents niveaux (faible, substantiel, élevé), de garantie – et donc de confiance – s'attachant aux moyens d'identification électroniques, selon les éléments de sécurité (techniques, procéduraux, organisationnels) mis en œuvre. Il fixe par ailleurs un principe d'interopérabilité et d'opposabilité à l'échelle européenne des schémas d'identification notifiés par les différents États à la Commission européenne.

À ce jour, 17 de nos voisins ont ainsi notifié un schéma d'identification (regroupant à la fois le moyen technique d'identification et le parcours utilisateur permettant de s'en servir) de niveau élevé.

Pour combler notre retard et contribuer à la sécurisation d'un écosystème numérique national en constante augmentation, notamment dans le domaine public (projet AP2022), se traduisant par des échanges massifs de données, les ministres de l'Intérieur, de la Justice et le secrétaire d'État chargé de la Transition numérique ont, en janvier 2018, mis en place un programme interministériel ayant pour objectif de concevoir et de déployer un moyen d'identification électronique – l'identité numérique régalienne – susceptible d'atteindre ce niveau de garantie élevé.

La généralisation, à partir de l'été 2021, d'une nouvelle carte d'identité, dotée d'une puce pouvant permettre de servir de source à ce futur moyen d'identification électronique, sera une étape clé dans l'avancement du projet.

Qu'est-ce que l'« identité numérique régalienne » ?

Dans son rapport de juin 2020 [(1)], le Conseil national du numérique parle d'identités numériques au pluriel. Selon la définition retenue, un même usager dispose en effet *de facto* de plusieurs identités sur Internet :

- Au sens le plus large, l'identité numérique est assimilable à l'« empreinte digitale », englobant toutes les traces laissées sur la toile (géolocalisation, habitudes de navigation, ressources consultées, etc.).
- L'identité numérique dite « déclarative » est celle(s) que l'internaute se choisit librement, notamment dans ses interactions sur les réseaux sociaux (comme le choix d'un pseudo sur Twitter).
- Enfin, l'identité numérique dite « civile », « légale » ou encore « régalienne », est celle qui correspond

(1) Rapport demandé en juillet 2019 par le secrétaire d'État chargé de la Transition numérique (2020) : « Identités numériques : clefs de voûte de la citoyenneté numérique ».

aux données d'état civil, et celle sur laquelle repose l'exercice des droits et devoirs citoyens. En regard des termes du règlement eIDAS, elle se compose des données d'identité dite « pivot [2] ».

C'est à cette dernière acception, transposition dans le monde numérique de l'identité physique attestée notamment par les titres d'identité, que le reste de l'article fera référence.

Des enjeux multiples

« L'identité numérique est l'élément pivot qui déterminera de quelle manière chacun d'entre nous pourra accéder à la multiplicité des usages qui forment notre vie quotidienne, dans le respect de sa liberté, de son intégrité et de son individualité », rappelle le Conseil national du numérique.

Au-delà de la confiance d'ensemble dans l'écosystème numérique soulignée en introduction, qui conditionne évidemment la poursuite de son développement, les enjeux de l'identité numérique sécurisée sont multiples :

- **Un enjeu de souveraineté**. Depuis 1792 en France, l'État a la responsabilité régalienne de l'état civil. La production de titres d'identité physiques en est le prolongement. Si l'État n'est pas en capacité, dans un délai raisonnable, d'offrir un service équivalent à ses citoyens dans le monde numérique, la pression des besoins est tel qu'il sera *de facto* contraint de le « déléguer » soit à une solution publique étrangère (interopérable en France en application du règlement européen eIDAS), soit à un acteur privé, les GAFAM investissant massivement dans le domaine. Ce faisant, il perdrait la maîtrise même de l'accès à ses propres services dématérialisés, y compris les plus sensibles. Le Conseil national du numérique soutient ainsi que les impacts de la numérisation des échanges et des rapports sociaux, sur notre société et ses valeurs, « imposent que le lien entre l'identité, garantie par l'État, et l'identité numérique, jusque-là plutôt associée aux fournisseurs de services privés, soit réinstauré et affirmé avec force ».
- **Un enjeu de lutte contre la fraude et contre l'usurpation d'identité en ligne**. Ce risque pèse de façon croissante sur le quotidien des Français qui craignent pour la protection de leurs données personnelles. Dans un récent sondage [3], un Français sur cinq déclare avoir déjà été victime d'une usurpation d'identité en ligne. Pour les fournisseurs de services dématérialisés, cet enjeu est massif. Ainsi, pour les banques, la 5e directive (UE) 2018/843 relative à la lutte contre le blanchiment des capitaux et la lutte contre le terrorisme exige le renforcement des mesures d'authentification en ligne. Sa transposition en droit français par ordonnance et décrets du 12 février 2020 prévoit notamment pour l'entrée en relation à distance le recours à des moyens d'identification électroniques qualifiés au niveau substantiel, au sens du règlement eIDAS.
- **Un enjeu d'inclusion.** À partir du moment où, *de facto*, l'identité numérique peut conditionner l'accès en ligne à l'exercice des droits et devoirs du citoyen numérique, il est impératif que le moyen d'identification électronique proposé soit accessible à tous, facilement et en toute confiance. L'identité numérique régalienne sécurisée peut également être en elle-même un facteur d'inclusion, en évitant des déplacements physiques ou la manipulation complexe de scans de justificatifs d'identité, en offrant à tous une solution simple et gratuite de sécurisation, trop souvent réservée jusqu'à présent aux seuls initiés à la sécurité numérique.
- **Un enjeu économique et de transformation numérique**. Une identité numérique sécurisée permet enfin la dématérialisation de bout en bout d'usages considérés jusqu'à présent comme trop sensibles pour l'être ou exigeant de multiples dispositifs de réassurance quant à l'identité de leur bénéficiaire. De la même façon, elle peut permettre l'ouverture et/ou la simplification de nouveaux services privés en ligne, dont la phase de confinement sanitaire a prouvé l'utilité.

(2) Nom (courant et/ou d'usage), prénom, date et lieu de naissance, sexe.
(3) Sondage IPSOS réalisé pour le compte du programme « Identité numérique », en octobre 2019.

L'identité numérique, dont le marché est estimé par une étude [4] de 2019 comme susceptible de dépasser le milliard d'euros d'ici dix ans, est un formidable vecteur d'innovation et de croissance, et inscrite comme telle au plan de relance. La filière industrielle française est particulièrement dynamique et reconnue sur un marché international en pleine expansion.

Le futur moyen d'identification électronique régalien

Au quotidien, nous nous authentifions en ligne sur nos multiples comptes par l'association d'un identifiant et d'un mot de passe. À mesure que ces derniers sont de plus en plus nombreux et de plus en plus complexes, leur gestion devient un des facteurs pénalisant l'usage d'Internet. Selon une étude récente [5], la création de ces comptes en ligne est la première source d'agacement des internautes. Leur fiabilité est réduite [6], obligeant les fournisseurs d'usages sensibles à ajouter des dispositifs de réassurance complémentaires parfois complexes.

S'agissant des usages publics, la plateforme FranceConnect a, depuis 2016, apporté une première étape de simplification et de sécurisation à cette phase d'identification et d'authentification : elle permet en effet d'avoir accès à plus de 600 services différents à partir d'une porte d'entrée (une « identité numérique ») unique (numéro fiscal *via* impôts.gouv.fr ou numéro de sécurité sociale *via* Améli par exemple), en vérifiant les données d'identité correspondantes auprès du répertoire national d'identification des personnes physiques géré par l'INSEE, avant de les transmettre aux fournisseurs de service qui en ont besoin.

Le niveau de garantie de ces identités numériques reste toutefois de niveau faible. L'objectif est par conséquent de mettre prochainement à disposition des usagers un moyen d'identification électronique avec un niveau de sécurité substantiel et/ou élevé au sens du règlement eIDAS. Un tel moyen suppose la conjonction d'au moins deux facteurs d'authentification [7], une vérification de l'identité du futur détenteur du moyen d'identification, et la mise en œuvre de mécanismes cryptographiques protecteurs des données d'identité. Au quotidien, le moyen d'identification électronique se présentera sous la forme d'une application mobile ou d'une application *web*, en interaction avec un titre d'identité électronique.

À défaut de numéro unique d'identification ou de registre unique de population comme dans de nombreux autres pays européens, seuls les titres d'identité garantis par l'État font en effet autorité en France pour la preuve et la vérification d'identité des personnes physiques. Munis d'une puce protégeant les données d'identité, les passeports, les titres de séjour et, demain, la future carte nationale d'identité électronique pourront devenir ainsi également, si l'usager le souhaite, sans recourir à un fichier central et sous sa seule maîtrise, la source de son identité numérique en ligne.

Un recours limité et facultatif à la technologie de reconnaissance faciale, toujours sous contrôle humain

Pour atteindre un niveau de garantie substantiel ou élevé, il faut s'assurer que le moyen d'identification électronique est bien créé au bénéfice de son titulaire légitime. La vérification d'identité de ce dernier doit donc faire l'objet d'une attention particulière. Cette vérification peut s'opérer, selon le règlement eIDAS, soit en face-à-face (par un agent de guichet assermenté), soit par un dispositif équivalent (vérification d'identité à distance). Les exemples étrangers montrent

(4) Étude EY Parthénon sur le modèle économique de l'identité numérique.
(5) "Customers attitudes to digital identity: Meet the expectation of tomorrow", Onfido.
(6) Assimilable à une garantie de niveau « faible » au sens du règlement eIDAS.
(7) On distingue habituellement trois types de facteurs : ce que je possède (téléphone, courriel, carte..) ; ce que je sais (code, mot de passe..) ; ce que je suis (donnée biométrique).

que ces deux modes d'enregistrement sont nécessaires à l'adoption et au déploiement des moyens d'identification électronique. Le premier oblige à un déplacement, mais est plus inclusif. Le second permet à l'usager de créer son identité numérique quand et où il le souhaite.

S'agissant du face-à-face physique, en application des recommandations du rapport du Conseil national du numérique et de la mission parlementaire, il est envisagé, pour remplir cette condition préalable à la création d'un moyen d'identification par l'usager, de capitaliser sur le temps de vérification d'identité au moment de la délivrance d'un nouveau titre d'identité par les agents en mairie, lieu de confiance par excellence.

Si l'usager le préfère, un mode d'enregistrement complètement digitalisé pourrait lui être proposé. Dans cette hypothèse, la vérification d'identité serait opérée en deux temps : par la mise en œuvre d'un algorithme de comparaison entre le visage de l'usager, transmis par *selfie* et vidéo, et la photographie de son titre d'identité ; et la vérification du résultat de cette comparaison, confirmé ou infirmé par un opérateur, spécialement formé à cet effet, selon les préconisations de l'ANSSI (agence nationale de la sécurité des systèmes d'information). La technologie dite de reconnaissance faciale, dans son acception d'authentification [8], n'intervient donc qu'au moment de la création de l'identité numérique, uniquement si l'usager préfère ce parcours utilisateur, et sous contrôle humain.

La promesse d'un nouveau service public de confiance

L'identité en ligne porte la promesse d'une nouvelle manière, à la fois sûre et simple, de s'identifier et de s'authentifier en ligne comme dans différentes situations de la vie où cela est nécessaire : accéder à un lieu sécurisé, réaliser une procuration en ligne… Le futur moyen d'identification électronique régalien, appuyé sur les titres d'identité, n'a pour autant pas vocation à être utilisé dans toutes les interactions, notamment les plus quotidiennes qui se contentent largement de niveaux de sécurité inférieurs.

Par ailleurs, la France a une histoire singulière avec l'identité numérique. Depuis une vingtaine d'années, plusieurs projets plus ou moins directement liés à l'identification électronique ont échoué pour des raisons diverses ; ils ont en commun d'avoir toujours suscité de fortes résistances. Si l'encadrement juridique, national et européen a, au cours des années récentes, profondément évolué, et si les enjeux de sécurisation sont de mieux en mieux compris, les enseignements du passé ne doivent pas être oubliés.

L'enjeu de conviction et d'adhésion est par conséquent sans doute le plus complexe à maîtriser. Le succès du projet est conditionné non seulement par la qualité de la solution technique et la pertinence des usages qui lui seront associés, mais également et surtout par la confiance que les usagers y accorderont. Proportionnalité d'utilisation, non-traçabilité des usages, protection et frugalité des données, réversibilité, transparence de l'application, sont autant de gages indispensables, à accompagner d'une forte et durable action de pédagogie et de communication, à laquelle doivent être associées l'ensemble des parties prenantes de l'écosystème numérique. Avec pour objectif partagé, selon les termes du Conseil national du numérique, « la mise en place d'une identité numérique citoyenne, de confiance, inclusive, dynamique et propice au développement d'innovations : soit une identité numérique à la française ».

Bibliographie

EYNARD J., BENSA C., BRUGGEMAN M., MANGIN C., MONTEIL M. & NEIRINCK C. (2019), Journée d'étude « L'identité à l'épreuve du numérique », IDP-Université Toulouse 1 Capitole.

(8) Voir sur le site de la CNIL : « Reconnaissance faciale : pour un débat à la hauteur des enjeux », https://www.cnil.fr/fr/reconnaissance-faciale-pour-un-debat-a-la-hauteur-des-enjeux

Le rôle des communautés (*open source, open data, open gov*)

Par **Mathilde BRAS**
Experte de la transformation numérique de l'action publique,
Membre de la Fondation internet nouvelle génération

Public Money? Public Code! En septembre 2017, un collectif d'organisations de la société civile, mené notamment par l'association de défense du logiciel libre Free Software Foundation Europe, lance une campagne multilingue appelant les représentants et décideurs publics européens à adopter des législations statuant que tout « logiciel financé par le contribuable pour le secteur public soit disponible publiquement sous une licence de logiciel libre et ***open source*** » [(1)]. Depuis son lancement, près de 30 000 personnes et plus de 200 organisations – publiques, privées, associatives – ont rejoint cet appel. La philosophie sous-jacente à ce plaidoyer en particulier a eu une grande résonance auprès de nombreux mouvements, tantôt impulsés par la société civile, tantôt proposés par l'acteur public, dont la principale motivation est souvent la même : la transparence – technique ou non technique – de l'action publique est l'un des garants de la confiance démocratique et du respect des droits fondamentaux.

Lors des premiers pas de l'***open data*** en France, l'article 15 [(2)] de la Déclaration des droits de l'homme et du citoyen a été l'étendard, tant des associations que des administrations publiques, pour mettre à jour, avec la loi pour une République numérique de 2016 [(3)], la législation sur le droit à l'information et « augmenter » la loi d'accès aux documents administratifs de 1978 [(4)]. Depuis 2014, la participation de la France au Partenariat pour un gouvernement ouvert (PGO) a permis d'impulser des actions pour rapprocher l'administration de collectifs tiers (société civile, entrepreneuriat, recherche, etc.). Initiative multilatérale lancée en 2011 par huit pays signataires, le PGO promeut l'***open government***, ou ***«open gov»***, favorisant les valeurs d'ouverture et de transparence publiques, les nouvelles formes de dialogue et de concertation avec la société civile, et le rôle du numérique pour faire vivre ces valeurs.

L'ouverture des données publiques, la mise à disposition des codes sources développés par les administrations et la co-construction des politiques publiques impliquent un changement de posture des acteurs publics. **Dès lors qu'il s'agit de mettre en place des « dispositifs d'ouverture publique »** voués à améliorer la confiance des citoyens envers la puissance publique, **assembler des communautés d'acteurs pluriels – agents publics, entrepreneurs, chercheurs, représentants de la société civile – a un impact certain sur les politiques publiques**. L'apport de la « puissance créatrice de la multitude [(5)] » dans l'État est vecteur d'innovation technologique

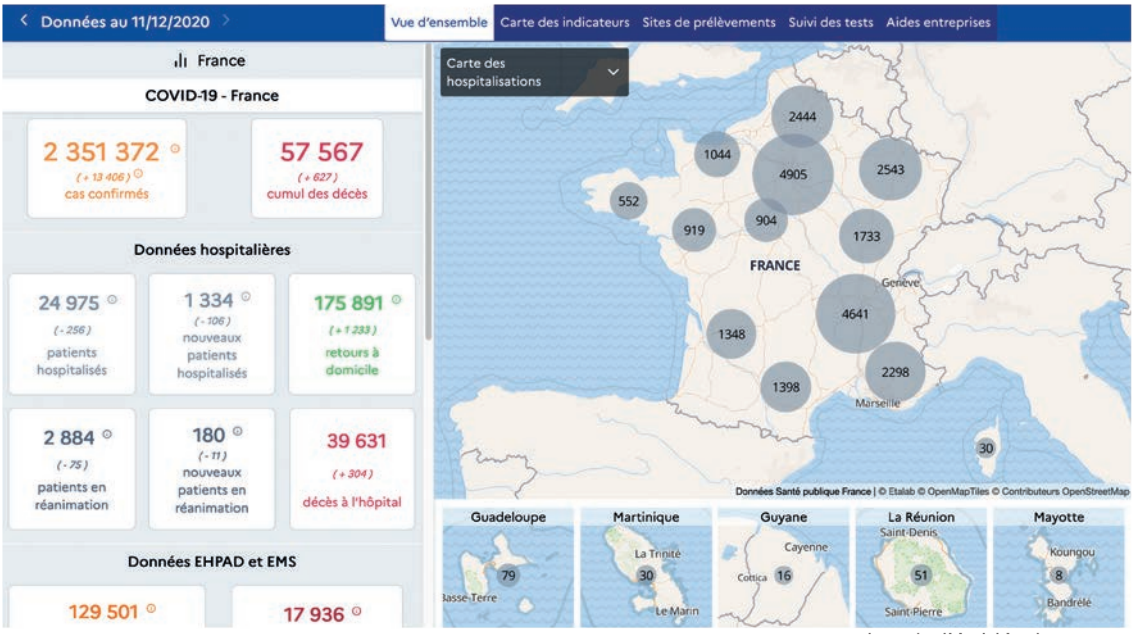
(1) https://publiccode.eu/fr/openletter/
(2) Déclaration des droits de l'homme et du citoyen, article 15 « La société a le droit de demander compte à tout agent public de son administration », https://www.conseil-constitutionnel.fr/le-bloc-de-constitutionnalite/declaration-des-droits-de-l-homme-et-du-citoyen-de-1789
(3) Loi n°2016-1321 du 7 octobre 2016 pour une République numérique, https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000031589829/
(4) Loi n°78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public, et diverses dispositions d'ordre administratif, social et fiscal, https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000339241/2020-12-12/
(5) COLIN N. & VERDIER H. (2015), *L'âge de la multitude. Entreprendre et gouverner après la révolution numérique*, Armand Colin.

et organisationnelle. Cette puissance ouvre de nouveaux champs de réflexion sur les modèles et imaginaires de l'action publique.

La suite de cet article propose d'illustrer l'approche « par communautés » dans plusieurs projets et dispositifs « publics et ouverts » en lien avec le numérique, et d'y apporter des éclairages prospectifs.

La crise Covid-19, révélatrice de l'engagement des communautés *open data* et *open source* pour l'action publique

Lors des premières semaines de la crise sanitaire liée à l'épidémie de Covid-19, les sources officielles d'informations pour suivre l'évolution du nombre de personnes décédées ou hospitalisées étaient difficilement accessibles et visualisables par le grand public. Des premières consolidations de données ont été réalisées *via* l'initiative **OpenCovid19**, portée par des acteurs de la société civile. Cette brique initiale a été reprise par Etalab [6], en coordination avec le Service d'information du gouvernement (SIG) et Santé publique France, pour construire un tableau de bord officiel, permettant de visualiser l'ensemble des données de l'épidémie de Covid-19 [7].



