INSTITUT DIDEROT

LES CARNETS DE L'INSTITUT DIDEROT

Les nouvelles lignes d'affrontement dans un monde numérisé : l'ère des frontières.com

Nicolas ARPAGIAN

INSTITUT DIDEROT // www.institutdiderot.fr / @InstitutDiderot

LES CARNETS DE L'INSTITUT DIDEROT

Les nouvelles lignes d'affrontement dans un monde numérisé : l'ère des frontières.com

Nicolas ARPAGIAN

JANVIER 2023

Sommaire

Avant-propos

« Frontières, limites, transitions et transgressions » : tel est le thème que le Conseil d'orientation de l'Institut Diderot a choisi pour l'année universitaire 2022-2023. Nous avions en effet le sentiment qu'un des traits caractéristiques de notre époque était que les frontières devenaient de plus en plus poreuses, les limites de plus en plus incertaines, les transitions de plus en plus nécessaires (spécialement en matière énergétique), les transgressions, selon les cas, de plus en plus fréquentes, tentantes ou inquiétantes. Ainsi avons-nous traité du climat et de la transition énergétique [1], de la question de l'hybridation, au sens propre ou métaphorique du mot [2], des OGM [3], des mouvements migratoires [4], des limites du savoir et de la vulgarisation scientifique [5], de la frontière entre le normal et le pathologique, spécialement s'agissant de la dépression [6], de l'usage et des limites des

1. Christian de Perthuis, *Changement climatique : comprendre et agir,* 2022.
2. Claudine Cohen, *Franchir les limites : transitions, transgressions, hybridations,* 2022.
3. George Freyssinet, *Les solutions apportées par les biotechnologies végétales,* 2022.
4. Catherine Wihtol de Wenden, *Migrations: un équilibre mondial à inventer,* 2022.
5. Étienne Klein, *La vulgarisation scientifique est-elle un échec ?,* 2022.
6. Hugo Bottemanne, *La dépression : le mal du siècle ?* (à paraître)

statistiques [7], des diverses communautés qui cohabitent dans notre pays [8], donc aussi du wokisme [9], des rapports entre les sexes ou les genres, donc du féminisme et de ses différents courants [10], mais aussi des transgenres [11], comme nous traiterons prochainement des transclasses [12], de l'avenir respectif de la droite et de la gauche [13], des rapports entre la croissance et le bonheur [14], enfin des limites de l'humanisme, voire de l'humanité [15].

Sur ce thème général, nous ne pouvions que rencontrer la révolution numérique, qui bouleverse si profondément les frontières et limites traditionnelles, que ce soit entre les États, entre les organisations, entre les communautés ou entre les individus. Nous avons demandé à Nicolas Arpagian, membre de notre Conseil d'orientation et éminent spécialiste de la cybersécurité, de nous aider à y réfléchir. Son dernier livre, *Frontières.com* (Éditions de L'Observatoire, 2022), sous-titré « *Numérique : comment survivre à la confusion qui vient ?* » nous a paru au cœur de notre sujet et de nos préoccupations. Merci à lui d'avoir bien voulu en résumer pour nous l'essentiel.

7. Dominique Deprins, *La statistique, de la fiction au réel* (à paraître)
8. Haïm Korsia, *L'avenir des juifs français,* 2022 ; Voir aussi Chems-eddine Mohamed Hafiz, *Manifeste contre le terrorisme islamiste,* 2022.
9. Jean-François Braunstein, *Les dangers du wokisme* (à paraître)
10. Caroline Fourest, *L'avenir du féminisme,* 2023.
11. Claude Habib, *Transgenres et conséquences* , 2022.
12. Chantal Jaquet, *Devenir transclasse : comment échapper aux destins déjà écrits ?*
13. Renaud Dély, *L'avenir de la gauche française* (à paraître) - (une autre rencontre est prévue sur l'avenir de la droite).
14. Claudia Sénik, *L'économie du bonheur : la croissance rend-t-elle les individus heureux ?*
15. Jean-Michel Besnier, *L'avenir du posthumanisme ou les limites de l'humain.*

Ce qu'il montre, et qui confirme notre intuition de départ, c'est d'abord que « le numérique rend les frontières poreuses ». Les trois composantes traditionnelles des États – un système juridique, une population, un territoire – sont de plus en plus traversées ou concurrencées par celles d'entreprises multinationales, à commencer par les GAFAM et autres géants du Web.

C'est vrai s'agissant du droit : les États « n'ont pas encore réussi à réglementer efficacement l'espace globalisé et interconnecté d'Internet », alors qu'à l'inverse « plusieurs entreprises produisent des dispositifs juridiques, soutenus par une puissance sans égale » et n'hésitent pas à intervenir dans le champ politique (voyez Twitter et Trump) ou même militaire (voyez Microsoft et l'Ukraine).

C'est le cas aussi s'agissant de la population. La généralisation du numérique fait que « n'importe qui peut tour à tour devenir contributeur, relais ou consommateur » de produits informationnels, ce qui réduit ou menace « certains privilèges d'État », comme l'établissement de l'identité des personnes, et aboutit à une hyperpersonnalisation, laquelle tend à enfermer chacun dans un profil établi, tout en réduisant sa capacité « de se projeter dans un récit collectif ». Nouveau danger pour nos démocraties : l'omniprésence du numérique renforce l'individualisme (au risque « d'effriter le lien social ») tout en menaçant les libertés individuelles.

Enfin, s'agissant du territoire, « l'un des effets majeurs du numérique est de déplacer le domaine d'exercice de

la souveraineté », qui dépend moins de la localisation des data centers que de la nationalité de leurs gestionnaires ou de celle, de plus en plus incertaine et invérifiable, des utilisateurs, si bien que « le numérique met en difficulté les logiques territoriales de l'État-nation ». Certains pays résistent pourtant efficacement à cette utopie « d'un monde interconnecté, fluide, interopérable », mais ce sont le plus souvent des États autoritaires, comme la Chine ou la Russie (« Internet, en Chine, n'est en fin de compte qu'un Intranet », intégralement contrôlé par le pouvoir politique). Cela met nos démocraties devant un défi considérable : comment faire pour que « la fluidité bienvenue du numérique » ne nous conduise pas, par ignorance ou naïveté, « à perdre la maîtrise de nos intérêts stratégiques et nos libertés individuelles » ?

Le débat, après l'exposé si riche de Nicolas Arpagian, a montré à quel point les enjeux sont cruciaux, que ce soit s'agissant des réseaux pédophiles, du terrorisme, de la cybersécurité ou de la cyberguerre. Cela vaut pour les États, pour les entreprises, mais tout autant pour les individus. Défendre les droits de l'homme, c'est aujourd'hui défendre aussi « les droits de *l'homo numericus* que nous sommes devenus ». Comment ? Bien sûr par la réglementation, quand elle est à la fois possible et nécessaire. Mais également et surtout par l'éducation : il s'agit de « faire en sorte que nous soyons des consommateurs-citoyens-électeurs exigeants et informés ». Cela suppose qu'on ne fasse pas trop confiance aux opérateurs, ni aux différentes applications, par exemple de messagerie ou de recherche, que nous utilisons tous les jours.

Quand je quittais ce jour-là les locaux de l'Institut Diderot, un mot m'est revenu, en l'occurrence en latin : *Caute* (« prends garde », « sois vigilant »). C'était la maxime de Spinoza, qui aimait trop la liberté pour ne pas se méfier de ceux qui ont intérêt à la réduire ou à la supprimer.

André Comte-Sponville
Directeur général de l'Institut Diderot

Les nouvelles lignes d'affrontement dans un monde numérisé : l'ère des frontières.com

Le numérique rend les frontières poreuses. C'est notamment vrai des frontières par excellence, celles des États. Ces derniers se caractérisent habituellement par trois composantes : un système de droit organisé, qui s'exerce sur une population rassemblée sur un territoire. Or, plusieurs grands acteurs du numérique sont aussi producteurs de normes, disposent d'une population – leurs utilisateurs – et d'un territoire, le cyberespace et leurs infrastructures informatiques. La puissance financière de ces firmes n'a en outre rien à envier à celle de nombreux gouvernements. Des actions réservées autrefois aux États sont dorénavant aussi le fait de tels acteurs non étatiques.

Cette porosité n'est pas nécessairement problématique en soi, à condition d'être lucides et informés à son sujet, de manière à ne pas la subir. Dès lors que nous sommes tous constamment connectés, il est vital d'avoir une meilleure connaissance du droit et de la technologie afin de pouvoir comprendre les spécificités de cet environnement numérique. Et reprendre une part de contrôle.