Capture d'écran du 11 décembre 2020 des données officielles sur la progression de l'épidémie en France de la plateforme des données publiques www.data.gouv.fr : https://dashboard.covid19.data.gouv.fr/

Dans les territoires, de nombreuses communautés de "*makers*" se sont engagées pour fabriquer du matériel à destination des personnes en première ligne (respirateurs *open source*, visières imprimées en 3D, etc.) [8].

(6) Département de la direction interministérielle du numérique (DINUM), Etalab coordonne la conception et la mise en œuvre de la stratégie de l'État dans le domaine de la donnée : https://www.etalab.gouv.fr/
(7) Voir le billet de *blog* du département Etalab « Comment les administrations ont collaboré à l'ouverture des données du coronavirus : le cas français », juin 2020 : https://www.etalab.gouv.fr/comment-les-administrations-ont-collabore-a-louverture-des-donnees-du-coronavirus-le-cas-francais
(8) Une plateforme recense des initiatives de "*makers*" pendant la crise Covid-19 : https://covid-initiatives.org/

Ces dynamiques récentes illustrent le caractère structurant de la contribution de la société civile aux stratégies numériques publiques. Ce rôle peut d'ailleurs être institutionnalisé, comme le **projet BAN** (base adresse nationale) [9], qui a fait l'objet d'un partenariat entre La Poste, l'Institut national de l'information géographique et forestière (IGN), l'État (et notamment la direction générale des finances publiques) et l'association OpenStreetMap France, pour constituer et maintenir un référentiel commun autour des données des adresses. Sans être toujours formalisés, des collectifs partagent des connaissances, échangent des techniques et des offres d'emploi sur les sujets de l'*open data*. La communauté **#teamopendata** réunit des agents publics en charge de l'ouverture des données, des prestataires, militants, chercheurs et citoyens. La communauté « **Blue Hats – hackers d'intérêt général** » encourage l'usage et la contribution au logiciel libre dans l'administration.

Entrepreneurs d'intérêt général : créer et animer une communauté d'innovateurs publics et d'innovateurs numériques

« Faire entrer les entrepreneurs d'intérêt général pour améliorer les rapports entre les citoyens et les responsables publics […] et apporter un service supplémentaire. » Tel a été le défi lancé par le président de la République François Hollande lors d'un échange avec la société civile en préparation du 4e sommet mondial du Partenariat pour un gouvernement ouvert, organisé à Paris en 2016 [10]. **Depuis l'année 2017, des « promotions » d'entrepreneurs d'intérêt général (EIG) rejoignent des administrations publiques afin de relever, avec des agents publics désireux d'innover, des défis, des projets en matière de transformation numérique**.

Capture d'écran du 11 décembre 2020 des données officielles sur la progression de l'épidémie en France de la plateforme des données publiques www.data.gouv.fr : https://dashboard.covid19.data.gouv.fr/

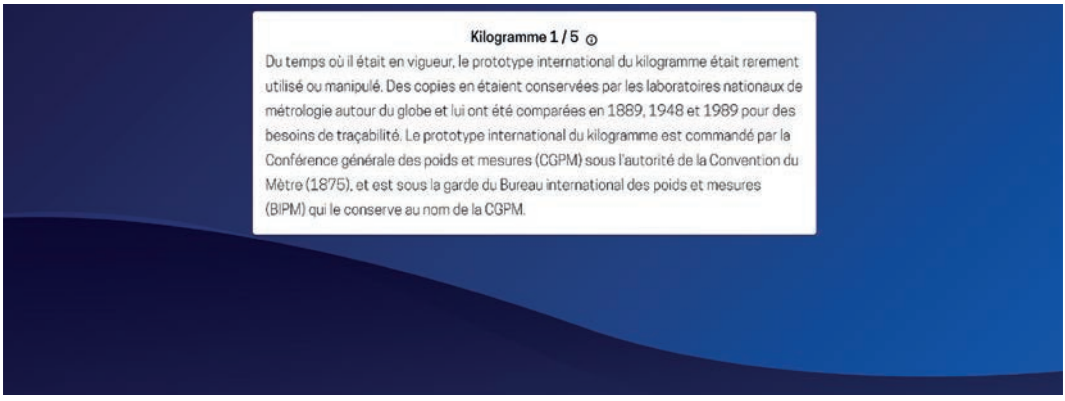
Ce programme original de « recrutement » permet d'introduire et de pérenniser, dans l'administration, davantage de compétences en développement informatique, sciences des données et *design*, des métiers en tension dans le secteur privé et difficiles à attirer dans le secteur public. **Pour assurer le bon déroulement des projets**, et garantir des collaborations utiles entre les agents publics et les EIG, **une équipe de coordination du programme, hébergée au sein d'Etalab, accompagne cette communauté**, en faisant appel à des méthodes d'animation, de

(9) https://www.etalab.gouv.fr/acteurs-publics-et-societe-civile-sassocient-pour-la-constitution-dune-base-adresse-nationale-ban-collaborative
(10) https://www.dailymotion.com/video/x4fdfed

partage de connaissances, et documente de manière ouverte les projets [11] et le programme [12]. Cette approche peut être rattachée au concept d'innovation ouverte à plusieurs égards : l'ensemble des développements réalisés par les équipes d'EIG est en *open source*, si bien que les briques technologiques sont réutilisables pour d'autres projets numériques ouverts ; le fait de recruter des compétences extérieures à l'administration témoigne de son ouverture ; et, enfin, la communauté des EIG s'est réunie au sein d'une association, « Léon » (les entrepreneurs ouverts du numérique), qui, au fil des promotions, partage des expériences et des conseils, et poursuit des collaborations avec les administrations [13].

Les nouvelles frontières de la contribution ouverte pour l'intelligence artificielle : le projet PIAF « pour des intelligences artificielles francophones »

Lancé en juin 2019, le projet PIAF vise à construire et à mettre à disposition des données d'entraînement de questions-réponses en français, afin d'améliorer la performance d'agents conversationnels et de moteurs de recherche qui utilisent des technologies d'intelligence artificielle. **Dès la fondation du projet, l'approche communautaire a été intégrée : pour construire ce jeu de données d'entraînement**, il est nécessaire d'annoter des textes (dans le cas de PIAF, des extraits d'articles de Wikipédia) ; **cette annotation doit être réalisée par des personnes humaine**s. Rapidement, des questions éthiques se sont posées. Dans quelle mesure l'annotation volontaire n'est-elle pas du travail gratuit ? Quelles sont les sources de « motivation » des contributeurs pour participer à construire un jeu de données dont on ne peut connaître tous ses usages ? En guise de comparaison, dans le cadre d'un chantier participatif, ma motivation à y contribuer ne sera pas la même si le chantier est destiné à construire un centre pour accueillir des personnes vulnérables ou s'il s'agit d'y abriter une prison. Dans le cadre du projet PIAF, même si les usages n'étaient pas encore déterminés au démarrage, l'amélioration de la lisibilité du droit était particulièrement motrice [14].



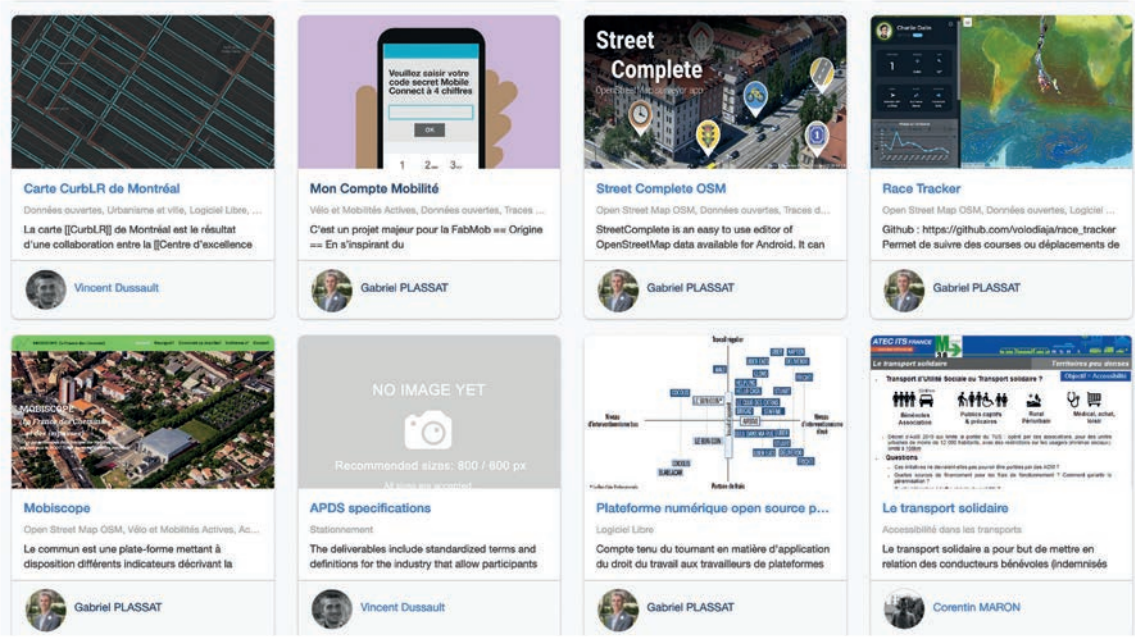
Aperçu de l'interface d'annotation de PIAF : https://app.piaf.etalab.studio

(11) Dépôt des codes sources de projets EIG : https://github.com/entrepreneur-interet-general/
(12) Voir le site de documentation du programme : https://doc.eig-forever.org/, donnant aussi à voir les outils d'animation de la communauté (outil de rétrospective hebdomadaire par exemple).
(13) Voir le site du programme : https://entrepreneur-interet-general.etalab.gouv.fr/. Plusieurs billets de blog mettent en lumière comment des projets ont aussi fait participer des communautés et associations numériques, comme Wikimédia France : https://entrepreneur-interet-general.etalab.gouv.fr/blog/2018/10/12/retour-sur-atelier-wikipedia-au-mobilier-national.html
(14) En témoigne le projet d'application PIAFAgent, destinée à faciliter la recherche d'information des agents publics sollicités par les citoyennes et les citoyens : https://piaf.etalab.studio/application-piaf/

Pour remédier à ces limites, **les porteurs du projet ont fait le choix d'une approche pédagogique et transparente**. **Les moments d'annotation** des articles Wikipédia **sont devenus des temps d'acquisition de connaissances sur les enjeux liés au traitement automatique du langage**. **La transparence s'est incarnée par la publication d'une charte**, exposant aux contributeurs le sens du projet : en y contribuant, on « s'engage » en quelque sorte à améliorer la présence de *corpus* francophones dans le domaine de l'IA et à mettre ces données à disposition du plus grand nombre [15]. Ces deux actions ont d'ailleurs permis d'ouvrir le projet à des publics plus techniques : le projet PIAF a été présenté à des étudiants et à des équipes de recherche en intelligence artificielle pour aborder ces enjeux éthiques.

De l'assemblage de communautés à la mise en « communs » : la Fabrique des Mobilités

À l'initiative de la Fabrique des Mobilités se trouvent plusieurs acteurs publics et privés, notamment l'agence de la transition écologique (ADEME), **qui entrevoient l'opportunité de se réunir pour inventer les mobilités de demain et pour partager les ressources** – expertises, données, codes sources, méthodes – **qui permettent de les construire**. La création d'une structure associative en 2018 a permis cette « mise en "communs" », puisque des ressources sont « mises en partage au sein d'une communauté d'acteurs qui définit ses règles de gouvernance pour les gérer ». Le rôle de la Fabrique des Mobilités est d'animer des communautés et d'outiller au mieux les communs produits. Les personnes qui adhèrent et participent à l'association peuvent créer ou rejoindre une « communauté d'intérêt » sur une thématique (covoiturage, véhicule électrique, véhicule *open source*, etc.), impulser des projets, participer au développement de communs.



Aperçu de plusieurs communs de la Fabrique des Mobilités : https://wiki.lafabriquedesmobilites.fr/wiki/Communs

(15) Les enseignements de l'approche contributive du projet PIAF sont détaillés dans l'article de *blog* suivant : https://piaf.etalab.studio/enseignements-contributions/. Ce projet a fait l'objet d'une publication scientifique à l'occasion de la conférence LREC en 2020 : https://www.aclweb.org/anthology/2020.lrec-1.673/

L'effet démultiplicateur est bien présent : plusieurs projets numériques publics, comme le « registre de preuve de covoiturage [16] » ou « mon compte mobilité [17] », sont accueillis comme des communs de la Fabrique des Mobilités, impliquant non seulement que des garanties sont apportées pour maintenir ces projets, mais signifiant aussi que les briques technologiques et d'apprentissages tirés de ces projets, développés sur un territoire donné, peuvent être utiles à d'autres, y compris à l'étranger.

Derrière ce modèle en construction, on entrevoit l'opportunité de transformer certaines logiques partenariales entre l'État et des acteurs privés, notamment dans le domaine du numérique : **une association peut devenir le tiers de confiance** dans la définition des standards de partage de données publiques ou d'intérêt général, **dans la construction des infrastructures publiques numériques, dans l'imagination des communs numériques d'intérêt général.**

Confiance numérique, capacités publiques ?

Ouvrir et activer les capacités publiques. Ces dispositifs illustrent l'impact de l'ouverture de l'action publique et la contribution de communautés à celle-ci. Coproduire des ressources avec l'aide de communautés numériques permet de répondre à des situations de crise. Ouvrir le secteur public à des compétences en numérique augmente ses capacités à se transformer. Faire connaître les potentiels de l'intelligence artificielle apporte de nouvelles perspectives sur son usage éthique. Créer des instances associatives en vue d'inventer une nouvelle politique publique réinvente le modèle partenarial de l'action publique.

(16) https://wiki.lafabriquedesmobilites.fr/wiki/Preuve_de_covoiturage
(17) https://wiki.lafabriquedesmobilites.fr/wiki/Mon_Compte_Mobilit%C3%A9

Perspective historique sur la liberté d'expression

Par **Maryse ARTIGUELONG**
vice-présidente de la Ligue des Droits de l'Homme et vice-présidente de la Fédération Internationale des Droits de l'Homme
Et **Henri LECLERC**
président d'honneur de la Ligue des Droits de l'Homme

Dans le préambule de la Déclaration universelle des droits de l'homme, en 1948, les nations réunies après la fin de la deuxième guerre mondiale proclament que « la plus haute aspiration de l'homme » est « l'avènement d'un monde où les êtres humains seront libres de parler et de croire, libérés de la terreur et de la misère ». Ainsi, le premier droit fondamental qui englobe et dépasse la liberté de la presse est bien la liberté d'expression. C'est aussi la signification de l'article 11 de la Déclaration des droits de l'homme et du citoyen (1789), dont le texte admirablement concis définit à la fois le contenu et les frontières de cette liberté : « La libre communication des pensées et des opinions est un des droits les plus précieux de l'Homme : tout Citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la Loi. » Seule de toutes les libertés énoncées par le texte, elle est affirmée comme étant une des plus précieuses. Après les débats enflammés des Lumières sur le sujet, elle vise toutes les formes d'expression alors connues, la parole, l'écriture et l'imprimerie, et prend pour l'avenir une portée générale concernant tous les modes d'expression et de communication qui pourraient se révéler. Le débat avait été rude ce 24 août 1789, et deux tendances extrêmes et minoritaires se manifestaient : les conservateurs qui souhaitaient que soient reconnus, proclamés et protégés les droits de la religion de l'Église et du roi, et de l'autre côté ceux qui, tel Robespierre, aspiraient à ce que la liberté soit infinie et sans limites. Marat disait d'ailleurs « La liberté de tout dire n'a d'ennemis que ceux qui veulent se réserver la liberté de tout faire. Quand il est permis de tout dire, la vérité parle d'elle-même et son triomphe est assuré. » C'est une lumineuse formule de Mirabeau qui a permis à la fois d'écarter la censure, qui avait été au XVIII^{e} siècle un tourment incessant, par le mot « répondre » censé écarter toute censure préalable, et de donner un espace et des frontières à la liberté en prévoyant la possibilité d'en définir les abus, mais en réservant cette possibilité à la loi.

C'est évidemment surtout au travers du développement considérable de la presse de masse au XIX^{e} siècle que va se poser la question de l'exercice de cette liberté. Napoléon l'avait totalement supprimée, puis peu à peu cette liberté émergera à nouveau jusqu'à ce que Charles X tombe pour avoir voulu rétablir la censure. Et à peine la II^{e} République a-t-elle été proclamée, établissant une liberté d'expression presque totale, que le parti de l'Ordre arrivé au pouvoir la restreindra considérablement avant même le coup d'État du 2 décembre 1851, posant un problème nouveau en imposant des contraintes financières insupportables à la presse, un secteur non lié à la richesse et aux forces économiques montantes. Lamennais doit fermer son journal socialisant en concluant ainsi « Silence au pauvre [(1)] ! »

Il faudra attendre la III^{e} République pour que, à l'issue d'un débat parlementaire d'une très grande richesse où s'illustre le jeune Clemenceau, une loi précise les abus dont les journaux auront à

(1) https://aimable-faubourien.blogspot.com/2010/08/silence-au-pauvre-lamennais-1848.html

répondre, et dégage ainsi l'espace de la liberté. C'est la loi du 29 juillet 1881 sur la liberté de la presse [2], mais qui vise en réalité tous les moyens de communication, au moins dans ses principes généraux. Ce sont les publicateurs gérants des journaux, ou maisons d'édition faciles à identifier qui sont responsables au premier chef, y compris pénalement. Certes des lois comme les fameuses « loi scélérates » de 1894 [3], prises sous prétexte de réprimer les anarchistes, vont restreindre l'expression du mouvement social, mais dans l'ensemble le système a tenu. Ce qui a menacé la liberté de la presse est évidemment le coût économique de sa production, que tentèrent de mieux contrôler, dans le sillage du programme du Conseil national de la Résistance, des ordonnances en 1944.

Des améliorations comme les lois Pleven de 1972 réprimant les actes de discrimination, de haine ou de racisme ont étendu le champ des droits protégés, mais voilà que certains trouvant trop protectrices les restrictions procédurales, et notamment la courte prescription, veulent exclure certains abus réprimés par la loi de ce cadre trop favorable selon eux. C'est ainsi que, d'un côté, les apologies du terrorisme et, de l'autre, les propos racistes devraient être chassés du droit à la liberté d'expression pour subir le sort des procédures de droit commun. Et lorsque commence à craquer le tissu serré de la loi, d'autres veulent s'insinuer dans la brèche, et déjà des demandes sont faites de sortir de l'espace précis de la liberté d'expression provocations ou injures contre les policiers, ou propos harcelants ou outrageants contre les femmes ou les homosexuels. Il y a là une incontestable dérive. Les abus de la liberté d'expression peuvent être sévèrement sanctionnés si le législateur le décide, mais exclure des expressions, même insupportables, du champ de l'expression pour en faire des actes de droit commun représente un danger. Sortir des frontières de ce droit, de cette liberté, c'est en brouiller l'espace.

La réglementation juridique de l'expression dans l'audiovisuel a posé de nouveaux problèmes. Faut-il se souvenir de l'émergence dans les années 1970 des radios libres et du débat sur la persistance du monopole d'État sur la radio et la télévision, si manifeste au cours de la crise de mai 1968. François Mitterrand qui s'était engagé personnellement dans ce combat y mit fin. La loi du 30 septembre 1986 confirmera et développera le principe de la liberté de la communication audiovisuelle telle qu'elle avait été instaurée, avec la suppression du monopole d'État sur la radio et la télévision par les lois de novembre 1981, mai 1983 et ensuite du 29 juillet 1987. Mais l'effervescence de l'« expression libre », à laquelle on avait assisté au temps où il s'agissait de véritables actes de résistance, a été émoussée par la mainmise de l'argent, des puissances économiques et par les incertitudes des organismes de contrôle successivement mis en place par l'État dans les années qui ont suivi.