I. DROIT

Il faut le reconnaître, les États, malgré leurs efforts, ou peut-être parce qu'ils ne se sont pas mis en position d'aboutir, n'ont pas encore réussi à réglementer efficacement l'espace globalisé et interconnecté d'Internet. OCDE, Union européenne, ONU – par l'intermédiaire de l'UIT (Union internationale des télécommunications)… Toutes ces organisations ont essentiellement produit des déclarations et des concepts théoriques. Mais quand il s'est agi de passer à l'opérationnel, rien ne s'est vraiment produit de si concret, si ce n'est :

– La Convention de Budapest de 2001, instituée par le Conseil de l'Europe et initiée à l'origine pour lutter contre la pédocriminalité. Elle a mis en place une coopération au-delà de la seule entente régionale et à laquelle d'autres pays hors UE, les États-Unis par exemple, ont commencé à souscrire ;

– Le Règlement Général sur la Protection des Données (RGPD) de 2018, qui ne vaut qu'au seul niveau européen, avec en revanche une vraie production normative concernant les données personnelles. Il va de pair avec un autre texte moins connu, la directive NIS (de 2018, et sa version NIS2 en 2023), portant sur les « Opérateurs de Services Essentiels » : des sociétés pour lesquelles les États sont en droit d'imposer un cahier des charges en matière de sécurité numérique, au nom des intérêts supérieurs de la Nation. En France, on a ainsi défini douze secteurs d'activité, par exemple le traitement de l'eau,

l'énergie, l'alimentation, la banque, les télécoms, dont les principales entreprises ne sont pas autonomes en matière de politique de cybersécurité. Parce qu'une défaillance de leur part mettrait en péril l'ensemble du pays.

On s'est un peu facilement moqué de ces initiatives européennes – comme dit le dicton, les Européens régulent, les Chinois copient et les Américains créent. Cette production normative européenne a toutefois influencé un certain nombre de pays. Les États-Unis se sont inspirés de NIS en matière d'infrastructures critiques et la Chine a aussi réglementé dans ce domaine-là.

Toujours est-il que le droit international public est parcellaire dans les domaines du numérique, tandis qu'à l'inverse plusieurs entreprises produisent des dispositifs juridiques, soutenus par une puissance sans égale. Lorsque Facebook décide que le tableau *L'Origine du monde* de Gustave Courbet relève de la pornographie, et le supprime de l'ensemble de ses plateformes, alors que c'est une œuvre exposée au Musée d'Orsay, on voit bien qu'il s'agit de l'application d'une norme interne qui s'impose directement à plus d'un milliard d'individus. Lorsque Twitter décide de bannir le 45e Président des États-Unis, cela se fait à la suite d'une décision interne, sans magistrats, sans Cour d'appel, sans plaidoirie. Une entreprise décide de façon unilatérale qu'à partir de demain telle personne (à tort ou à raison, ce n'est pas le sujet) ne va plus pouvoir s'exprimer sur son réseau. De la même manière, quand Elon Musk, à la sollicitation de l'Ukraine, décide de déplacer la constellation Starlink

au-dessus de ce pays, on a un entrepreneur qui choisit d'intervenir hors du cadre habituel régissant les relations entre États.

Twitter ou Meta ont même commencé à se doter de juridictions internes, en faisant appel à des universitaires, d'anciens responsables gouvernementaux et même un Prix Nobel de la Paix (Tawakkol Karman). Une espèce de droit se construit, en interne, qui a vocation à remplacer ou suppléer les instances officielles. C'est inquiétant, au point que le 11 janvier 2023, dans le *Wall Street Journal*, Joe Biden, président des États-Unis d'Amérique, a signé une tribune demandant aux Républicains et aux Démocrates de s'unir contre les géants du numérique, (c'est le titre, *Unite against Big Tech abuses* [16]). De même, le très libéral *The Economist* avait appelé à réagir contre les BAADD (nos GAFAMs), ces entreprises à la fois *Big*, *Anticompetitive*, *Addictive* et *Destructive to Democracy*. Même ceux qui ont une acception libérale de l'économie s'interrogent donc, en sus de la question de la concurrence, sur le rôle de ces entreprises au-delà de leur stricte activité économique [17].