Une grande évolution sur le plan des principes a été apportée par l'article 10 de la Convention européenne des droits de l'homme, qui exprime plus exhaustivement ce que dit la Déclaration de 1789, et impose aux États du Conseil de l'Europe une conception large et concrète. Les arrêts de la Cour européenne de Strasbourg, de plus en plus souvent, imposent leurs conceptions et orientations en général libérales et limpides aux juridictions françaises, et on peut citer une formule mythique sans cesse reprise et qui éclaire bien cette conception de la liberté : « La liberté d'expression constitue l'un des fondements essentiels d'une société démocratique, l'une des conditions primordiales de son progrès et de l'épanouissement de chacun. Sous réserve des restrictions mentionnées, notamment dans l'article 10 de la Convention européenne des droits de l'homme, elle vaut non seulement pour les informations ou les idées accueillies avec faveur, ou considérées comme inoffensives ou indifférentes, mais aussi pour celles qui heurtent, choquent ou inquiètent l'État ou une fraction quelconque de la population. Ainsi le veulent le pluralisme, la tolérance et l'esprit d'ouverture sans

(2) https://www.legifrance.gouv.fr/loda/id/LEGITEXT000006070722/2020-12-14/
(3) https://fr.wikipedia.org/wiki/Lois_de_1893_et_1894_sur_l'anarchisme

lesquels il n'y a pas de société démocratique. » On ne saurait guère dire mieux le sens et l'espace de la liberté d'expression, cette colonne qui soutient la démocratie.

La révolution numérique, soutien à la démocratie ?

Diffuser, confronter des idées, débattre permet d'élargir son horizon, de faire évoluer les opinions et les théories, et devrait favoriser la démocratie. Il est indéniable que depuis l'arrivée de l'Internet, du *web* 2.0 et des réseaux sociaux les moyens pour s'informer et s'exprimer sont devenus instantanément accessibles au plus grand nombre. Ce que l'on nomme « révolution numérique » a pu être comparée à l'invention de l'imprimerie. En effet, les outils numériques favorisent la production, la diffusion des savoirs, l'accès à l'information et la possibilité pour quiconque d'exprimer ses idées, et de les diffuser, plus ou moins largement selon sa maîtrise des technologies.

Cette ouverture de nouveaux espaces de liberté implique des droits nouveaux. Si l'accès à l'Internet a été reconnu par le Conseil des droits de l'homme de l'ONU comme un droit fondamental, la gratuité de la plupart des contenus et des services (hormis l'accès au réseau) a généré des modèles économiques basés sur la collecte massive et l'exploitation commerciale des données à caractère personnel, grâce aux capacités de stockage, aux algorithmes et à l'intelligence artificielle toujours plus performants.

Ces modèles qui lient les revenus *marketing* à la quantité de données collectées et transformées en profils à vendre, et les revenus publicitaires liés au trafic et au temps passé sur les sites ou les plateformes, ont obligé les institutions à repenser la protection de droits fondamentaux comme la garantie de la liberté d'expression ou la protection de la vie privée (ainsi que le soulignait le Conseil d'État [4] dans son étude annuelle en 2014). C'est une condition pour préserver la confiance des citoyens envers les entreprises du numérique et favoriser les échanges commerciaux. Aux garanties historiques (voir ci-dessus), la Convention 108 du Conseil de l'Europe [5] et le RGPD [6] de l'Union européenne sont venus adapter ces droits, tout comme le projet de résolution de l'ONU sur le droit à la vie privée [7] devrait les renforcer.

Mais garantir des droits ne suffit pourtant pas à faire du numérique un espace sûr pour la liberté d'expression. En effet, les dangers inhérents sont à l'échelle de la puissance de ses outils. Ils sont principalement de deux natures : la surveillance subie par les internautes et la « malveillance » qui peut s'y dérouler sous couvert d'un anonymat relatif.

La surveillance

Celle-ci a très tôt été décelée, étudiée et dénoncée par les défenseurs des libertés. Elle se traduit au mieux par une forme qui peut sembler anodine comme le profilage, la publicité ciblée dont les entreprises du numérique (notamment les GAFAM [8]) abusent pour rémunérer les services gratuits qu'elles fournissent, au pire par des formes de manipulation et par la surveillance par les services de renseignement de la plupart des États qu'Edward Snowden a révélée en 2013 [9]. Ces révélations ont brutalement fait prendre conscience de l'étendue des données collectées auprès des entreprises du numérique et remis en cause la confidentialité des données, ce qui a menacé

(4) Conseil d'État, « Étude annuelle 2014 - Le numérique et les droits fondamentaux », https://www.conseil-etat.fr/ressources/etudes-publications/rapports-etudes/etudes-annuelles/etude-annuelle-2014-le-numerique-et-les-droits-fondamentaux

(5) https://edoc.coe.int/fr/internet/7734-convention-108-convention-pour-la-protection-des-personnes-a-legard-du-traitement-des-donnees-a-caractere-personnel.html

(6) Règlement général sur la protection des données, 2016 : https://www.cnil.fr/fr/reglement-europeen-protection-donnees

(7) Le droit à la vie privée à l'ère du numérique : https://digitallibrary.un.org/record/3889702

(8) Google, Amazon, Facebook, Apple, Microsoft.

(9) https://fr.wikipedia.org/wiki/R%C3%A9v%C3%A9lations_d%27Edward_Snowden

durablement la confiance des internautes. En effet, se savoir surveillé conduit à ne plus se comporter naturellement mais tel que l'on imagine devoir le faire pour être dans la norme, ce qui constitue une entrave à la liberté d'expression. Ainsi, par exemple, la pénalisation de la consultation de sites relatifs au djihadisme (y compris à titre informatif) a entraîné une autocensure préjudiciable au droit à l'information, alors qu'il est garanti par le PIDCP [10].

Cette surveillance a bien sûr été amplifiée depuis le début de ce siècle en raison des attentats commis par des terroristes utilisant les outils numériques. Ces mesures de surveillance généralisée [11] par les gouvernements conduisent à s'interroger : « sommes-nous tous des suspects potentiels [12] ? » L'ONU et la Cour de justice de l'Union européenne pour leur part s'opposent à cette surveillance généralisée.

Cybercriminalité, haine en ligne, comment les traiter ?

Comme toutes les libertés, la liberté d'expression a des limites, mais les outils numériques, par leur facilité d'utilisation et la garantie, parfois illusoire, de l'anonymat, ont rapidement donné lieu à des excès : commentaires ou propos injurieux, incitation aux discriminations et à la haine, menaces... souvent désignés comme « discours haineux », cette dénomination n'ayant toutefois pas de qualification juridique. Ces propos sont pourtant constitutifs de délits, mais ils sont souvent amplifiés par l'instrumentalisation de leur dimension affective et par les méthodes des plateformes qui favorisent leur viralité par des algorithmes. La viralité des polémiques génère en effet un fort trafic à l'intérieur de ce qu'il est convenu de nommer des « bulles de filtres » : les utilisateurs des plateformes reçoivent des informations ou des propos censés refléter leurs opinions, mais en fait ils sont manipulés [13] pour projeter ces perceptions dans le monde « réel ». Ce sont ces phénomènes des discours de haine et des infox ou "*fake news*" qui pourraient devenir une menace grave pour nos démocraties.

Paradoxalement, c'est à ces entreprises [14] que l'on demande de lutter contre les « discours haineux » [15]. Cette lutte n'est pas satisfaisante, notamment parce que les mesures utilisées par les plateformes manquent de transparence et d'efficacité (suppression de contenus, de comptes sans avertissement) et paraissent souvent incompréhensibles, entre autres, parce que la sémantique des contenus en cause peut être complexe et perçue par une intelligence artificielle ou un modérateur ne connaissant pas toutes les subtilités de l'invective... Les plateformes n'autorisent pas toujours un recours contre leurs mesures d'intervention, et, enfin, elles ne prennent pas le problème à l'origine (ce qui n'est bien sûr pas leur rôle). Par ailleurs, leur coopération pour révéler l'identité de leur(s) client(s) lorsqu'une action judiciaire est entamée n'est pas toujours aisée.

Préserver la liberté d'expression nécessite un investissement dans l'éducation et la formation des citoyens, mais aussi de redonner sa place au juge, garant des libertés, pour lutter contre les « discours » qu'il aura pu qualifier de « haineux ».

(10) Pacte international relatif aux droits civils et politiques : Article 19 - § 1 protège le droit de ne pas être inquiété pour ses opinions - § 2 garantit le droit à la liberté d'expression, qui comprend la liberté de rechercher, de recevoir et de répandre des informations et des idées de toute espèce, sans considération de frontières, par quelque moyen que ce soit.
(11) Loi de programmation militaire, loi relative au renseignement...
(12) https://www.coe.int/fr/web/freedom-expression/freedom-of-expression-still-a-precondition-for-democracy-
(13) Voir l'exemple du scandale Cambridge Analytica : https://www.cnil.fr/fr/affaire-cambridge-analytica-facebook ou https://fr.wikipedia.org/wiki/Scandale_Facebook-Cambridge_Analytica
(14) Elles sont pour la plupart de droit états-unien, où la liberté d'expression n'a pratiquement pas de limites, et n'ont culturellement pas les mêmes pratiques de modération.
(15) Voir les dispositions que portait la proposition de loi dite « loi Avia » : https://www.cncdh.fr/fr/publications/avis-relatif-la-proposition-de-loi-visant-lutter-contre-la-haine-sur-internet

Inclusion numérique au cœur des politiques publiques

Par **Florence PRESSON**
Adjointe au maire de Sceaux (92) déléguée aux transitions et à l'économie circulaire et solidaire

La transition numérique

Née à la fin des années 1960, je fais partie de la génération qui a vécu une première transition numérique. J'ai exercé un métier qui n'existait pas pour la génération précédente. Un métier que ne pouvait pas m'avoir proposé la conseillère d'orientation au lycée.

Du Minitel aux premiers ordinateurs portables

J'ai commencé ma carrière en tant que conceptrice de services professionnels en télématique. Les clients de l'entreprise pour laquelle je travaillais étaient des cabinets de recrutement. Ces cabinets publiaient des offres d'emploi, les candidats remplissaient un formulaire, et, selon les critères recherchés, les candidats étaient appelés pour convenir d'un rendez-vous.

Le Minitel, le numérique pour tous

En 1980, alors qu'il y a moins de 5 % de foyers qui sont équipés d'ordinateurs, le gouvernement met à disposition de tous un Minitel, un outil qui permet de rechercher un numéro de téléphone, de lire le programme du cinéma (3615 Allociné), de répondre à des annonces…

La distribution gratuite des Minitels dans les foyers met tous les ménages à égalité, riches, pauvres, tous accèdent au même service. Son utilisation est simple, les services développés sont intuitifs, le premier pas vers Internet débute.

Le Minitel, un outil pour les entreprises

Les entreprises qui gèrent des flottes de commerciaux comprennent très vite que cet outil va leur permettre de réaliser des gains de temps et de performance très importants. En effet, avant le Minitel, les commerciaux rédigeaient des comptes rendus de leurs visites à la main, sur papier, les envoyaient aux assistantes, qui les triaient, les saisissaient, faisaient les synthèses… Le temps de faire tout cela, l'information n'était déjà plus à jour.

Les comptes rendus de visite saisis, chaque soir, par les commerciaux sur leur Minitel ont été les premiers pas vers la digitalisation des entreprises, un changement de rythme de travail et la fin de certaines fonctions dans les services.

L'arrivée des ordinateurs portables

Très vite, tout s'est accéléré. Je suis passée de conceptrice d'applications télématiques à la conception et au développement de programmes de saisie de comptes rendus de visite et de suivi d'activité des commerciaux. Le bénéfice pour les commerciaux était tel qu'ils n'hésitaient pas à transporter des ordinateurs portables qui pesaient plus de 5 kg.

Tout s'accélère

Cette accélération n'a pas cessé. Les ordinateurs ont perdu du poids, ils ont gagné de la performance et de l'espace. De plus en plus de nouveaux métiers ont vu le jour, des écoles ont commencé à se mettre en place. De nouvelles entreprises sont nées. La technologie s'est développée, des protocoles de communication sont apparus. Internet est ensuite arrivé et est vite devenu essentiel pour poursuivre la digitalisation des services des entreprises. Ces dernières n'hésitent pas à financer, en partie ou complètement, l'accès à Internet chez leurs salariés.

La révolution numérique

Toutes les entreprises ont vécu leur transition numérique, les services ont été digitalisés, les micro-ordinateurs ont colonisé les bureaux, la gestion et le traitement des données sont devenues stratégiques. Cette révolution s'est principalement cantonnée au domaine professionnel, dans un premier temps.

Au début des années 2000, de nouvelles opportunités de développement ont vu le jour avec Internet, la mobilité, le paiement en ligne, le multimédia, les données publiques…. Les outils numériques ont alors commencé à débarquer chez les citoyens.

La dématérialisation et les services à distance

Pour des raisons d'économie, de simplification des traitements, d'écologie (argument souvent évoqué, mais rarement efficient, car de nombreuses personnes éditent parfois le même document), les entreprises et administrations dématérialisent leurs documents. Ils ferment des accès au public (permanences, accueils…) en proposant un service en ligne. L'accès au service quels que soient l'heure et le jour est un véritable avantage, mais un inconvénient majeur pour ceux qui ne maîtrisent pas l'outil Internet.

La fracture numérique

Contrairement à l'époque du Minitel, qui était distribué gratuitement à toutes les familles, aujourd'hui, il est nécessaire de faire l'acquisition de son propre matériel : ordinateur ou tablette, raccordement (3G, 4G, 5G, fibre…) et abonnement. Ces choix sont difficiles à faire, et les citoyens n'ont pas spécialement d'aide pour se décider ; ils dépendent d'un vendeur qui a toutes les chances de privilégier le modèle pour lequel il a une bonne marge. Cela représente une première fracture, car certains publics n'ont pas accès à ces outils faute d'avoir le budget ou la connaissance pour réaliser un achat cohérent avec leur besoin. Il s'agit d'une première inégalité majeure.

Pour pallier ce manque, des collectivités locales mettent en place dans les mairies, les bibliothèques (souvent devenues des médiathèques), les écoles ou des espaces particuliers, des ordinateurs en libre-service.

La fracture d'usage

La véritable fracture numérique est la fracture d'usage. Les familles peuvent disposer d'un ordinateur, peuvent savoir jouer, télécharger des photos, l'utiliser pour se connecter avec leurs familles à distance…, mais ne pas savoir l'utiliser « réellement ».

Les raisons sont multiples : les générations d'avant les années 1970-1980 ne sont pas « nées » avec le numérique ; parfois, ces générations n'ont pas la compréhension ou l'agilité nécessaires à l'usage de certains programmes, algorithmes et applications. La barrière de la langue est aussi une réalité. De nombreux jeunes semblent maîtriser ces outils, tant ils sont habiles sur les réseaux sociaux et jeux divers… mais ils n'ont pas forcément la compréhension des traitements ou saisies attendus. Est-ce en raison de l'âge des concepteurs de ces applications ? Ils ne sont pas de la même

génération, ils poursuivent des démarches ou méthodes peut-être moins adaptées ? Il n'y a pas encore assez de femmes dans les postes de conception ou de développement d'application, c'est la complémentarité qui permet d'avoir des applications plus fluides.

Par ailleurs, ces applications sont souvent une transposition de services existants, et non le fruit d'une véritable réflexion méthodologique et portée sur la transition.

L'inclusion numérique

Quel que soit l'âge, quel que soit l'accès au matériel, nous ne pouvons nier que le numérique risque d'accélérer la fracture sociale dans tous les sens du terme. Une fracture au sein des classes sociales, une fracture dans le monde professionnel et l'accès à l'emploi, une fracture du lien entre les personnes. Imaginez un confinement pour une personne seule, qui n'a ni outils numériques ni d'accès à Internet !

L'éducation au numérique

L'école est le lieu où l'enfant, dès le plus jeune âge, doit pouvoir apprendre les usages du numérique. Ces usages sont complémentaires de ceux qu'il découvre avec ses parents (le jeu, l'appel en visio avec les grands parents, les photos, etc.).

Apprendre, c'est se familiariser avec les outils (recherche de contenu, site de références, volet commercial…) et développer un « *e*-esprit » critique. Ce n'est pas parce qu'un site propose la définition du « dérèglement climatique » qu'il s'agit de la vérité. L'enfant doit apprendre à réaliser des recherches multiples sur différents supports, confronter des définitions et avis, vérifier ses sources… et, petit à petit, s'approprier le sujet et développer son propre point de vue.

La politique municipale joue un rôle dans les écoles en mettant à disposition du matériel, mais ce matériel est le support d'un véritable apprentissage qui doit être réalisé par les enseignants. Se pose alors la question de leur propre formation ! Quand l'Éducation nationale propose des ateliers à distance, 20 heures par an, en partie sur le temps « libre » de l'enseignant, je ne pense pas que nous mettions en œuvre les clés de la réussite pour les enfants.

L'appropriation du numérique

Comme la dématérialisation des services à la population se développe très rapidement, un apprentissage est nécessaire pour les adultes, quel que soit leur âge et y compris ceux qui utilisent les outils numériques professionnellement. En effet, cet usage désigne souvent l'utilisation de fonctions générales basiques (traitement de texte, de tableaux et feuilles de calculs simples) et d'applications spécifiques à leur activité (CRM, GRC, etc.).

La connaissance de l'usage des réseaux sociaux et de la propriété des données ne s'apprend pas dans un cadre « public ». Il s'agit souvent d'un accompagnement par des opérateurs qui ont des avantages commerciaux à en tirer. La confiance entre pairs permet de réajuster la situation ainsi que le développement des solutions « d'avis » et de recommandations. Mais ce n'est pas suffisant. La simple phrase « quand c'est gratuit, c'est vous le produit » doit rester dans toutes les mémoires et à la base de tout usage.

Le constat et l'accompagnement « public »

2014 a été une année marquant le mandat de transition vers le numérique. C'est la première fois que des adjoints ou conseillers municipaux ont eu des délégations « numérique » ou « innovation » et où la notion de "*smart city*" est apparue assez largement.

Ces élus ont permis de mettre en œuvre la politique numérique des maires et de s'attaquer aux ruptures numériques dans les communes. De nombreuses actions et des réseaux d'élus ont vu le jour.

Information et sensibilisation

L'organisation de conférences et d'ateliers de découverte se sont développés. Des ateliers intergénérationnels ont été mis au point : la rencontre entre les séniors et les jeunes pour permettre la familiarisation aux nouveaux téléphones contribue aussi à solutionner la fracture entre générations et, parfois, de faire tomber les craintes de la part de ce public.

Accompagnement

La mise à disposition de matériels a été accompagnée par des agents communaux pour porter assistance à l'usage. Des « maisons de services au public » ont été lancées dans de nombreux quartiers dits « prioritaires ».

De la "smart city" à "l'Human SmartCity"

Après avoir prôné l'installation de capteurs, la collecte de données et l'usage d'applications censées répondre à tout, la commune a opté pour une approche plus « humaine ». D'autres types d'outils ont été développés, favorisant les interactions entre les élus, l'administration et les citoyens. Des applications permettant de donner son avis, de participer, dans une logique de co-construction, sont apparues dans de nombreuses communes. Ces outils ne se limitant pas uniquement à la relation élus/citoyens, mais ciblant aussi les relations citoyens/commerçants, citoyens/associations… facilitent le rapprochement de l'ensemble des parties prenantes qui font la vie d'une commune.