Ce rôle s'est notamment considérablement accru dans le domaine militaire, comme je l'ai déjà souligné au sujet de Starlink. L'audition par l'Assemblée nationale du général Aymeric Bonnemaison, chef d'État-major de la cyberdéfense française, en décembre 2022, est ainsi particulière-

16. https://www.wsj.com/articles/unite-against-big-tech-abuses-social-media-privacy-competition-antitrust-children-algorithm-11673439411
17. https://www.economist.com/leaders/2018/01/18/how-to-tame-the-tech-titans

ment éclairante [18]. On y apprend l'implication directe de grandes entreprises américaines dans le conflit ukrainien : Google et Microsoft. Dans ce second cas, le chiffrage irait pour cette dernière jusqu'à 100 millions de dollars et à une intervention allant au-delà de la mise à disposition d'infrastructures techniques, puisque Microsoft a assuré l'hébergement des données de l'État ukrainien, de manière à avoir une sauvegarde assurant sa continuité institutionnelle en cas de destruction des données, voire de perte de son territoire. Une entreprise privée a ainsi mis à disposition ses équipements en vue de garantir, en cas de besoin, le stockage et la sauvegarde numérique d'un État. Ajoutée à la mise à disposition de 100 millions de dollars, c'est une intervention politique majeure de la part d'une société privée, qu'on ne peut, je crois, comparer à un investissement pour vendre à terme des licences.

Cet activisme accru des acteurs du numérique en matière militaire apparaît aussi avec ce qui est la grande angoisse des défenses nationales : le prépositionnement, c'est-à-dire le déploiement d'éléments dormants numériques dans des organisations vitales, qui pourraient les faire dysfonctionner au commencement des hostilités.

Cet empiètement sur ce qui étaient des monopoles d'État se caractérise également dans l'espace numérique par le recours au cybermercenariat. Des professionnels aux activités crapuleuses se mettent ainsi ponctuellement

18. https://www.assemblee-nationale.fr/dyn/16/organes/commissions-permanentes/defense/actualites/conflit-ukrainien-audition-du-commandant-de-la-cyberdefense

au service des états-majors, pour des raisons idéologiques éventuellement, mais surtout pour des raisons d'intérêt bien compris. Puisqu'il faut bien à un moment avoir un pays où déposer son argent, le dépenser et vivre à l'abri des poursuites. Ces cybercriminels disposent ainsi d'une espèce de havre de paix où un gouvernement laisse s'embourber les procédures d'extradition les concernant avec, pour condition, de ne pas attaquer les ressortissants ou les entreprises dudit pays et de répondre aux requêtes de ce même État. L'avantage pour ce dernier étant d'avoir à disposition des experts très compétents et non officiels, dont ils pourront nier avoir une quelconque connaissance au cas où ils seraient découverts.

II. POPULATION

Dans le monde numérique, chose sans précédent, tout individu peut désormais, avec un équipement techniquement et financièrement accessible, à la fois recevoir des contenus, en produire, les relayer dans le monde entier de façon quasi instantanée, et les financer. Cela, qu'ils soient écrits, sonores ou filmés. C'est sans précédent, parce qu'auparavant, ces différentes dimensions étaient assez nettement séparées, avec quelques diffuseurs et beaucoup de destinataires, sur un modèle de gratuité avec de la publicité, type TF1, ou un modèle d'abonnement, à la façon de Canal Plus. L'abaissement des barrières technologiques et financières est tel que n'importe qui peut tour à tour désormais devenir contributeur, relais ou consommateur de ces produits informationnels.

C'est vrai, bien évidemment, de la diffusion de vidéos comme YouTube, mais aussi d'une multitude de services qu'auparavant seuls des experts en nombre limité pouvaient exploiter. Prenons deux exemples. Le premier défraie la chronique depuis novembre 2022 : ChatGPT. Que fait en fin de compte ce service ? Il consumérise un algorithme, c'est-à-dire qu'il le rend maniable et exploitable par n'importe quelle personne, qui lui attribuera éventuellement de nouvelles finalités et l'utilisera dans son quotidien… Ce n'est pas tant l'existence de l'outil qui crée la rupture mais bien sa mise à disposition au très grand public. C'est ce que fait ChatGPT ou ses équivalents, dans la conception d'images, de musiques ou de programmes informatiques, en présentant à terme l'accès au service sous la forme d'un simple onglet activable par tout un chacun, de manière à répondre à ses questions et à discuter avec lui. Notons, au passage, qu'un problème fondamental se pose à cette intelligence artificielle (IA) : par définition, elle ne peut exploiter que des contenus numérisés et mis en ligne. Ce qui n'a pas été numérisé et mis en ligne n'existe pas dans sa base de références. La question de la propriété intellectuelle des informations servant d'aliments à cette IA est en outre cruciale.

Le second exemple est la géolocalisation et le traçage d'autrui : auparavant apanage des services de renseignement avec des dispositifs d'écoute et de surveillance extrêmement complexes. Ces pratiques, illégales pour les personnes privées sans l'accord de ceux qui sont ainsi épiés, n'en sont pas moins fréquentes, grâce à des applications aujourd'hui facilement accessibles et utili-

sables par le très grand public. Les contentieux ès-affaires familiales regorgent de cas où de futurs ex-conjoints ont essayé de capter, grâce au numérique, des éléments pour pister leur partenaire.

Plus fondamentalement, certains privilèges d'État sont menacés par le numérique. C'est le cas d'un des plus importants d'entre eux : l'établissement de l'identité des personnes. Il est fréquent, désormais, quand vous voulez vous connecter à un nouveau service, qu'on vous demande soit de créer un compte, soit, plus rapidement et plus simplement, de vous inscrire avec votre compte Gmail ou Facebook. Qu'est-ce que cela signifie ? Qu'une entreprise, qui n'a rien à voir avec Facebook ou Google sur le plan comptable ou juridique, fait confiance à ces sociétés pour établir que l'utilisateur en ligne est bien celui qu'il prétend être. Certes, le gouvernement français a mis en place Franceconnect. Mais il n'en est pas moins concurrencé, et plutôt en retard, par rapport à ces grands acteurs de numérique. La question s'est même posée un temps de pouvoir payer ses impôts en se connectant avec son Gmail ou son compte Facebook.

Un autre exemple est la santé : l'État dispose d'organismes puissants (Agences Régionales de Santé, ministère de la Santé, INSERM…) mais finalement, durant la pandémie de Covid-19, c'est un jeune étudiant, Guillaume Rozier, à l'époque pas encore diplômé de Télécom Nancy, qui a trouvé une solution numérique pour mettre à disposition des autorités une photographie de l'état pandémique du pays.

Avec le numérique, des acteurs peuvent ainsi s'imposer sans passer par les institutions et les relais établis. Je pense par exemple à la diffusion du *Black Friday* en France : cette journée n'a aucun enracinement dans notre culture, mais par le biais des alertes et des notifications, elle connaît désormais un succès important, qui court-circuite complètement le système des semaines de soldes établies par des arrêtés préfectoraux. Idem pour *Halloween* désormais davantage inscrit dans la culture populaire que la traditionnelle fête de la Toussaint. TikTok est un autre exemple : sans aucune publicité, sous le radar des parents et des enseignants, cette application est devenue un phénomène de société chez les jeunes, en France et dans le monde. On en arrive à une situation où l'autorité normative, les adultes ou le législateur, ignore, ou en tout cas, n'apprend qu'avec beaucoup de retard, l'existence d'un environnement très rapidement investi par une masse considérable d'utilisateurs. La rapidité de diffusion et la masse d'informations passant désormais hors des règles et des canaux traditionnels de transmission sont impressionnantes.

En réponse, les États ont commencé à nommer des ambassadeurs en poste auprès des grands conglomérats du numérique. Comme s'il s'agissait de pays à part entière. En Corée du Sud, un diplomate avait ainsi pour responsabilité de suivre le compte Twitter de Donald J. Trump. Les États créent désormais des postes de diplomates dédiés à la représentation gouvernementale sur les sujets relatifs au cyberespace.