De nouveaux acteurs

Toutes les communes ne disposent pas des moyens à la fois financiers et en personnel pour résorber les fractures numériques. De nombreuses associations ont été créées ou ont complété leur offre de service par des actions d'inclusion numérique pour leur public. Des associations d'accompagnement de femmes en difficulté ont ajouté un volet numérique, tout comme celles qui luttent contre la précarité des familles ou bien pour l'accompagnement à l'intégration des sans domicile fixe ou réfugiés…

Pour ces différentes parties, les moyens humains, grâce aux bénévoles, sont présents, mais des moyens financiers complémentaires sont parfois nécessaires.

Les appels à projets et la participation des acteurs privés

Des entreprises développent le mécénat de compétences, parfois appelé le « prêt de main-d'œuvre », auprès de structures associatives. Ils proposent à des salariés d'apporter leurs connaissances et expériences afin d'accompagner des publics en difficulté ou de faciliter la mise en place de nouvelles stratégies pour ces associations.

Des fondations privées lancent régulièrement des appels à projets qui sont proposés aux associations, leur permettant de bénéficier de budgets complémentaires.

Les fondations « publiques »

J'appelle « fondation publique » une fondation gérée par des acteurs publics qui sont focalisés sur des valeurs de solidarité et de bien commun, et dont le financement est éthique.

La Fondation Afnic soutient les projets structurants locaux, qui ont pour but d'utiliser Internet à des fins de solidarité sociale et économique en diffusant des usages et connaissances. Sa mission est de développer la solidarité, de soutenir les mutations sociétales et de renforcer la cohésion sociale sur le territoire français.

Cette fondation, associée à la Fondation de France, a soutenu, depuis 2015, 244 projets pour un montant global de près de 5 millions d'euros.

Conclusion

La transition numérique est un axe majeur en France et dans le monde. Elle nécessite l'inclusion de tous : citoyens de tous les âges, entreprises et associations de toutes les tailles. Les élus locaux sont des tiers de confiance pour les citoyens. Ils ont une connaissance fine de leur territoire et, grâce à la relation privilégiée qu'ils ont avec les citoyens, ils jouent un rôle de facilitateurs et d'accélérateurs de cette transition. La réussite de cette transition numérique, tout comme l'appropriation des outils et des usages, est une source d'inspiration afin de mener les transitions en cours et ultérieures : transitions économique, environnementale, énergétique et sociale. La réussite de ces transitions est indispensable pour les années à venir et l'héritage que nous laisserons aux générations actuelles et futures.

Hors dossier
Art.Machines.Intelligence (1)

Par **Frederic Fol LEYMARIE**
Professeur au Goldsmith College de l'Université de Londres

Le sujet principal de cet article est de faire le sommaire de mes réflexions sur les potentiels qui se trouvent à l'intersection de l'art, des machines (y compris l'IA) et de l'intelligence. En plus de donner un aperçu de projets d'artistes utilisant des machines dans le cadre de leur travail artistique, je vais discuter des raisons pour lesquelles il y a un grand potentiel dans la fusion de ces disciplines.

Pour ce faire, je vais d'abord caractériser chacun des trois thèmes. Mes descriptions de ceux-ci seront sans doute biaisées, loin d'être complètes, mais suffisantes, je l'espère pour préciser comment leur fusion peut opérer. Je donnerai par la suite quelques exemples récents de projets d'artistes, avec lesquels j'ai collaboré, où ces trois disciplines sont réunies, dans le cadre d'un petit tour d'horizon.

Mais commençons tout d'abord par un des sujets se trouvant au coeur de notre discussion : l'intelligence artificielle (IA). Le dictionnaire de Cambridge lui donne comme definition : « L'étude de la façon de produire des machines qui possèdent certaines des capacités propres à l'humain, telles que la compréhension du langage, la reconnaissance des images, la résolution de problèmes et apprendre », par exemple, à jouer d'un instrument de musique.

(1) Graffiti du *tag* A.M.I. (Art.Machine.Intelligence) se situant à l'intersection des styles "*arrow*" et « machine », selon la nomenclature de l'artiste et théoricien Dado (Ferri, 2016) ; produit par Daniel Berio et le système AutoGraff (Berio, 2020).

Par ailleurs, je ne fais pas de distinction *a priori* entre l'« esprit » et le « corps » comme cela sera plus clair par la suite [2]. Comme je veux aborder le sujet même de ce qu'est l'intelligence, je veux me concentrer sur les qualités ou capacités que l'humain possède, mais que, à notre connaissance, aucune autre espèce ne partage, ou du moins pas à une telle hauteur ; il s'agit notamment du langage, des arts, de l'écriture, de la création et de l'utilisation d'outils, des sciences et de l'invention des mathématiques, et, sur le long terme, de l'accumulation de connaissances et de l'augmentation continuelle de notre horizon cognitif (Levin, 2019). Dans mon discours, je me concentrerai sur les arts, mais je considérerai aussi ces autres capacités, car toutes ne sont pas entièrement distinctes les unes des autres.

Les arts doivent être envisagés au sens large, à savoir (au moins) les arts dits « visuels » (dessin, calligraphie, peinture, sculpture, animation, cinéma et leurs extensions comme les jeux informatiques), la musique, le chant et la sonification, l'architecture (aussi paysagère), la littérature sous toutes ses formes, et les divers métiers dits « d'artisanat » tels la potterie, la menuiserie, l'horlogerie. Dans les exemples que je vais fournir, je vais me concentrer sur les arts dits « visuels ». Il s'agit en grande partie d'un biais personnel provenant de mes expériences et de mes propres intérêts de recherche axés dans ce domaine (en graphisme, vision, perception, créativité).

En outre, je me pencherai sur la production d'œuvres d'art ou d'artefacts, ainsi que sur leur évaluation, leur appréciation et le fait qu'ils sont porteurs d'informations. Je n'insisterai pas (trop) sur les aspects plus culturels (historiques, variations entre les cultures et les époques), ni sur les impacts économiques ou sociaux. Je laisse cela pour une discussion séparée (et plus approfondie).

Art

L'art (visuel) est d'après l'Encyclopedia Britannica : « Un objet visuel ou une expérience créée consciemment par l'expression d'une compétence ou d'une imagination » qui existe « dans un *continuum* qui va de fins purement esthétiques à une extrémité à des fins purement utilitaires à l'autre ».

Voici ci-dessous les sujets associés aux arts que je propose de considérer comme pertinents à notre discussion.

Production

La production désigne les actions prises par l'artiste qui impliquent l'utilisation du corps (de manière experte), mais aussi souvent l'utilisation de certaines extensions au corps : c'est-à-dire l'aide d'outils (tels que brosses, pinceaux, crayons) ; les techniques utilisées (souvent développées au cours d'une longue histoire, qui évoluent, s'oublient, resurgissent) ; l'observation et la rétroaction qui interviennent dans le processus créatif, comme l'évaluation visuelle de l'artefact actuel, l'influence des marques peintes sur les décisions prises, par exemple dans l'exécution d'un dessin ou d'une peinture (Arnheim, 1974).

Réflexion

La réflexion indique : la perception nécessaire à la création et à l'observation d'artefacts ; l'appréciation impliquant des décisions et des comparaisons en cours ; la planification des actions, des mouvements, l'utilisation des outils, l'utilisation des matériaux ; le bagage historique influençant le style propre d'un artiste et ses explorations d'idées nouvelles, largement acquises pendant la scolarité, l'éducation et/ou comme élève apprenti dans un studio d'artiste ; la mémoire de ses propres expériences créatives antérieures et de sa production passée ; le chaudron culturel

(2) Suivant en cela, entre autres, les enseignements du neurologue Antonio Damasio (Damasio, 1994).

dans lequel on vit qui influence sa créativité ; le sens et les discours donnés, associés aux artefacts produits ; les interprétations et appréciations données par les observateurs.

Communication

Sont désignés sous ce terme : les représentations des connaissances communicables de manière graphique et visuelle ; l'archivage des expériences, des idées, des souvenirs, des messages ; l'histoire et les transformations successives menant à une oeuvre d'art d'excellence (par exemple *La Joconde* de Léonard de Vinci).

Sentiments

Provoquer des émotions, à travers des souvenirs (visuels) ; générer ou représenter du plaisir ; représenter les relations entre les êtres, entre les humains et la nature, entre les humains et leurs habitats ; évoquer le caractère d'une personne (dans un portrait ou une sculpture, comme *Le Balzac* de Rodin).

Analyse

Découvrir différentes manières de projeter une idée, un paysage, un portrait, une interprétation ; rendre explicite et compréhensible visuellement un phénomène ou une situation complexe (*e.g.* techniques de rendus dans les dessins anatomiques de Léonard, de Michelange ou de Vesalius) ; interpréter visuellement des idées sur le monde, sur les théories (par exemple en physique, médecine, chimie) ; externaliser notre raisonnement (dans des croquis, des schémas, des dessins préparatoires).

Créativité

Repousser les limites de notre perception ; illustrer et documenter notre imagination, nos rêves, nos peurs, nos obsessions, nos passions ; inventer de nouveaux symboles visuels ; à l'origine de l'écriture [3].

J'ai l'intention d'essayer de convaincre le lecteur que l'art nous donne une fenêtre de choix sur l'intelligence (humaine). De plus, l'art évolue (dans sa pratique, ses supports et ses résultats) de pair avec les avancées réalisées sur nos outils les plus sophistiqués : les machines.

Machines (et ordinateurs)

Les machines sont aujourd'hui (et depuis au moins les débuts de la révolution industrielle) nos outils les plus avancés. Elles sont généralement conçues comme des extensions de notre corps ou de nos capacités. Leurs principales contraintes, et ce qui les distinguent d'autres formes d'outils, sont liées à l'apport d'énergie requis, à la qualité du contrôle disponible, et à la capacité de transformation (de la matière, de l'environnement). L'autonomie et la sophistication du contrôle de ces machines sont devenues des caractéristiques plus importantes avec l'invention et le développement continu de l'électronique et des ordinateurs.

Je me focalise ici sur les machines qui intègrent un côté numérique leur permettant de « toucher » le monde (avec capteurs) et de « calculer » (de raisonner vis-à-vis d'un sujet à partir des données captées). Les machines numériques doivent être considérées comme distinctes des outils plus

(3) On peut considérer que l'art a fourni le berceau de l'écriture. Les premières traces d'art visuel remontent à au moins 30 000 ans, par exemple, dans les peintures rupestres à Altamira en Espagne, à Chauvet en France, à Sulawesi en Indonésie. La sculpture de motifs et de formes dans la roche remonte à au moins 300 000 ans (Bednarik, 2003). Les origines (beaucoup plus récentes) de l'écriture, il y a environ 6 000 ans, se retrouvent dans des symboliques visuelles, sous forme de logogrammes, et apparaissent comme des extensions directes des formes d'art primitif les ayant précédées.

primitifs sans capacités programmables. Les machines numériques sont programmées pour :

- agir dans le monde ;
- réagir aux changements de conditions et aux événements perceptibles ;
- informer, traiter des données sur le monde, généralement dans un domaine d'action limité ou étroit.

L'évolution des outils menant aux machines programmables a suivi l'évolution de l'*homo sapiens*. Les traces originales de pratiques artistiques remontent à des centaines de milliers d'années, avec les premières gravures sur pierre (Bednarik, 2003). Tout au long de l'histoire, nous avons développé notre capacité d'impacts et de transformation de la matière par l'utilisation et l'évolution de nos outils, et ce en partie au travers de nos activités artistiques. Cette évolution suit « main dans la main » celle de nos capacités intellectuelles.

Intelligence

Je fonde ma définition de l'intelligence (humaine) sur les capacités permettant à un être d'agir dans le monde, de réagir au monde et d'approfondir sa compréhension du monde, et ce de maniere autonome. C'est une base assez générale qui peut être appliquée à tous les êtres vivants. Ainsi, je considère que différents niveaux d'intelligence sont disponibles pour toutes les espèces. Les humains ont un ensemble plus diversifié de capacités que les autres espèces, et sont en particulier moteurs dans l'évolution de leurs propres capacités, connaissances acquises, et représentations, voire compréhension, du monde.

Ci-après, quelques-unes des dimensions importantes selon lesquelles l'intelligence (humaine) s'exprime.

Perception

La perception du monde par l'entremise de nos sens est prise en charge par des « interfaces utilisateur » intégrées à nos systemes nerveux et tactiles (Hoffman, Singh & Prakash, 2015 ; Koenderink, 2019). Nous ne pouvons comprendre le monde à l'intérieur et à l'extérieur de notre corps que via de telles interfaces. Par exemple, nous percevons les couleurs de manière particulière, qui sont des fabrications par notre système nerveux aidant à comprendre ce que nous ressentons visuellement. Une autre espèce exposée au meme signal électromagnétique aura une interprétation sous une palette des couleurs différente (qui correspond à sa souche évolutive). Les couleurs chez l'humain sont également apprises (liées à la culture) et peuvent évoluer, être affinées avec le langage (en associant des significations fines aux percepts) [(4)]. Nous percevons les objets comme des formes, auxquelles peuvent être associées des fonctions particulières (*e.g.*, différents objets faisant office de « chaise »). De telles « formes » font à nouveau partie de notre interface avec le monde (Leymarie, 2011), et sont à distinguer de la physicalité de l'objet lui-même (c'est-à-dire de l'assemblage de molécules constitutives de l'objet). Il s'agit d'un point de vue similaire à « l'icône sur écran » représentant un dossier et lié à un espace physique dans la mémoire de l'ordinateur : il n'y a pas de véritable dossier dans l'ordinateur, mais la forme du dossier nous évoque sa finalité et fonction potentielle (Hoffman, Singh & Prakash, 2015 ; Koenderink, 2019).

(4) Par exemple, la couleur bleue est inexistante en grec ancien ; Homère décrit la mer comme « couleur du vin ». Aujourd'hui, certaines tribus humaines manquent encore d'une notion du bleu ; ainsi, les Himbas ne font aucune réelle distinction entre les nuances de vert et de bleu. Cependant, ils ont beaucoup plus de mots, que dans nos cultures citadines, pour des variations dans les verts (Roberson *et al.*, 2006).

Communication
Nous utilisons nos systèmes nerveux et tactiles entrelacés (et le reste du corps) pour recevoir et émettre des informations. Nous utilisons le langage, les gestes, les expressions faciales, le contact visuel, la pose corporelle, l'odeur, et plus encore, pour exprimer des idées, des émotions, des messages subtils.

Actions
Nous nous déplaçons à travers le monde avec notre corps articulé, saisissant et manipulant des objets, en mode exploratoire.

Analyse
Raisonner, observer, conclure, comparer et faire des choix.

Apprentissage
Nous apprenons de par nos expériences, par le jeu et les répétitions. Nous apprenons des autres, par la scolarité, des livres et d'autres mécanismes d'archivage. Nous perfectionnons nos compétences en nous exposant à des maîtres. Nous apprenons à travers des représentations que nous exprimons au travers de croquis et de dessins ; l'évolution de la représentation des formes et autres concepts au travers du dessin chez les enfants est très caractéristique de ce type d'apprentissage (Golomb, 1994).

Mémoire
Les expériences mémorisées orientent nos actions et nos décisions futures. Nous organisons (probablement) et prolongeons nos souvenirs pendant nos rêves.

Créativité
Nous innovons. Nous associons des sujets et des concepts de manière nouvelle. Nous réinterprétons les anciennes façons de représenter notre monde.

Outils
Nous concevons des outils. Les outils deviennent des extensions de notre corps, sous le contrôle de notre intellect. Les outils nous permettent de mieux utiliser les sources d'énergie que l'on trouve dans la nature. Les outils évoluent avec nous, sous notre contrôle. Certains de ces outils peuvent étendre nos domaines sensoriels, comme lorsque nous visualisons le monde des molécules ainsi que le monde des galaxies.

Externaliser (une partie de) l'intelligence
Je fais l'hypothèse que l'évolution de l'intelligence, que l'on peut considérer comme étant à son stade le plus avancé chez les humains modernes, est étroitement liée à la coévolution des outils. Les outils nous ont poussés à explorer notre monde de manière de plus en plus raffinée et puissante. Le résultat le plus récent de cette coévolution peut être vu dans nos machines, en particulier celles qui peuvent être programmées et dotées d'un certain niveau d'autonomie.

Fait historique intéressant, les premières machines programmables ont émergé du monde des arts et de l'artisanat. En 1768, l'horloger suisse Pierre Jaquet-Droz, élève de Daniel Bernoulli, conçoit et construit un automate sous forme humaine, appelé « l'écrivain ». Composé d'environ 6 000 pièces, il contient une roue programmable dans laquelle différentes formes peuvent être interchangées. Chacune de ces formes agit comme une mémoire (ancêtre du disque avec instructions gravées) qui peut être déchiffrée afin que l'automate exécute l'écriture d'un message particulier (ainsi que diverses animations de son corps, de ses yeux, etc.) ; jusqu'à 40 caractères peuvent ainsi être écrits

à la fois par l'automate. « L'écrivain », ainsi que deux autres automates sophistiqués (mais pas aussi facilement reprogrammables), « le dessinateur » et « la musicienne », peuvent encore être observés fonctionnant au Musée d'art et d'histoire de Neuchâtel, en Suisse. Le prochain progrès majeur pour les machines programmables est venu au début du XIX^{e} siècle (vers 1805), avec l'invention du métier à tisser dit de Jacquard. Conçu pour un tissage textile efficace, ses actions et les motifs qu'il produit sont programmables par l'utilisation de cartes perforées pliables (un moyen d'imprimer du code qui sera utilisé dans les ordinateurs électroniques numériques contemporains, jusqu'aux années 1980). Les étapes suivantes au XIX^{e} siècle ont été les machines de Babbage, en particulier le moteur analytique programmable, et les concepts de programmes algorithmiques et de code par Ada Lovelace. Puis viendront au XX^{e} siècle Turing, von Neumann et l'éclosion de l'ordinateur et de ses suites (Hey et Pápay, 2014).

L'impact de l'IA

Pour certains, l'étude, la conception et le progrès de nos machines les plus avancées peuvent être considérés comme une entreprise distincte de l'étude de la nature humaine. Cependant, les origines du domaine de l'intelligence artificielle (IA) donnent un son de cloche différent, celui-ci ayant émergé de l'idée suivante (McCarthy *et al.,* 2006) : « L'étude doit procéder sur la base de la conjecture que chaque aspect de l'apprentissage ou toute autre caractéristique de l'intelligence [humaine] peut en principe être si précisément décrit qu'une machine peut être amenée à le simuler ».

La machine moderne, à travers ce manifeste, peut être vue comme une extension naturelle de notre développement intellectuel en tant qu'espèce capable de concevoir ses propres outils et moyens de communication ainsi que des représentations du monde.

Dans ce contexte, il est proposé que les sujets qui font partie des arts (comme la créativité, l'expertise ou la maîtrise) et des machines (telles que leur conception, l'ingénierie, le contrôle et leurs applications) puissent être réunis pour nous aider à étudier et mieux comprendre de quoi l'intelligence humaine elle-même est formée. Ensemble, ils peuvent également nous aider à augmenter nos capacités intellectuelles. En outre, ils peuvent plus simplement dupliquer ou simuler certaines de ces capacités, tel qu'envisagé par le manifeste de 1955 de McCarthy *et al.*, ou encore par Turing dès 1950 (Turing, 1950).