Une autre conséquence sans précédent du numérique sur la population est l'amplification de l'effet Dunning-Kruger. Étienne Klein en a beaucoup parlé, ici-même entre autres, concernant la pandémie de Covid-19 [19] : quelqu'un qui en a juste appris un peu sur un sujet ne le maîtrise pas suffisamment pour mesurer son ignorance et ce qu'il lui reste à apprendre. Il tend alors à surestimer sa maîtrise et à se croire habilité à se prononcer sur le domaine en question. Cela, alors qu'à l'inverse, quelqu'un qui a acquis un niveau intermédiaire, mesurant l'étendue de ce qu'il ne connaît pas encore, aura tendance à sous-estimer son niveau de compétence. On a ainsi vu des légions de gens donner leur avis sur la pandémie et les mesures à prendre, parce qu'ils avaient consulté trois sites Internet. Il en va de même pour de nombreux sujets. Le nucléaire, par exemple. Grâce à l'accessibilité de l'information en ligne, un individu peut désormais prétendre s'ériger au même niveau d'expertise qu'une autorité officielle, qui a produit du savoir documenté. C'est évidemment très déstabilisant : à partir du moment où vous morcelez les sources d'information, vous fragilisez l'ensemble de la structure, et des gens qui ont collecté des éléments disparates, à leur mesure, vont à leur tour produire du contenu et fragiliser encore plus l'information collective. C'est d'autant plus problématique que la diffusion de la connaissance, comme je le disais au sujet de ChatGPT, est de plus en plus confiée au numé-

19. *La vulgarisation scientifique est-elle un échec ?*, décembre 2021, consultable sur : https://www.institutdiderot.fr/les-publications-de-linstitut-diderot/la-vulgarisation-scientifique-est-elle-un-echec/.

rique, avec par conséquent des moyens de manipulation importants. À grande échelle, en termes de nombre de personnes concernées et de géographie. Comme le disait Orwell dans *1984*, « qui commande le passé, commande l'avenir » : si vous êtes capables de réexpliquer aux gens ce qui s'est passé avant, vous êtes en mesure de façonner leur manière d'aborder le monde ; et « qui commande le présent, commande le passé » : quand vous êtes en position d'autorité, vous maîtrisez les archives et vous pouvez donc tronquer, altérer, modifier le passé. Le problème, avec le numérique, étant qu'il peut se prêter à cette altération du passé, parce que le patrimoine se réduit au patrimoine numérisé, potentiellement manipulable ou effaçable.

Le grand risque, enfin, du numérique est le contrôle social à des niveaux jamais imaginés auparavant. Le profilage presque ultime des usages de l'individu aboutit au crédit social chinois, l'agglomération de l'ensemble de vos activités : traversez-vous dans les clous, donnez-vous votre sang, rédigez-vous des commentaires politiques défavorables sur les réseaux sociaux… ? Le résultat étant l'attribution d'une cote à la hausse ou à la baisse, avec des conséquences sur votre qualité de vie et l'accès à certaines prestations.

La géolocalisation est le cheval de Troie de ce contrôle. On parle sans cesse, en France, de *smart cities*, autrement dit, d'amélioration de la vie en milieu urbain grâce au numérique. Mais comment aboutit-on à cette optimisation ? Par le suivi des déplacements et des interactions,

afin « d'optimiser » l'ensemble. Un cas très intéressant est celui du projet de « Google City » lancé par Toronto en 2017. Cette ville avait demandé à Sidewalk Labs, filiale de Google/Alphabet, sur une zone d'à peu près cinq hectares, d'enregistrer tous les déplacements, 24 h sur 24 h, pour mieux comprendre comment la cité fonctionne. Et pour remonter en cas d'incidents, aux enchaînements de situations qui y ont conduit. Cela aurait permis, en retour, d'améliorer et d'automatiser les flux et les services : feux, déchets, éclairage, etc. Technologiquement et budgétairement, c'était faisable. Il s'avère que la gestionnaire du programme a avoué à un moment que, selon elle, c'était un outil de surveillance avant d'être un outil administratif de gestion publique administrative. Elle a démissionné, puis le confinement est venu, et le projet a été enterré. Mais l'idée était de descendre jusqu'au profilage de chaque individu. Avec, pour défense, l'idée que les pixels ne permettaient pas d'identifier les visages. Ce qui est évidemment dérisoire : si vous constatez que le même pixel prend une voiture de telle marque tous les matins pour aller au même endroit, en repart, etc., ce n'est pas très compliqué de l'identifier. D'autant plus qu'en l'occurrence Google dispose par ailleurs vraiment de tous les moyens pour croiser ses données et savoir *in fine* de qui il s'agit.