Dans ce qui suit, je décrirai quatre projets phares et leur artiste associé comme exemples de la manière dont le trio « art, machine, intelligence » peut être fusionné, et ce de diverses façons.

Art.Machine.Intelligence dans la pratique

Art informatique évolutif : William Latham

Créativité : comment la simuler et la stimuler davantage

Dans les années 1980, William Latham, alors étudiant en arts au Royal College of Arts de Londres, descendait souvent le long de la rue Exhibition Road pour se rendre en quelques minutes au Musée d'histoire naturelle, où il pouvait pendant des heures contempler la créativité et la grande diversité dont la nature est féconde. Ainsi inspiré, il a par la suite inventé une méthode créative basée sur son interprétation de l'évolution biologique et son rôle dans la création de la diversité des formes. L'algorithme, dans un cas appelé « FormSynth », était basé sur des règles simples et sur un mode itératif (Todd et Latham, 1992). Latham dessinait divers arbres évolutifs (Figure 1), sur de grands et très longs rouleaux de papier (par exemple, 2 mètres sur 8 mètres). Finalement, il réalisa les limites pratiques de cette approche, et vers la fin des années 1980 il rejoignit le centre de

Figure 1. FormSynth, un exemple d'exploration artistique de la diversité des formes par arbres évolutifs, par William Latham, autour de 1985.

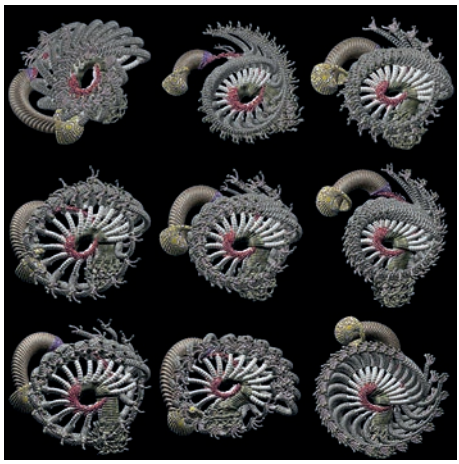


Figure 2. Mutator, un programme informatique combinant FormSynth avec une simulation d'évolution ultra-rapide ; neuf formes complexes ont évolué, et seul un sous-ensemble est choisi pour la prochaine itération-génération (par mariage et/ou mutation) ; travail de Latham en collaboration avec Todd (Todd et Latham, 1992).

recherche britannique d'IBM près de Winchester. Une nouvelle activité fut alors créée au croisement de l'art, de la science et de la discipline de l'infographie en pleine évolution. Là, il travailla avec différents chercheurs et notamment initia un partenariat à long terme (et toujours en cours) avec l'inventeur et informaticien Stephen Todd (auteur de plus de 80 brevets). Ensemble, ils ont contribué à la création d'une discipline que nous pouvons maintenant appeler « l'art informatique évolutif » (Antunes, Leymarie & Latham, 2016).

FormSynth fut transformé en un programme informatique qui résulta en un système beaucoup plus sophistiqué et plus étroitement lié à l'évolution biologique, que Latham et Todd ont appelé « Mutator » (Todd et Latham, 1992 ; Lambert, Latham, & Leymarie, 2013). Dans ce système, des mutations et des mariages ont lieu, produisant une descendance multiple, ce de manière pseudo-naturelle (par exemple, avec deux parents ou plus fournissant leurs « gènes » sous forme de séquences de code avec des instructions sur l'assemblage de formes constitutives et leurs caractéristiques associées). Toute cette simulation de processus évolutifs accélérés reste sous la direction de l'oeil humain : l'artiste y joue le rôle de généticien-jardinier sélectionnant les descendants les plus prometteurs en fonction de leur valeur esthétique perçue (Figure 2).

À partir du milieu des années 1990, Latham rejoint le domaine en plein essor des jeux vidéo et crée son propre studio. J'ai rencontré Latham vers 2005 et je l'ai convaincu de se joindre à nous à l'Université de Londres pour revenir à ses premiers travaux de pionnier. Plus tard, Stephen Todd a de nouveau rejoint Latham, et ensemble ils sont revenus à leur travail original avec un oeil neuf. Ils ont retravaillé et transformé le système évolutif original en « MutatorVR », où l'artiste ou l'utilisateur/observateur peut s'immerger dans les processus évolutifs numérisés et bénéficier des progrès réalisés en informatique au cours des deux dernières décennies (Latham *et al.*, 2020) (Figure 3).

L'art (et le *design*) lui-même a une histoire qui se lit comme un conte évolutif. Les idées et les techniques du passé informent la prochaine génération de créateurs. Les compétences et l'esthétique du passé font partie de leur ADN artistique, que certains modifient, parfois radicalement, en participant au processus d'évolution au fil des siècles. Ce que des artistes

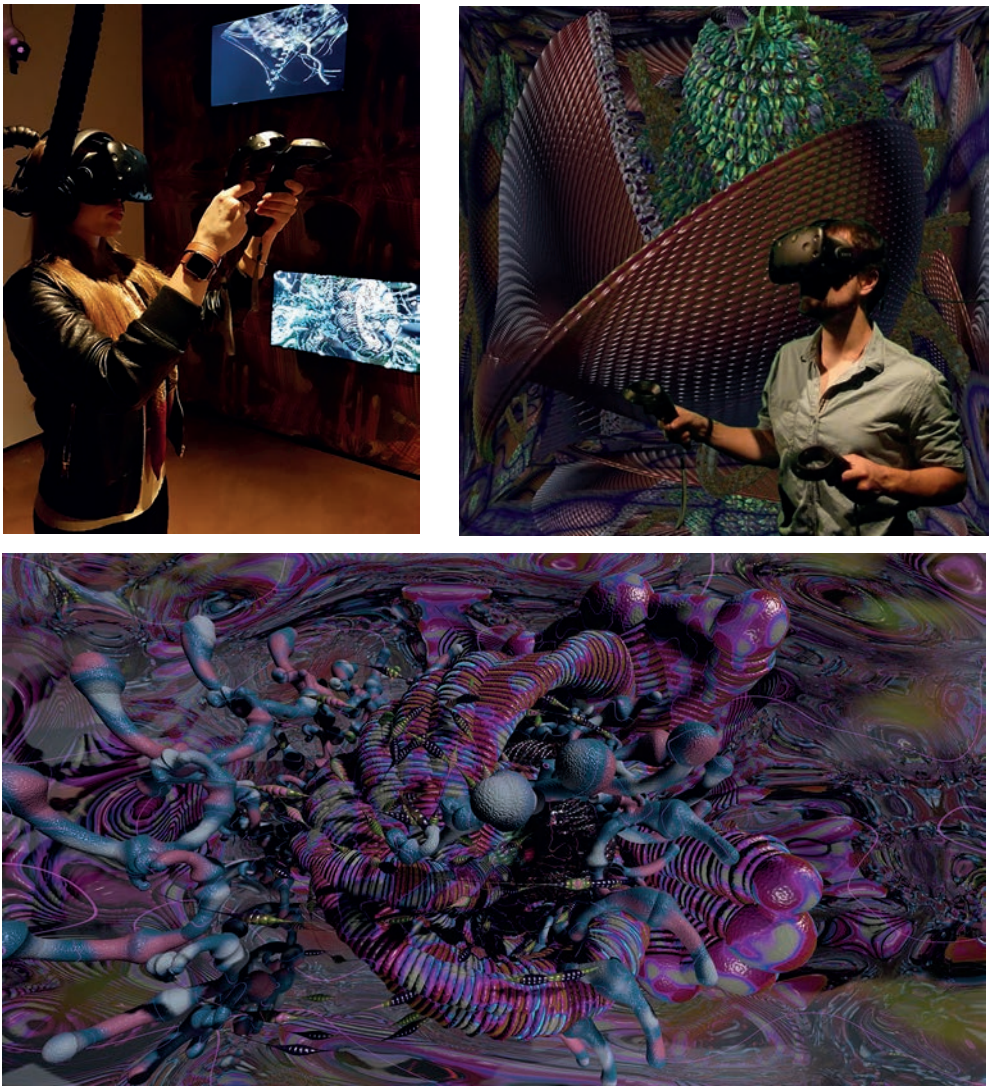


Figure 3. Mutator VR, 1re rangée : exemples d'installations immersives. 2e rangée : vue prise de l'intérieur de l'un des univers imaginaires (dynamique, évolutif et itératif) de William Latham.

contemporains comme Latham en sont venus à réaliser, c'est que les simulations d'un processus créatif évoluant relativement lentement peuvent éventuellement être grandement accélérées grâce au potentiel de l'informatique. L'utilisation de machines numériques, équipées de capteurs (caméras, microphones) et de dispositifs en sortie (écrans, haut-parleurs, casques de réalité virtuelle (RV)) ou d'autres dispositifs d'interface utilisateur (tels les contrôleurs manuels de RV qui peuvent fournir un *feedback* haptique au travers de vibrations) offre également de nouvelles possibilités pour révéler la pensée intime (ou l'imagination) de l'artiste : comment la pratique traditionnelle (croquis, itérations, *designs* raffinés, pièce finale) peut être modélisée et transformée en une plateforme informatisée interactive qui soit capable de plonger plus intensément le sujet dans le monde créatif d'un artiste. Une telle machine devient une nouvelle interface avec laquelle l'esprit humain peut interagir.

Portraits et art robotique : Patrick Tresset

Incarnation : l'importance du corps

J'ai rencontré Patrick Tresset, alors artiste de la scène des arts visuels de Londres, lorsque je suis arrivé dans la capitale outre-Manche fin 2004 pour débuter ce qui était alors le premier master en science des arts et de l'informatique au Royaume-Uni [5]. Tresset avait également une formation en programmation, qu'il avait acquise au cours de ses études en France, s'était installé à Londres une quinzaine d'années auparavant pour s'établir en tant qu'artiste visuel et avait exploré de nombreux genres différents, allant du portrait à la peinture abstraite. Tresset faisait partie de la première génération d'étudiants diplômés et de chercheurs avec lesquels j'ai eu le plaisir de collaborer en rejoignant Goldsmiths (*college* satellite de l'Université de Londres).

Tresset avait rejoint le master de Goldsmiths pour explorer comment mieux combiner ses expériences précédentes en programmation avec sa passion pour les arts visuels et la créativité. L'un des projets qu'il a poursuivis pendant cette période se démarquait des autres : essayer de modéliser sa propre pratique artistique, ses compétences et son style de réalisation de croquis et de portraits rapides, ayant une qualité visuelle certaine, fort eloigné des oeuvres d'art informatisées de l'époque. En essayant de modéliser les différentes étapes principales suivies par Tresset lors de la préparation puis l'exécution de ses croquis, nous avons créé un premier système logiciel simple nommé « AIkon » (Tresset et Leymarie, 2005, 2006) [6]. Tresset a alors exploré les possibilités offertes par le système et ses paramètres, en dérivant vers divers autres styles, ressemblant plus ou moins à ses propres dessins à la main, (Figure 4).

Figure 4. AIkon-1 : exemples de portraits automatiques, avec à la 1ere rangée : premiers résultats avec tracés arrondis ; stèle d'Al-Uzza ou Allat, du Temple des Lions Ailés à Pétra en Jordanie ; l'écrivain, bio-chimiste et humaniste Isaac Asimov ; le physicien Stephen Hawkins. 2e rangée : la créatrice du premier programme pour ordinateur Ada Lovelace ; le pionnier du cinéma muet et acteur légendaire Buster Keaton ; l'actrice, productrice et inventrice Hedy Lamarr ; le mathématicien et pionnier de l'informatique Alan Turing.

(5) En anglais : "MSc Arts Computing", renommé plus tard "MA Computational Arts".
(6) AIkon, aussi appelé « Ikonographe artistique », « automatisé », « autonome » ou « artificiel ».

Mais nous étions tous deux insatisfaits à l'issue de ce premier projet (que nous appelons maintenant « AIkon-1 »). Nous avions un modèle de travail reposant sur des caractéristiques d'une image ou d'une photographie sur lesquelles il fallait se concentrer lors d'un rendu rapide de dessin au trait, mais nous ne pouvions pas recréer les détails subtils des traces laissées par la main de l'artiste. En particulier, les hésitations, le caractère unique de chaque geste de la main et la manipulation d'un outil de dessin ou d'un pinceau se sont avérés difficiles à modéliser. Après une pause de quelques années, et avec l'aide financière du Leverhulme Trust [7], Tresset a pu travailler à nouveau avec moi, et nous nous sommes alors engagés dans un second projet de recherche à plus long terme, appelé « AIkon-2 ».

C'était en 2009, et une évolution majeure avait eu lieu dans le monde de la robotique. Il était désormais possible de commander et de fabriquer soi-même des bras robotisés à des prix très raisonnables (quelques centaines d'euros) pour obtenir de simples manipulateurs controllables. De plus, la communauté scientifique internationale avait mis au point des plates-formes logicielles pour la programmation de la robotique qui simplifiaient grandement les tâches d'envoi de commandes de contrôle aux robots [8].

Ces deux avancées ont permis à des non-spécialistes (en robotique) aux moyens financiers modestes de commencer à construire et à tester des prototypes non triviaux. Tresset a commandé les premiers servomoteurs et diverses pièces, conçu et construit un bras (avec épaule, coude et poignet articulés) avec une simple pince pour la « main », qui pouvait tenir un stylo (généralement un BIC). Il a également conçu une plate-forme robotique sur laquelle était montée une petite caméra, qui pouvait tourner avec 2 degrés de liberté et jouait le rôle d'un « oeil ». Tresset a finalement surnommé l'ensemble du système « Paul le robot ». Le bras, l'oeil et un ordinateur portable étaient solidement fixés à une simple table, l'ordinateur portable ou « cerveau » demeurant caché sous la table (Figure 5). Paul a fait ses débuts publics à la foire d'art Kinetica, à Londres, en février 2010. Il a immédiatement capté l'attention du public. De longues files d'attente ininterrompues se formaient chaque jour. L'une des vidéos produites pendant cette période, pour une exposition dans une galerie londonienne en 2011, a reçu à ce jour plus de 3,4 millions de vues (visites sur internet) et continue d'attirer l'attention et des commentaires, certains soulignant la nature étrange (*uncanny* en anglais) de l'expérience [9].

Figure 5. AIkon-2 : Stella, un des premiers portraits (signé) produits par Paul le robot, Londres, 2011.

(7) https://www.leverhulme.ac.uk/
(8) L'une de ces plates-formes logicielles, déjà populaire à l'époque, était YARP ("yet another robot platform", www.yarp.it), et une autre qui venait de voir le jour était ROS, le système d'exploitation robotique désormais bien reconnu dans la communauté robotique internationale (www.ros.org).
(9) Sur YouTube : https://youtu.be/bbdQbyff_Sk

La plate-forme robotique a permis un mimétisme plus proche des mouvements subtils de la main humaine (Tresset et Leymarie, 2012). De par sa prise en charge de la conception du bras, Tresset s'est rendu compte que ce dernier n'avait pas besoin d'être trop précis dans la façon dont il réalisait son mouvement, comme ce serait le cas pour les applications robotiques traditionnelles. Le bras du robot pouvait avoir un tremblement naturel, et ne pas atteindre systématiquement les objectifs de position fixés par ses routines de contrôle. De plus, le fait d'avoir un mouvement articulé sous la forme d'un bras simple permettait des variations dans les traces produites qui ressemblaient à l'incertitude observable des propres productions de l'artiste humain. Du côté de la recherche, nous avons poussé plus loin nos explorations et avons finalement conclu le projet avec une publication, où nous rapportions nos premières tentatives d'introduction de *feedback*s visuels en direct. Comme l'artiste humain, Paul le robot pouvait observer ses propres traces et gestes, à l'aide de son oeil-caméra (qui, jusque-là, avait été utilisé uniquement pour trouver et capturer une vue unique d'un visage d'un passant proche). Et son cerveau artificiel pouvait évaluer en temps réel la qualité du rendu dessiné pour décider où concentrer son attention au fur et à mesure du dessin (Tresset et Leymarie, 2013).

Tresset s'est ensuite éloigné du milieu universitaire pour se tourner vers le monde des foires d'art, des événements art-science, des galeries d'art, au Royaume-Uni, en Europe et dans le monde entier. Ce qui est toujours le cas à ce jour (Figure 6). Tresset a déménagé récemment son atelier de Londres à Bruxelles. Dans les années qui ont suivi notre dernière collaboration (en 2013), il a continué à explorer des améliorations possibles pour ses robots (Kluszczyński, 2016 ; Maddox-Harle, 2017). Il a collaboré avec d'autres chercheurs et a même aidé certaines entreprises de robotique à ajouter la capacité de dessiner à leurs propres robots, comme le robot humanoïde Sophia de Hanson Robotics fin 2019 [(10)].

Figure 6. Patrick Tresset et ses robots dessinateurs. À gauche : « La classe », où l'on découvre une classe entière de robots, chacun ayant ses caratérisques uniques, qui suivent l'instruction du maître robot (en 2017 environ). À droite : « 5 robots nommés Paul » et l'artiste (autour de 2015).

Le passage du logiciel au matériel, dans la forme d'un corps (robotique), a joué un rôle important dans l'évolution de la pratique artistique de Tresset. Les différences de signatures stylistiques lors du passage de solutions uniquement logicielles, telles que celles illustrées par Alkon-1, à un système robotique comme Paul le robot, furent spectaculaires. L'utilisation d'un corps robotique a permis à Tresset à l'époque de capter les subtilités du mouvement et leur rapport à la qualité des traces dessinées, tout en se concentrant sur d'autres aspects de la conception de la plate-forme robotique et des potentiels de performance.

Du point de vue de l'art et de la performance, Paul le robot devient une petite expérience théâtrale pour le sujet humain. Le sujet doit se tenir ou s'asseoir près de l'entité robotique, rester immobile (autant que possible) pendant environ 20 minutes durant lesquelles la machine effectue sa série

(10) www.hansonrobotics.com

d'observations et de gestes de dessin, qui se terminent par sa propre signature. Tout au long de cette performance, le robot fait des bruits inhabituels, hésite, regarde à nouveau le sujet, semble penser, puis continue à dessiner en regardant sa production. Une expérience relationnelle unique s'établit entre l'humain et la machine. Le sujet humain repart avec un souvenir indélébile.

Tresset choisit de garder ses robots clairement reconnaissables comme des machines articulées. Il est l'artiste humain, concepteur et ingénieur en chef qui explore l'utilisation de telles machines pour étendre sa portée artistique. Le corps de Paul le robot devient une autre incarnation possible pour Tresset, qui est accessible, contrôlable et reprogrammable par l'artiste humain. Le corps du robot est aussi un outil sophistiqué permettant à l'artiste d'explorer de nouvelles possibilités créatives.

Calligraphie et graffiti digitalisés : Daniel Berio

Cinématique et mouvement corporel : expertise, esthétique

Le travail sur la robotique et le portrait avec Tresset a attiré l'attention de communautés très diverses, de l'informatique et de la robotique aux arts, aux foires d'art, aux musées (un portrait a été acquis par le prestigieux Victoria and Albert Museum de Londres), aux événements artistiques et scientifiques, ainsi que de multiples médias. Il a également attiré l'attention de nombreux artistes et aspirants innovateurs en art et en science. L'un d'eux, Daniel Berio, un graffeur italien, a décidé de rejoindre mon équipe à Goldsmiths en 2015. Daniel avait de bonnes connaissances en programmation graphique, et venait tout juste d'être diplômé de la Royal Academy of Art de La Haye, où il avait développé quelques premières machines pouvant dessiner.

Afin d'aller au-delà des résultats des projets AIkon (1 et 2) avec Tresset, nous avons décidé, Berio et moi, très tôt de nous concentrer sur l'importance du mouvement dans la réalisation de traces manuscrites ou dessinées. L'hypothèse principale à tester consistait à connaître quelle est l'influence de la vitesse et de l'accélération le long d'une trace faite par une main experte (c'est-à-dire par un artiste). En raison de l'expérience de Daniel, nous nous sommes d'abord concentrés sur la production de graffitis. Le graffiti en tant que forme d'art moderne a émergé à New York au début des années 1970 avant de se répandre dans le monde entier, en particulier dans les grandes villes, où de nouveaux styles ont été inventés. Dans sa plus simple expression, le graffiti est une forme d'écriture rapide, laissant une signature ou une étiquette, ou une série de formes de lettres sans signification *a priori* distincte (en tant que mots). Le but est de réaliser un résultat graphique spectaculaire, généralement sur une grande surface murale extérieure. À l'origine, les artistes graffeurs étaient souvent considérés comme des vandales ou comme faisant partie d'un mouvement de protestation [(11)]. Cela a eu une forte influence sur le développement de divers styles, où la vitesse d'exécution est devenue une caractéristique clé. Après des années de pratique, les artistes de rue les plus talentueux finirent par développer leur propre style graphique et une grande maîtrise dans la réalisation de leurs oeuvres d'art (Arte, 2015 ; Ferri, 2016).

En analysant le domaine de l'écriture et du dessin ainsi que son évaluation esthétique, nous avons constaté que d'autres domaines connexes ajoutaient des contributions majeures à considérer pour nous aider à mieux comprendre le processus de production du graffiti et de la calligraphie en général. En psychologie, les scientifiques avaient commencé depuis la fin du XX^{e} siècle à étudier attentivement les relations existantes entre la cinématique du mouvement et la qualité des traces observées (Babcock et Freyd, 1988 ; Pignocchi, 2010). Un certain nombre de résultats étaient disponibles, décrivant les caractéristiques des mouvements utilisés dans la pratique du dessin et de

(11) Je ne considère pas ici les questions sociales et politiques liées aux graffitis, comme forme de protestation ou d'émancipation de la jeunesse. Je me concentre uniquement sur les qualités graphiques et le processus de production d'un tel art.

l'écriture. En particulier, l'hypothèse avait été faite qu'un observateur pourrait apprécier les traces vues dans la calligraphie en reconstruisant dans son propre cerveau les séquences de mouvements probables utilisées dans la production originale (Freedberg et Gallese, 2007). En d'autres mots, un observateur naïf (pas nécessairement un expert ou un artiste) générera une activation neuronale dans la partie motrice de son cerveau très similaire à celle qu'il produit s'il effectuait physiquement des séquences de mouvements similaires (Leder, Bär & Topolinski, 2012). Ce que vous voyez stimule votre système nerveux comme si vous aviez fait vous-même les mouvements nécessaires pour réaliser le dessin. De plus, la reconnaissance de l'utilisation de mouvements rapides et fluides conduit à une meilleure appréciation du travail ; cela pourrait à son tour constituer une base possible pour une théorie de l'esthétique.

Du côté informatique, un nouveau champ de recherche scientifique est apparu dans les années 1980, appelé « graphonomie » (Kao, Hoosain & van Galen, 1986). Initialement focalisée sur l'ingénierie et la modélisation de systèmes pour dupliquer ou reconnaître des signatures (et détecter les contrefaçons, notamment sur les chèques bancaires), la graphonomie avait mûri et proposait quelques modèles mathématiques très descriptifs de la cinématique des mouvements rapides réalisés par le haut du corps (torse, bras, main) lors du dessin ou de l'écriture (Maarse, van Galen & Thomassen, 1989 ; Plamondon, 1995 ; Teulings, 1996). En complément de ces résultats, nous avons également exploré l'état de l'art en robotique, où les mouvements sont étudiés, planifiés et mis en œuvre par des routines de contrôle sur la base de cadres probabilistes (Calinon et Lee, 2019), lorsqu'il s'agit de contextes imprécis ou adaptatifs et d'architectures robotiques plus proches du corps humain, parfois appelées « conformes », c'est-à-dire flexibles dans leur conception et leur contrôle (pas trop rigide). Les robots conformes et souples sont souvent conçus pour agir à proximité des humains, dans des scénarios collaboratifs.

Le travail avec Berio a maintenant intégré toutes ces sources de connaissances qui ont été rapportées dans un certain nombre de publications et de démonstrations (Berio et Leymarie, 2015 ; Berio, Calinon & Leymarie, 2016 ; Berio, Calinon & Leymarie, 2017 ; Berio, Calinon & Leymarie, 2017 ; Berio et al., 2017 ; Berio, Leymarie & Plamondon, 2018 ; Berio et al., 2019 ; Berio, Leymarie & Calinon, 2020). Nous avons montré qu'il est possible de récupérer des cinématiques (paramètres de mouvement) à partir de traces statiques, de sorte que les mouvements régénérés et les nouvelles traces sont semblables à ceux des experts humains (Figure 7) (Berio, Leymarie & Plamondon, 2020) ; nous avons établi et démontré une première méthode d'apprentissage applicable aux robots collaboratifs humanoïdes, pour leur permettre d'écrire une calligraphie de qualité humaine (Figure 8), et produit une interface utilisateur, où l'artiste humain peut générer et contrôler facilement des traces calligraphiques d'une manière plus naturelle et aboutissant à une cinématique semblable à celle de l'expert humain (Berio, Leymarie & Plamondon, 2018 ; Berio, Leymarie & Calinon, 2020).

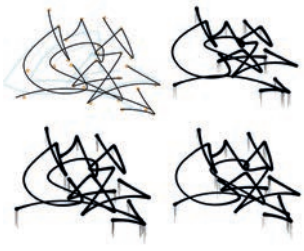


Figure 7. Exemples de tags générés automatiquement sur la base d'un nombre restreint de cibles (point en jaune, en haut, à gauche) et variations paramétriques guidant la cinématique du geste et du tracé (Berio et Leymarie, 2015).

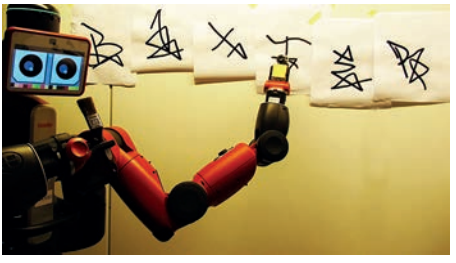


Figure 8. Le robot Baxter (robot humanoide non rigide, concu par Rethink Robotics) ayant appris à écrire ses propres tags de qualité s'approchant de ce qu'un humain peut produire (Berio, Calinon & Leymarie, 2016).

Figure 9. Génération de graffitis de divers styles à partir d'une représentation des lettres sous forme d'un graphe (Berio *et al.*, 2019).

Un projet en cours va au-delà des traces dessinées unidimensionnelles et considère la forme de lettre en 2D (Berio *et al.*, 2019). Nous intégrons de nouveaux résultats inspirés de la psychologie (perception de la forme) pour permettre la récupération systématique des squelettes de traits à partir de tout symbole en 2D ressemblant à une lettre. L'hypothèse étant qu'un trait distinctif commun aux formes de lettres dans toutes les langues (des caractères kanji aux alphabets occidentaux) est leur génération via une série de mouvements de traits (d'une position cible à une autre, lors de l'utilisation d'un stylo ou d'un pinceau) constituant des séries de tracés (Figure 9), y compris des boucles et tracés sinueux, avec des applications possibles au domaine du tissage et de l'impression 3D (Figure 10). Un autre thème de recherche en cours est axé sur l'apprentissage par des architectures de réseaux neuronaux des nombreux paramètres nécessaires pour contrôler ces systèmes calligraphiques informatisés ou robotiques (Berio *et al.*, 2017).

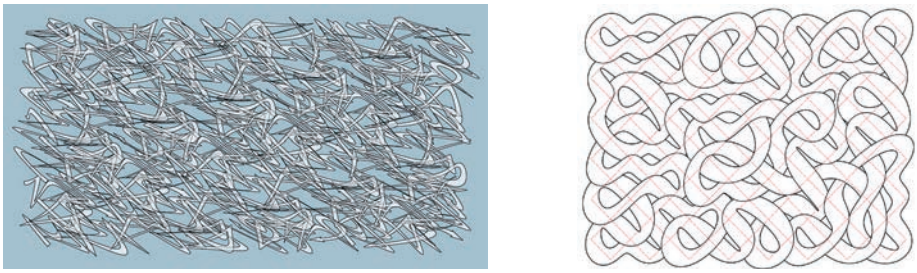


Figure 10. Génération de tracés de tissages sous forme de graffitis, à partir d'une représentation des « lettres » (ou d'un parcours) sous forme d'un graphe (Berio, 2020).

Apprentissage profond et mondes intérieurs : Terence Broad

Réseaux de neurones à découvert : exploration du fonctionnement interne des architectures de réseaux de neurones artificiels

Les méthodes d'apprentissage profond (de l'anglais *deep learning* ou DL) utilisées dans les arts sont explorées (principalement) par une nouvelle génération d'artistes-programmeurs (Bessette, Leymarie & Smith, 2019 ; Akten, 2020). C'est aussi un moment historique particulier du développement scientifique et du partage des connaissances : les communautés scientifiques impliquées dans le développement du DL (et plus généralement de l'IA) ont pris l'habitude (surtout au cours de la dernière décennie) de publier du code « utilisable » et des jeux de données (avec étiquettes ou sémantique associée). Les jeux de données restent fragmentés, mais la situation est nouvelle : on met à disposition suffisamment d'informations pour que d'autres, pas forcément des experts en informatique ou en IA, se jettent dans ce bain technologique.

Cette disponibilité de logiciels de pointe et de données associées a ouvert la possibilité aux artistes – intéressés par le métier de la programmation – d'explorer cette sphère florissante [(12)]. Un artiste

(12) Ceci rappelle une autre époque charnière où la photographie, d'abord développée comme une technologie par des inventeurs et des ingénieurs, a été adoptée par les arts après quelques années de premières explorations, d'abord du portrait, puis comme son propre médium artistique (Agüera et Arcas, 2017).

cherchera non seulement à maîtriser (l'utilisation de) la technologie, mais à l'appliquer à de nouveaux objectifs, et il pourra également changer complètement la façon dont la technologie est utilisée, ou comment elle se comporte, avec la possibilité d'obtenir des résultats surprenants et intéressants.

Un ingénieur ou *data scientist* utilisera le DL pour répondre à des besoins spécifiques, tels que la génération de solutions plausibles basées sur un ensemble de données initiales, lorsque confronté à des données modifiées ou à un nouvel ensemble de paramètres. L'artiste, en revanche, ne s'intéresse pas nécessairement au plausible, et recherche plutôt l'extraordinaire, qui va révéler peut-être de nouvelles émotions en réponse à des images ou des artefacts jamais encore observés.

Dans les applications classiques (avec un objectif utilitaire identifié *a priori*), les systèmes DL sont traités comme des boîtes noires : leur fonctionnement interne peut tout aussi bien rester incompréhensible (tant qu'ils fournissent des résultats utiles). Dans un contexte artistique, l'inverse est souvent vrai : comprendre (une partie) du fonctionnement interne à un système est souvent la clé pour fournir un plus grand contrôle créatif à l'artiste. Différentes stratégies sont utilisées ; on peut essayer de « casser » le système DL (pour conduire à des résultats inattendus), en utilisant des données différentes, en modifiant les paramètres d'entrée habituels, en recâblant l'architecture DL, et voir où cela mène. Une autre stratégie est de chercher des moyens de mieux contrôler le système, par exemple de pouvoir peindre à l'aide d'un réseau de neurones artificiels (RNA) qui reste sous la direction de l'artiste, et de créer une interface utilisateur pour une architecture donnée adaptée aux besoins de l'artiste.

Le mot qui vient souvent à l'esprit lorsque l'on considère des oeuvres d'art créées avec l'aide du DL est « rêveur » [13]. Les résultats évoquent les mondes imaginaires que nous associons aux rêves, ou peut-être des mondes intérieurs fantastiques, fruits de notre imagination. Fait intéressant, à la base même des RNA se trouve l'objectif de construire des simulacres de ce qui peut être observé dans nos systèmes nerveux biologiques. Les RNA sont conçus pour apprendre à réagir à différentes données provenant de sources extérieures, en ayant été au préalable exposés à des quantités massives de données avec sémantique associée.

De la même manière, les rêves humains sont souvent le résultat de constructions créatives obtenues à partir de souvenirs (récents ou anciens). De nouveaux scénarios ayant leurs origines dans des situations réelles rencontrées précédemment sont joués dans notre petit théâtre intime.

Pour illustrer mes réflexions, je considère certains des travaux récents d'un jeune artiste-programmeur, Terrence Broad. Dans *Blade Runner - Autoencoded, Broad*, en collaboration avec Mick Grierson, il a utilisé un type de RNA, appelé « auto-encodeur », pour recréer les images d'un film (Broad et Grierson, 2017). L'auto-encodeur est d'abord formé par l'encodage d'un flux d'entrée, dans ce cas précis il s'agit des images originales du film de science-fiction *Blade Runner* (1982). En gros, la moitié de l'architecture RNA est utilisée pour « compresser » les informations contenues dans le film dans un espace latent (la boîte noire). L'autre « moitié » décode cet espace latent pour régénérer autant que possible l'entrée. Après avoir réglé les paramètres de l'architecture et effectué divers cycles d'apprentissage à différentes échelles, les auteurs ont pu demander au système de recréer une version du film à partir de sa « mémoire » (encodée). Alors que certaines scènes, généralement des séquences statiques dans l'original, sont bien recréées, la plupart des scènes restantes est une approximation reconnaissable avec un style « rêveur » et « flou » [14]. Les auteurs ont ensuite exploré la reconstruction d'autres films en utilisant les paramètres dérivés de *Blade Runner* et ont obtenu divers rendus au style que je qualifie de « rêveur » (*dreamy* en anglais) (Figure 11).

(13) Un terme plus technique a été proposé qui s'associe à cet effet visuel : « indétermination visuelle » (Hertzmann, 2020).
(14) Une vidéo YouTube documentant le projet a attiré plus de 260 000 vues (https://youtu.be/3zTMyR-IE4Q).

Figure 11. Films auto-encodés (Broad et Grierson, 2017) : cadres de films avec l'original (à gauche) et le reconstruit (à droite). 1re rangée : *Blade Runner* (1982). 2e rangée : *A Scanner Darkly* (2006).

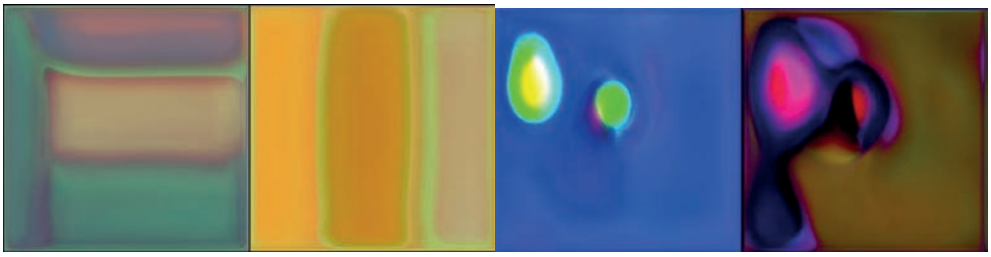


Figure 12. Équilibre instable (Broad et Grierson, 2019) : paires de résultats transitoires par un couple de réseaux de neurones (architecture GAN) essayant de se surpasser l'un l'autre.

Dans le projet nommé *"(un)stable equilibrium"* (équilibre instable), Broad et Grierson ont utilisé un autre type de RNA, les *generative adversarial networks* (ou GANs), et ce, d'une manière inhabituelle : sans aucune donnée d'apprentissage (Broad et Grierson, 2019). Un GAN a généralement deux réseaux DL essayant de se surpasser l'un l'autre. De subtils changements dans les paramètres, les détails architecturaux ou les détails d'optimisation conduisent à une palette de duos intéressants et novateurs, rappelant le mouvement artistique minimaliste des années 1960. À la suite de ce travail, du côté créatif et artistique, Broad a remporté le Grand Prix ICCV 2019 Computer Vision Art Gallery (Figure 12) [(15)].

Le travail suivant impliquait également une architecture de type GAN, utilisée de manière « sournoise ». Les GANs aujourd'hui sont en particulier utilisés pour produire des "*DeepFakes*" (Karnouskos, 2020). L'objectif commun est de laisser l'architecture de DL bicéphale affiner ses compétences afin de générer des images indiscernables de photographies ou de films réels. Mais que se passe-t-il si vous inversez un tel objectif et laissez le GAN se surpasser en créant un contenu non naturel et auparavant jamais vu ? C'est ce que Broad en collaboration avec Grierson et moi-même explorons dans "Amplifying the uncanny", un article décrivant un système qui nous conduit du réel vers l'irréel, l'inconnu, peut-être même l'effrayant ou l'étrange (Broad, Leymarie

(15) https://computervisionart.com/pieces2019/unstable-equilibrium/

& Grierson, 2020a). Broad a produit en utilisant cette méthode une série d'oeuvres d'art intitulée "Being foiled", soit « être déjoué » (Figure 13) [16]. La traversée de la vallée de l'étrange (*uncanny* en anglais) est une manière d'étudier et de représenter certaines émotions humaines qui ont été explorées dans divers domaines tels que la psychologie et la robotique (Mori, 1970).

Figure 13. Traverser la « vallée étrange » à l'envers (Broad, Leymarie & Grierson, 2020a). Deux exemples, à partir d'une photographie réaliste/naturelle (à gauche) et se déplaçant vers l'étrange (vers la droite).

Dans son travail le plus récent, Broad explore les moyens possibles « d'ouvrir le capot » de la boîte noire du DL. En identifiant diverses couches et paramètres dans un GAN responsable de la représentation et de la manipulation de caractéristiques spécifiques, par exemple les yeux, le nez ou la bouche, dans des images de portraits ou des photos, l'artiste commence à prendre le contrôle de l'architeture neuronale. Une étape suivante consiste à introduire des transformations particulières sous forme de filtres dans les couches hautes d'un GAN. Broad explore plus en détail un tel outil dans un ensemble d'oeuvres d'art récentes nommées "Disembodied gaze" (ou « regard désincarné) [17] (Figure 14), et "Teratome" (Figure 15) [18]. Le côté technique, fruit d'une collaboration de Broad avec Grierson et moi-même, est expliqué dans un récent rapport (Broad, Leymarie & Grierson, 2020b).

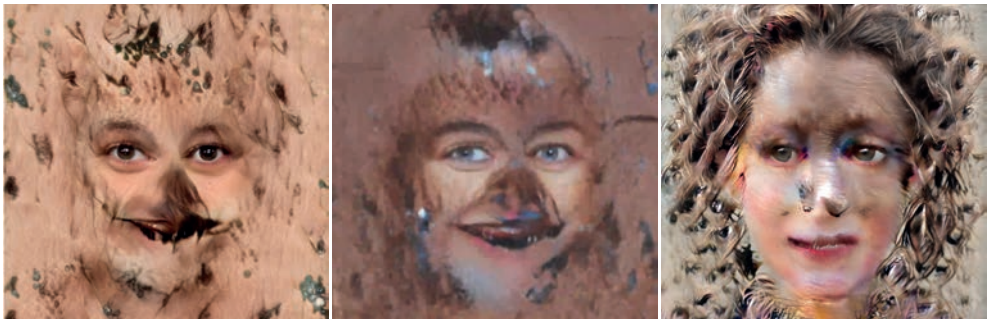


Figure 14. Regard désincarné par T. Broad, utilisant l'architecture "*network bending*" (Broad, Leymarie & Grierson, 2020b) : quelques résultats d'un réseau de neurones (architecture GAN) obtenus en gardant fixes seulement les paramètres responsables de la reconstruction des yeux, et en laissant le réseau libre dans sa reconstruction créative du reste du visage et fond d'image.

(16) https://terencebroad.com/works/being-foiled
(17) https://terencebroad.com/works/disembodied-gaze
(18) https://terencebroad.com/works/teratome

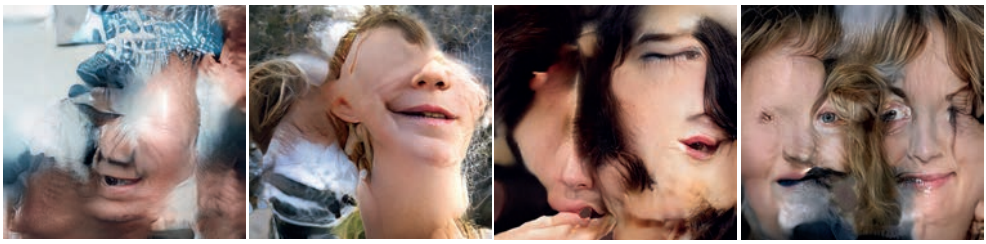


Figure 15. Quelques exemples tirés de la série "Teratome" de T. Broad, utilisant l'architecture "*network bending*" (Broad, Leymarie & Grierson, 2020b). Des filtres ont été insérés dans les couches supérieures d'un réseau de neurones (architecture GAN) pour perturber, inverser et tordre le processus de formation d'image.

L'A.M.I. en point de fuite

J'ai soutenu qu'il existe une fusion naturelle à explorer du trio Art/Machine/Intelligence (A.M.I.). Par « naturel », je me réfère à la signification de ce terme en biologie et en théorie de l'évolution : la sélection est féconde, c'est-à-dire bien adaptée, ici, au contexte d'étude de l'intelligence elle-même.

En outre, c'est un objectif ambitieux d'explorer la création artistique par l'entremise de nos machines les plus sophistiquées. J'ai présenté un argumentaire et quelques exemples provenant de certains artistes contemporains pour démontrer la faisabilité : 1) d'étudier les niveaux d'intelligence avec une telle focalisation, et 2) de simuler et éventuellement d'étendre les niveaux d'intelligence associés. Je souligne que je considère pour l'heure ces extensions comme directement utilisables seulement par les humains eux-mêmes.

Plutôt que de souhaiter, voire d'espérer, qu'une intelligence générale artificielle (AGI en anglais) « émerge » de constructions complexes, mathématiques et algorithmiques, je préfère penser à l'A.M.I. pour son potentiel dans l'étude et l'extension de l'humain. Je soutiens qu'une focalisation sur des jalons de recherche concrets, en particulier lorsque nous étudions et simulons des compétences artistiques, à des niveaux de plus en plus élevés, peut conduire à des percées concrètes et importantes dans la compréhension de l'intelligence elle-même.

Je remercie Arnaud de la Fortelle (MINES ParisTech) de m'avoir proposé de soumettre un article portant sur l'intersection « Art et Intelligence Artificielle », tout en me laissant libre de mon approche du sujet.

Bibliographie

AGÜERA Y ARCAS B. (2017), "Art in the Age of Machine Intelligence", *Arts,* 6(4).

AKTEN M. (2020), "Foreword", *in* LEYMARIE F. F., BESSETTE J. & SMITH G. W. (éd.) *The Machine as Art / the Machine as Artist*, iv–vi. MDPI.

ANTUNES R. F., LEYMARIE F. F. & LATHAM W. (2016), "Computational ecosystems in evolutionary art, and their potential for the future of virtual worlds", *in* SIVAN Y. (éd.) *Handbook on 3D3C platforms: Applications and tools for three dimensional systems for community, creation and commerce*, 441–73, Springer.

ARNHEIM R. (1974), *Art and visual perception: A psychology of the creative eye*, new version, expanded and revised, University of California Press in Berkeley.

ARTE A. (2015), *Forms of rockin': Graffiti letters and popular culture*, Dokument Press.

BABCOCK M. K. & FREYD J. (1988), "Perception of dynamic information in static handwritten forms", *The American Journal of Psychology*, pp. 111-130.

BEDNARIK R. G. (2003), "The earliest evidence of palaeoart", *Rock Art Research,* 20(2), pp. 3-28.

BERIO D., AKTEN M., LEYMARIE F. F., GRIERSON M. & PLAMONDON R. (2017), "Calligraphic stylisation learning with a physiologically plausible model of movement and recurrent neural networks", *Proceedings of the 4th Acm International Symposium on Movement and Computing*, London, UK.

BERIO D. (2020) "AutoGraff: Towards a computational understanding of graffiti writing and related art forms", Ph.D. thesis, Goldsmiths, University of London.

BERIO D., ASENTE P., ECHEVARRIA J. & LEYMARIE F. F. (2019), "Sketching and layering graffiti primitives", *Proceedings of the 8th Acm/Eurographics Expressive Symposium on Computational Aesthetics and Sketch Based Interfaces and Modeling and Non-Photorealistic Animation and Rendering*, Genoa, Italy: Eurographics Association, pp. 51-59.

BERIO D., CALINON S. & LEYMARIE F. F. (2016), "Learning dynamic graffiti strokes with a compliant robot", *Proceedings* of IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), Daejeon, Korea, pp. 3981-3986.

BERIO D., CALINON S. & LEYMARIE F. F. (2017), "Generating calligraphic trajectories with model predictive control", *Proceedings of the 43rd Graphics Interface*, Edmonton, Canada, pp. 132-139.

BERIO D., CALINON S. & LEYMARIE F. F. (2017), "Dynamic graffiti stylisation with stochastic optimal control", *ACM Proceedings of the 4th International Conference on Movement and Computing*, 18, London, UK.

BERIO D., LEYMARIE F. F. & CALINON S. (2020), "Interactive generation of calligraphic trajectories from gaussian mixtures", *in* BOUGUILA N. & FAN W. (éd.) *Mixture Models and Applications*, Unsupervised and Semi-Supervised Learning Series, Springer, pp. 23-38.

BERIO D. & LEYMARIE F. F. (2015), "Computational models for the analysis and synthesis of graffiti tag strokes", *in* ROSIN P. (éd.) *Computational Aesthetics (Cae)*, Eurographics Association, pp. 35-47.

BERIO D., LEYMARIE F. F. & PLAMONDON R. (2018), "Expressive curve editing with the sigma lognormal model", *Proceedings of the 39th Annual European Association for Computer Graphics Conference: Short Papers*, Eurographics Association, pp. 33-36.

BERIO D., LEYMARIE F. F. & PLAMONDON R. (2020), "Kinematics reconstruction of static calligraphic traces from curvilinear shape features", *in* PLAMONDON R., MARCELLI A. & FERRER M. A. (éd.) *The Lognormality Principle and its Applications in e-Security, e-Learning and e-Health*, World Scientific, chapter 11, pp. 237-268.

BESSETTE J., LEYMARIE F. F., and SMITH G. (2019), "Trends and anti-trends in techno-art scholarship", *Arts,* 8(3).

BROAD T. & GRIERSON M. (2017), "Autoencoding Blade Runner: Reconstructing films with artificial neural networks", *Leonardo*, 50(4), pp. 376-83.

BROAD T. & GRIERSON M. (2019), "Searching for an (un)stable equilibrium: Experiments in training generative models without data", *Proceedings of the Neurips Workshop on Machine Learning for Creativity and Design*, Vancouver, Canada.

BROAD T., LEYMARIE F. F. & GRIERSON M. (2020a), "Amplifying the uncanny", *in* VERDICCHIO M., CARVALHAIS M., RUIBAS L. & RANGEL A. (éd.) *Proceedings of the 8th Conference on Computation, Communication, Aesthetics and X (xCoAx)*, https ://proceedings.xcoax.org/.

BROAD T., LEYMARIE F. F. & GRIERSON M. (2020b), "Network bending: Manipulating the inner representations of deep generative models", Goldsmiths, University of London.

CALINON S. & LEE D. (2019), "Learning control", *in* VADAKKEPAT P. & GOSWAMI AA. (éd.) *Humanoid Robotics: A Reference*, Springer, pp. 1261-1312, https ://doi.org/10.1007/978-94-007-6046-2_68

DAMASIO A. R. (1994), *Descartes' Error: Emotion, Reason and the Human Brain*, Grosset Putnam.

FERRI A. (2016), *Teoria Del Writing, La Ricerca Dello Stile*, Professional Dreamers.

FREEDBERG D. & GALLESE V. (2007), "Motion, emotion and empathy in aesthetic experience", *Trends in Cognitive Sciences,* 11(5), pp. 197-203.

GOLOMB C. (1994), "Drawing as representation: The child's acquisition of a meaningful graphic language", *Visual Arts Research,* 20(2), pp. 14-28, http ://www.jstor.org/stable/20715828.

HERTZMANN A. (2020), "Visual Indeterminacy in GAN Art", *Leonardo,* 53(4), pp. 424-428.

HEY T. & PÁPAY G. (2014), *The Computing Universe: A Journey Through a Revolution*, Cambridge University Press.

HOFFMAN . D., SINGH M. & PRAKASH C. (2015), "The interface theory of perception", *Psychonomic Bulletin and Review,* 22(6), pp. 1480-1506.

KAO H. S. R.,van GALEN G. P. & HOOSAIN R. (1986), *Graphonomics: Contemporary Research in Handwriting*, Advances in Psychology, 37, Elsevier.

KARNOUSKOS S. (2020), "Artificial intelligence in digital media: The era of deepfakes", *IEEE Transactions on Technology and Society,* 1(3), pp. 138-147.

KLUSZCZYŃSKI R. W. (2016), *Patrick Tresset: Human Traits and the Art of Creative Machines*, Laznia Centre for Contemporary Art, Gdańsk, Poland.

KOENDERINK J. J. (2019), "Vision, an optical user interface", *Perception,* 48(7), pp. 545-601.

LAMBERT N., LATHAM W. & LEYMARIE F. F. (2013), "The emergence and growth of evolutionary art — 1980-1993", *Leonardo,* 46(4), pp. 367-375, http ://doi.org/10.1162/LEON_a_00608

LATHAM W., TODD S., TODD P. & PUTNAM L. (2021), "Exhibiting mutator VR: Procedural art evolves to virtual reality", *Leonardo*, pp. 1-14, https://doi.org/10.1162/leon_a_01857

LEDER H., BÄR S. & TOPOLINSKI S. (2012), "Covert painting simulations influence aesthetic appreciation of artworks", *Psychological Science,* 23(12), pp. 1479-1481.

LEVIN M. (2019), "The computational boundary of a "self": Developmental bioelectricity drives multicellularity and scale-free cognition", *Frontiers in Psychology,* 10:2688.

LEYMARIE F. F. (2011), "On the visual perception of shape: Analysis and genesis through information models", *Proceedings of the SHAPES 1.0 Workshop*, Karlsruhe, Germany, CEUR-WS.org.

MAARSE F. J., van GALEN G. P. & THOMASSEN A. J. W. M. (1989), "Models for the generation of writing units in handwriting under variation of size, slant, and orientation", *Human Movement Science,* 8(3), pp. 271-288.

MADDOX-HARLE R. (2017), "Review of 'Patrick Tresset: Human traits and the art of creative machine'", *Leonardo*.

McCARTHY J., MINSKY M. L., ROCHESTER N. & SHANNON C. E. (2006), "A proposal for the dartmouth summer research project on artificial intelligence, August 31, 1955", *AI Magazine* 27.

MORI M. (1970), "The uncanny valley", *Energy,* 7(4), pp. 33-35.

PIGNOCCHI A. (2010), "How the intentions of the draftsman shape perception of a drawing", *Consciousness and Cognition,* 19(4), pp. 887-898.

PLAMONDON R. (1995), "A kinematic theory of rapid human movements. Part I. Movement representation and generation", *Biological Cybernetics,* 72(4), pp. 295-307.

ROBERSON D., DAVIDOFF J., DAVIES I. R. L. & SHAPIRO L. R. (2006), "Colour categories and category acquisition in Himba and English", *in* PITCHFORD N. & BIGGAM C. P. (éd.) *Progress in Colour Studies: Volume II. Psychological Aspects*, John Benjamins publishing, pp. 159-172.

TEULINGS H.-L. (1996), "Handwriting movement control", *Handbook of Perception and Action,* 2, pp. 561-613.

TODD S. & LATHAM W. (1992), *Evolutionary Art and Computers*, Academic Press.

TRESSET P. & LEYMARIE F. F. (2005), "Generative portrait sketching", *in* TWAITES H. (éd.) *Proceedings of the 11th International Conference on Virtual Systems and Multimedia (Vsmm)*, Ghent, Belgium, pp. 739-748.

TRESSET P. & LEYMARIE F. F. (2006), "AIKON: The artistic/automatic IKONograph", *SIGGRAPH Research Posters*, 37, Boston, MA, USA, ACM.

TRESSET P. & LEYMARIE F. F. (2012), "Sketches by Paul the robot", in CUNNINGHAM D. & HOUSE D. (éd.) *Computational Aesthetics in Graphics, Visualization, and Imaging*, The Eurographics Association, http://dx.doi.org/10.2312/COMPAESTH/COMPAESTH12/017-024.

TRESSET P. & LEYMARIE F. F. (2013), "Portrait drawing by Paul the robot", *Computers and Graphics,* 37(5), pp. 348-363.

TURING A. M. (1950), "Computing machinery and intelligence" *Mind,* LIX(236), pp. 433-460.

Résumés

Abstracts

seeing, thinking and acting formed during the individual's socialization) with a context that actualizes them. As a survey of persons who regularly drive for Blablacar shows, these drivers thus developed a mental disposition for thrift or even asceticism, along with relational skills and, sometimes, even an appreciation of "others". During a period of social vulnerability with their status at stake, these drivers turned to ride-sharing, a practice that someone close to them had brought to their attention and encouraged. For this sharing to last, these dispositions, which have a weak basis, must be reinforced.

On 16 March 2020, educators had to respond to the closing of schools in France on account of the pandemic, an exceptional event with an impact on 12 million pupils, more than 20 million parents, 800,000 teachers and 400,000 employees of the Ministry of National Education. The response to this emergency and to the expectations of these various parties was a massive shift toward digital technology and its resources, such as the educational material proposed by the ministry, its agents and partners (e.g., the CNED's "Ma classe à la maison" or the ENT's "Espaces numériques de travail"). This articulation (specific to France) of public policies about digital technology with support from a multitude of actors proved to be relatively effective, as attested by the OECD, which cited France as one of the best organized countries that provided for continuous schooling. This review of feedback from this experience during the pandemic identifies axes for the development of a digital culture shared by a system of education in movement.

Faced with the wide variety of security products (firewalls, VPNs, etc.), users sometimes feel helpless. How to know which are the best? The security certifications made in France under ANSSI's supervision are based on an objective, duplicable assessment. They are one answer to this question, at least for products (such as debit/credit cards) with highly standardized features. Although this process offers a widely recognized, serious warrant of security, it relies on procedures worked out about twenty years ago and is not really adapted for products that offer a higher level of security. The European certification process now being rolled out will eventually replace national assessment procedures. It seeks to broaden the scope of certification so as to allow for assessments of everyday devices and take into account a product's full life cycle.

The security of everyday uses of software is a key question, whether in transportation (automobile, airplanes, trains) or the health sector. However this question has gone unanswered for systems that incorporate artificial intelligence (AI). A key for coming up with an answer is to work out ethical guidelines for building trust by defining a set of shared requirements. Before implementing these requirements and, too, the requirements related to specific applications and their use cases, a technical framework must be set up to review the whole AI chain from design through assessments to rollout. This means both developing the software bricks for algorithmic engineering and AI systems, and

occurred, and all sectors, actors and citizens have now been swept into the digital era. Digital "integration" and identification are major issues for our society. The role of local authorities is the cornerstone for a "humane smart city" open to everyone.

Miscellany

82 Art.Machine.Intelligence

Frederic Fol LEYMARIE

I will present some thoughts about the potentials that lie at the intersection of art, machines (including AI) and intelligence. I wish not simply to give an overview of today's practice by artists using, or sometimes developing, some aspects of the use of machines in their practice, but rather discuss why there is great potential in the mixing of these disciplines.
To do so, I will characterize each of the three topics. My descriptions of these topics will be far from complete overviews, but sufficient I hope to make clear how I consider the potentials offered by considering the junction or fusion of the 3 topics of "art", "machines" and "intelligence". I will give also some recent and current examples practices and projects of artists I have engaged with, where the 3 disciplines are brought together, as a short overview.
Finally, I suggest that rather than fixate on General Artificial Intelligence, we ought to rather focus on more reasonable objectives such as Art.Machine.Intelligence.

Ont contribué à ce numéro

Serge ABITEBOUL est depuis 2018 membre du collège de l'Arcep (autorité de régulation des communications électroniques, de la poste, et de la distribution de la presse). Il est chercheur à l'Inria et l'ENS à Paris.
Serge Abiteboul a obtenu son doctorat de l'Université de Southern Californie, et une thèse d'État de l'Université de Paris-Sud. Il est chercheur à l'Institut national de recherche en informatique et automatique depuis 1982, directeur de recherche émérite depuis 2019, et, depuis 2016, dans une équipe de recherche de l'École normale supérieure de Paris. Il a été maître de conférences à l'École polytechnique, professeur invité à Stanford et Oxford University, et professeur affilié à l'École normale supérieure de Cachan. Il a été détenteur de la chaire Informatique et sciences numériques au Collège de France en 2011-2012 et de la chaire Francqui à l'Université de Namur en 2012-2013. Il a cofondé la société Xyleme en 2000. Il a reçu le prix de l'innovation ACM SIGMOD en 1998, le prix EADS de l'Académie française des sciences en 2007, le prix Milner de la Royal Society en 2013, et une bourse du Conseil européen de la recherche (2008-2013). Il est devenu membre de l'Académie des sciences de France en 2008, et membre de l'Académie de l'Europe en 2011. Il a été membre du Conseil national du numérique (2013-2016) et président du conseil scientifique de la Société d'informatique de France (2013-2015). Il est, depuis 1917, président du conseil stratégique de la Fondation Blaise Pascal. Ses travaux de recherche portent principalement sur les données, la gestion de l'information et des connaissances, en particulier sur le *web*.
Serge Abiteboul écrit également des romans, des essais, et est éditeur et fondateur du Blog binaire. Il a été commissaire de l'exposition Terra Data à la Cité des sciences en 2017-2018.
→ ***Qualité, équité, transparence, vérification et explicabilité des décisions algorithmiques***

Maryse ARTIGUELONG est consultante informatique retraitée, vice-présidente de la Ligue des droits de l'homme (LDH) depuis 2017 et vice-présidente de la Fédération internationale des droits de l'homme (FIDH) depuis 2016.
Elle assure l'animation du groupe de travail « Libertés & Technologies de l'information et de la communication » de la LDH et le pilotage politique de différents projets européens transnationaux portant sur la protection des données personnelles (« jeunes et internet » avec la réalisation d'une bande dessinée, « fichage institutionnel » avec la réalisation d'un « passeport » sur les fichiers), la réalisation pour la LDH de différents mini-guides sur le numérique et la vie privée (vidéosurveillance, citoyenneté et numérique, jeunes et réseaux sociaux).
Elle est membre du « Groupe de contacts » du Conseil d'État pour l'étude annuelle 2014, « Le numérique et les droits fondamentaux ».
Elle participe au titre de la LDH à différents travaux de la Commission nationale consultative des droits de l'homme (CNCDH) pour certains avis, notamment : la lutte contre les discours de haine sur Internet ; la loi contre la corruption et la protection des lanceurs d'alerte ; la « Protection de la vie privée à l'ère numérique » ; la proposition de loi visant à lutter contre la haine sur Internet ; le suivi numérique des personnes.
Elle contribue en tant qu'observateur aux travaux du bureau de la convention 108 du Conseil de l'Europe.
→ ***Perspective historique sur la liberté d'expression***

Bruno BAGARRY est psychologue, psychothérapeute et psychanalyste en libéral et en institution. Il intervient au sein de centres médicaux psychologiques et associations de santé. Membre des séminaires psychanalytiques de Paris et d'espace analytique, il encadre des groupes cliniques et participe à des cartels de recherche. Il assure la supervision individuelle et collective de cliniciens et psychanalystes. En tant que conférencier, son enseignement se consacre principalement à la psychanalyse et à la psychopathologie.
Il est également formé à des techniques psychothérapiques telles que l'Analyse transactionnelle (EAT et ATORG), l'EMDR (Institut français d'EMDR), l'hypnose (Hypnodyssey - Jean Becchio) et la Gestalt (EPG). Il est psychologue du travail (CNAM) et *coach* certifié de l'Académie du coaching. Il a occupé des fonctions de direction de services culturels et de ressources humaines au sein de collectivités territoriales et d'organismes privés.
→ ***Les ressorts de la confiance***

Côme BERBAIN est directeur de l'innovation du groupe RATP et directeur du programme « Véhicule autonome ». Ingénieur du corps des Mines, docteur en cryptographie, son parcours alterne entre entités privées (Orange, Trusted Logic) et publiques (ministère de la Défense, ANSSI, direction interministérielle du numérique) dans les domaines de la transformation numérique et de la cybersécurité. En 2017 et 2018 il est conseiller au cabinet du secrétaire d'État chargé de la Transition numérique, où il porte les sujets de transformation numérique de l'État et de confiance numérique, avant de devenir Chief Technology Officer de l'État à la direction interministérielle du numérique en 2019. Il rejoint la RATP en novembre 2019.
→ ***Introduction***

Mathilde BRAS est experte de la transformation numérique de l'action publique. Passionnée des enjeux sociopolitiques du numérique, Mathilde Bras débute sa carrière en tant que rapporteur au sein du Conseil national du numérique, de 2013 à 2016. Elle contribue à l'élaboration de plusieurs rapports, sur la fiscalité, les politiques commerciales, la transformation du travail et de l'activité. Elle a activement participé à la coordination de la concertation « Ambition numérique », préparatoire à la loi pour une République numérique. En 2016, elle rejoint Etalab, département de la direction interministérielle du numérique, où elle coordonne les actions de gouvernement ouvert au niveau national et dirige de 2017 à 2020 le programme « Entrepreneurs d'intérêt général », qui consiste à rapprocher les métiers du numérique de ceux du service public et à former une nouvelle génération de talents au sein de l'administration. Engagée pour le numérique d'intérêt général, Mathilde Bras est trésorière de la Fabrique des Mobilités, association visant à accélérer l'innovation ouverte dans les nouvelles mobilités. Elle est également membre de la Fondation internet nouvelle génération, qui conduit des actions en faveur de la convergence des transitions numérique et écologique, et apporte son expertise auprès d'administrations, en France et à l'étranger.
→ ***Le rôle des communautés (open source, open data, open gov)***

Fabien CAPARROS, capitaine de frégate, est le chef de l'état-major de la sous-direction Stratégie, au sein de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Son expérience opérationnelle d'officier de marine et ses compétences d'ingénieur en cybersécurité l'ont amené à s'intéresser tout particulièrement aux problématiques de gestion des risques numériques. Au cours des quatre dernières années, il a dirigé l'élaboration d'un *corpus* doctrinal et méthodologique de haut niveau au profit des entreprises et des administrations. Il est notamment le coauteur de la méthode d'analyse des risques numériques EBIOS Risk manager.
Fabien Caparros est ingénieur de l'École navale. Il est également diplômé d'un mastère spécialisé en réseau et télécommunication militaire et d'un Global Executive MBA de l'école de commerce KEDGE Business School.
→ ***L'atout confiance***
Maîtriser le risque numérique pour construire la cyber-résilience

Julien CHIARONI est directeur du grand défi sur la « sécurisation, la fiabilisation et la certification des systèmes à base d'intelligence artificielle », financé par le Conseil français de l›innovation. Auparavant, il était directeur de la stratégie et des programmes au List, institut du CEA sur les technologies du numérique et l'intelligence artificielle, avec plus de 700 chercheurs sur ces thématiques. Avant cela, il a occupé des postes opérationnels à responsabilités croissantes, tant scientifiques que managériales, au Leti puis à la Direction de la recherche technologique du CEA, et contribué à de nombreux projets partenariaux de recherche, notamment à vocation de transfert à l'industrie, dans le domaine du numérique. Responsable de programme de 2008 à 2010, il coordonne le programme nanosciences et nanotechnologies de l'Agence nationale de la recherche (ANR). Au service de l'État à l'étranger de 2010 à 2012, Julien Chiaroni occupe les fonctions d'attaché de coopération scientifique et universitaire au consulat de France à Hong Kong et Macao. Julien Chiaroni est ingénieur diplômé de l'ENSPG (Phelma), d'un master recherche en matériaux de Grenoble-INP et d'un mastère spécialisé en « Humanités Digitales » de Sciences Po.
→ ***Vers la confiance, voire la certification, des systèmes à base d'intelligence artificielle***

Josette DEBROUX est maîtresse de conférences en sociologie à l'Université Lyon 2. Elle est membre de l'équipe « Modes, espaces et processus de socialisation » du Centre Max Weber (UMR 5283). Ses travaux récents s'intéressent aux rapports entre mobilité sociale et mobilité spatiale, et plus particulièrement aux mobilités résidentielles vers l'espace rural isolé et vers les zones périurbaines. L'objectif de ses travaux est de montrer que les « choix » de localisation résidentielle prennent sens au regard de la socialisation familiale, de la trajectoire sociale. Ils montrent également que les manières d'habiter ou d'investir tel ou tel espace s'articulent avec d'autres formes d'investissement dans d'autres sphères (à l'exemple de la sphère professionnelle) et analysent en retour les effets des expériences socialisatrices résidentielles sur les trajectoires et les identités sociales. Josette Debroux travaille, par ailleurs, sur le covoiturage entre inconnus et s'intéresse plus particulièrement aux dispositions sociales qui favorisent l'engagement dans cette pratique. Elle participe à une recherche collective en cours sur les relations de voisinage.
Bibliographie (sélection) :
(2018), « Les ressorts de l'engagement dans une pratique de consommation collaborative. Le cas des conducteurs d'une plateforme de covoiturage », *L'homme et la société*,207(2), L'Harmattan, pp. 187-217.

(2013), « S'assurer une position résidentielle en zone périurbaine : des pratiques résidentielles marquées par l'origine, la trajectoire sociale et les perspectives de mobilité professionnelle », *Regards sociologiques*, n°45/45, pp. 209-223.
(2011), « Stratégies résidentielles et position sociale : l'exemple des localisations périurbaines », *Espaces et sociétés*, n°144-145, pp. 121-139.
(2003), « La dynamique complexe des migrations d'actifs vers l'espace rural isolé », *Espaces et sociétés*, n°113/144, pp. 215/232.
→ ***L'engagement dans une pratique collaborative : une question de « confiance » ?***

Marie-Laure DENIS est diplômée de l'Institut d'études politiques de Paris en 1988, ancienne élève de l'École nationale d'administration (promotion « Condorcet »). Elle a été auditrice de 1992 à 1995, puis maître des requêtes de 1998 à 2002 au Conseil d'État. De 2017 à 2019, elle était Conseiller d'État, rapporteur à la 6e chambre de la Section du contentieux et membre de la Section du rapport et des études.
Marie-Laure Denis a été directrice adjointe du cabinet du maire de Paris de 1996 à 1998, et directrice du cabinet du ministre délégué à la Famille et directrice adjointe du cabinet du ministre de la Santé, de la Famille et des Personnes handicapées de 2002 à 2004. Elle a été membre du CSA (conseil supérieur de l'audiovisuel) de 2004 à 2011, puis membre de l'ARCEP (autorité de régulation des communications électroniques et des postes) de 2011 à 2016. De 2017 à 2019, elle était membre du CORDIS (comité de règlement des différends et des sanctions) de la commission de régulation de l'énergie (CRE). Elle a été nommée présidente de la CNIL à compter du 2 février 2019.
→ ***RGPD, trois ans après, où en est-on ?***

Henri ISAAC, docteur en sciences de gestion, est maître de conférences à PSL, Université Paris-Dauphine, et chercheur au sein de Dauphine Recherches en Management (CNRS, UMR 7088). Il a été directeur de la Recherche et directeur académique à Neoma Business School (2009-2012), et vice-président « Transformation numérique » de l'Université Paris-Dauphine (2014-2016). Il dirige le parcours management télécoms et médias du Master « Systèmes, Information, Réseaux, Numérique ». Il est président du Think Tank Renaissance Numérique.
Auteur de plusieurs ouvrages, *Modèles d'affaires des plateformes* (Vuibert, 2021, à paraître), *E-commerce. Vers le commerce connecté* (4ème édition, 2017, Pearson France), et co-auteur de *Marketing digital* (7ème édition, 2020, Pearson), il a également publié de nombreux articles dans des revues académiques comme *Journal of Business Strategy, European Journal of Information Systems*, *International Journal of Innovation and Technology Management*, *International Journal of Mobile Communications*, *Revue Française du Marketing*, *Système d'Information & Management*, *Revue Française de Gestion*.
→ ***Numérique et confiance***

Clément JEANNEAU est le cofondateur de Blockchain Partner, *leader* français du conseil stratégique et technique sur les technologies *blockchain*. Son équipe a notamment conçu la première *blockchain* française d'État, auprès de l'Agence nationale des fréquences, et a accompagné la Banque de France dans la réalisation de la première application *blockchain* mise en production par une banque centrale dans le monde.
Au-delà de ces technologies, il conseille les acteurs publics et privés sur les questions de prospective, liées ou non au numérique. Il est l'auteur du rapport « L'Âge du web décentralisé » (Fondation Digital New Deal), du site SignauxFaibles.co dédié aux mouvements émergents, et de la *newsletter* « Nourritures terrestres » qui explore les enjeux de la transition écologique.
→ ***Blockchain : quelle confiance, pour quels usages ?***

Renaud LABELLE est ancien élève de l'École polytechnique et de l'école nationale supérieure des télécommunications, et ingénieur général des Mines.
À partir de 1999, il réalise une première partie de sa carrière au ministère des Armées. Il y occupe différentes fonctions dans les domaines des télécommunications et de la sécurité des systèmes d'information (notamment en cryptographie) : expert, responsable d'équipes de différentes tailles (entre 10 et 140 personnes), conseiller et directeur de programme.
Il rejoint l'ANSSI en février 2018, pour occuper le poste d'adjoint du sous-directeur Expertise, la sous-direction qui regroupe notamment les laboratoires de recherche en sécurité des systèmes d'information, les experts en charge de l'assistance aux ministères et aux entreprises critiques, et le centre de certification national. Il en devient le sous-directeur en juillet 2020.
→ ***La certification de produits fonctionne-t-elle ?***

Alain LACABARATS est président de chambre honoraire à la Cour de cassation.
Il a dirigé le service de documentation et d'études de la Cour de cassation de 2004 à 2009, puis a présidé successivement la troisième chambre civile de cette Cour de 2009 à 2011, puis la chambre sociale de 2011 à 2014.
Il a été membre du Conseil supérieur de la magistrature de 2015 à 2019.
Il a présidé le Conseil consultatif de juges européens, organe consultatif du Conseil de l'Europe pour les questions de statut des juges et de fonctionnement des systèmes judiciaires.
Membre du comité d'experts de l'Organisation internationale du travail, il participe également aux travaux de plusieurs comités de déontologie (ministères sociaux, juridictions financières, collèges de déontologie des Jeux olympiques Paris 2024 et de la SOLIDEO), et est conciliateur au Comité national olympique et sportif français.
→ ***La procédure et la confiance des citoyens en la justice à l'épreuve de la dématérialisation***

Henri LECLERC a été avocat pénaliste de 1955 jusqu'en décembre 2020.
D'abord collaborateur du grand avocat Albert Naud, secrétaire de la Conférence, il est intervenu dans de nombreuses causes criminelles très médiatisées et de grands procès de presse. Il a été membre du Bureau national du PSU à la fin des années 1960, membre de commissions de réforme pénale, notamment la commission Justice pénale et Droits de l'Homme présidée en 1990 par Mireille Delmas-Marty.
Henri Leclerc a plaidé cinq fois contre la peine de mort. Aucun de ses clients n'a été condamné à mort. Dans ses mémoires, il rappelle que « c'est l'homme qu'on défend, celui qui est accusé d'avoir commis le crime » et non le crime. « Alors, il y a plusieurs cas de figure, » poursuit-il. « Il peut être innocent et là c'est très lourd, mais il peut être coupable. S'il est coupable, il a le droit d'être défendu, c'est-à-dire que l'avocat est celui qui ne va pas crier avec les autres. L'avocat est justement cette espèce de voix contradictoire : il va permettre, à un moment donné, à la justice de passer. »
Avocat du journal *Libération* de 1973 à 2006, il est devenu un spécialiste du droit de la presse et de la liberté d'expression. Il a toujours cherché à faire respecter la délicate équation de concilier le devoir d'informer et la recherche de la vérité avec le respect du droit et la légitime protection des individus.
Il a été président de la Ligue des droits de l'homme (LDH) de 1995 à 2000, il en est président d'honneur depuis 2000.
Il est l'auteur de :
- (2017), *La Parole et l'Action*, Fayard.
- (2005), *Le Code pénal,* Édition du Seuil
- (1994), *Un combat pour la justice*, Éditions La Découverte

Il est coauteur de :
- (2002) avec FRIDMAN W.-H., *La Défense*, Éditeur EDP SCIENCES
- (1996) avec THÉOLLEYRE J.-M., *Les Médias et la justice*, CFPJ

Il apparaît dans l'ouvrage :
- PERRIN C. & GAUNE L. (2010), *Parcours d'avocat(e)s*, Éditions du Cavalier bleu

→ ***Perspective historique sur la liberté d'expression***

Sylvain LEROY est ancien élève de l'École polytechnique et de l'école nationale supérieure des télécommunications, et ingénieur en chef des Mines.
Après un début de carrière en 2004 au sein du ministère de l'Économie, des Finances et de l'Industrie, il rejoint l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en 2009. Entre affaires européennes, relations industrielles et contrôle réglementaire, Sylvain Leroy a occupé différents postes au sein de l'ANSSI.
Il exerce la fonction de chef de division Produits et Services de sécurité depuis novembre 2019. Il est également représentant de la France à l'ECCG (European Cybersecurity Certifcation Group).
→ ***La certification de produits fonctionne-t-elle ?***

Frederic Fol LEYMARIE est professeur au Goldsmith College de l'Université de Londres. Il est fasciné par la façon dont nous percevons le monde, en particulier en ce qui concerne les dimensions visuelles, ce qui l'a conduit à travailler dans quelques domaines de recherche et d'applications, notamment : la vision, le graphisme, la robotique appliquée, les visualisations scientifiques, la mise sous forme de jeux informatiques de connaissances scientifiques. En parallèle, il collabore depuis deux décennies avec des artistes du monde des arts visuels dans le but de mieux comprendre leur *modus operandi*.
→ ***Art.Machines.Intelligence***

Jean-Marc MERRIAUX, inspecteur général de l'éducation, du sport et de la recherche, est directeur du numérique pour l'éducation (DNE) au sein du ministère de l'Éducation nationale, de la Jeunesse et des Sports. La direction du numérique pour l'éducation intègre aussi bien les enjeux de pilotage que les enjeux du numérique éducatif. Il a été auparavant directeur général du CNDP qu'il a transformé en Réseau Canopé, opérateur du ministère chargé de l'éducation, sur les enjeux de la formation des enseignants par le numérique, de la production de ressources pour accompagner les pratiques pédagogiques, le développement de la médiation numérique à travers des outils et des services développés au sein des ateliers Canopé. Il a une expérience de plus de 15 ans dans les questions en lien avec le numérique et l'éducation. Il a débuté sa carrière au sein de la Cinquième aujourd'hui France 5 (chaîne du savoir et la connaissance), où il a été successivement conseiller éditorial sur les programmes éducatifs, secrétaire général de l'antenne, directeur adjoint de l'antenne et des programmes, directeur délégué de l'antenne, de France 5, et directeur du département éducation du groupe France Télévisions. Il a une formation universitaire en économétrie et en économie industrielle avec une spécialisation dans les industries culturelles et de communication.
→ ***Le numérique à l'école : la crise sanitaire, une opportunité pour développer une culture numérique***

Bertrand PAILHÈS est directeur des technologies et de l'innovation de la CNIL depuis novembre 2019.
Diplômé de Télécom Paris et de Sciences Po Paris, il a travaillé sur la refonte du plan national de numérotation et les marchés de l'interconnexion fixe à l'ARCEP (régulateur des télécoms), puis sur les technologies numériques à la CNIL (autorité de protection des données) avant d'intégrer, en 2013, le cabinet de la ministre déléguée aux PME, à l'Innovation et à l'Économie numérique, Fleur Pellerin, puis celui d'Axelle Lemaire, secrétaire d'État chargée du Numérique. En tant que directeur de cabinet à partir de 2015, il a notamment conduit l'adoption de la loi pour une République numérique en octobre 2016. Bertrand Pailhès a, par la suite, été coordinateur national pour la stratégie d'intelligence artificielle définie en 2018.
→ ***Introduction***

Valérie PÉNEAU est diplômée de l'IEP de Paris et ancienne élève de l'École nationale d'administration. Elle est inspectrice générale de l'administration. Elle est chargée depuis janvier 2018 par le ministre de l'Intérieur, le ministre de la Justice et le secrétaire d'État chargé de la Transition numérique, du programme interministériel France Identité Numérique, chargé de concevoir et de déployer le futur moyen d'identification électronique régalien sécurisé.
→ ***Prouver son identité en ligne : l'enjeu d'une solution régalienne de confiance***

Florence PRESSON est adjointe au maire de Sceaux (92), déléguée aux transitions et à l'économie circulaire et solidaire. Son parcours professionnel qui a débuté dans les années 1990 l'a placée au cœur d'une révolution particulière, celle du numérique, avec un changement radical qui s'opérait dans le monde industriel.
Elle est « slasheuse », avec l'expertise et l'expérience des domaines suivants : stratégie numérique et accompagnement au changement ; Human SmartCity et écocitoyenneté ; économie circulaire et solidaire ; transition énergétique ; nature comestible en ville, alimentation et transition environnementale.
Elle est membre du conseil d'administration et du bureau de l'Institut national de l'économie circulaire (INEC), membre des groupes de travail « numérique » et « développement durable » de l'Association des maires de France (AMF), personnalité qualifiée à la fondation Afnic et conspiratrice positive de l'Institut des Futurs souhaitables.
→ ***Inclusion numérique au cœur des politiques publiques***