Ce profilage aboutit à une hyperpersonnalisation qui pourrait paraître séduisante, puisqu'elle aboutirait à vous proposer ce qui vous convient. Mais cette hyperpersonnalisation, en plus de vous enfermer dans un profil, affaiblit la capacité de se projeter dans un récit collectif.

On retrouve la grande crainte de Tocqueville dans *De la démocratie en Amérique* où celui-ci s'alarmait d'un individualisme aboutissant à ne plus se projeter que dans ce qu'il appelait « sa petite société ». Chacun ne voit pas au-delà de ses petits intérêts, avec évidemment une fragilisation du sentiment d'appartenance à la collectivité. La *res publica* est mise à mal, et ce qui inquiétait Tocqueville il y a bientôt deux siècles n'a jamais été aussi présent : l'hyperpersonnalisation risque d'effriter le lien social et la dégradation de ce liant est potentiellement déstabilisatrice.

III. TERRITOIRE

L'un des effets majeurs du numérique est de déplacer le domaine d'exercice de la souveraineté. Le territoire n'est plus une condition, nécessaire ou suffisante, de la souveraineté. Peu importe par exemple que tel centre de données (*data center*) se trouve sur votre territoire géographique ou non. C'est la nationalité de son gestionnaire qui compte. Ainsi, le droit étatsunien, largement extraterritorial, s'impose quand il s'agit de leur emploi dans des infrastructures soumises à la législation décidée à Washington.

Deuxième rupture : la notion d'origine géographique devient de plus en plus fragile étant donnée la diffusion des réseaux privés virtuels, les VPN. N'importe qui peut maintenant se connecter à un site en passant par ces VPN, qui permettent, le temps de la connexion, de

prétendre être localisé ailleurs dans le monde. Et ainsi endosser une grande diversité d'origines géographiques. Ce consumérisme de la nationalité fragilise évidemment les réglementations étatiques puisqu'un ressortissant peut toujours se faire passer pour un internaute venant d'un autre pays. Personne n'a établi à ce jour de solution robuste, notamment pour contrôler l'accès aux contenus pornographiques, interdits aux mineurs. Comment s'assurer que la personne devant l'écran est bien majeure ? Aucun pays n'a trouvé de réponse techniquement satisfaisante. On en reste pour l'instant à une simple déclaration de majorité, qui évidemment ne prouve rien. Les Britanniques ont voulu mettre en place un système de vérification, et ont finalement renoncé.

Enfin, de la même manière, le bannissement devient particulièrement difficile à mettre en œuvre. L'ARCOM peut bien interdire un site en France, mais les barrières techniques pour faire en sorte d'appliquer ces interdictions sont toutes relatives.

Droit, origine, bannissement : dans ces trois cas, on voit que le numérique met en difficulté les logiques territoriales de l'État-nation.

Cela ne signifie cependant pas que ces logiques territoriales disparaissent.

La loi russe impose ainsi que les données des ressortissants de la Fédération de Russie soient stockées dans ce pays. Ce qui a, par exemple, conduit un temps au blocage de LinkedIn, qui hésitait à se mettre en confor-

mité. Les États ne peuvent désormais faire l'impasse sur la question de savoir ce qu'ils pensent devoir se situer sur leur territoire national, et ce qu'ils peuvent laisser à des environnements techniques dont ils ne maîtrisent pas la localisation.

C'est un sujet majeur pour l'avenir : l'utopie originelle d'un monde interconnecté, fluide, interopérable, va-t-elle tenir devant la mainmise des États ? On voit des nations comme la Russie, la Chine, voire l'Inde, participer à la mise en place d'un splinternet, une balkanisation d'Internet, avec des îlots distincts régis strictement par les autorités nationales. Internet, en Chine, n'est en fin de compte qu'un Intranet. Comme dans une entreprise ou une administration, la direction centrale a une vue complète de ce qui se passe sur le réseau, parce qu'elle le détient, le gère et le maîtrise de bout en bout.

Le problème est que ce sont des États plutôt autoritaires qui engendrent cette dynamique, ce qui nous ramène aux questions du début, en matière de sécurité nationale. Les États démocratiques sont-ils capables de recruter les têtes bien faites dans ce domaine, sachant que la concurrence est très importante entre le public, le secteur privé et le monde criminel ? La question est d'autant plus aiguë que nous sommes dans un monde où encore plus qu'ailleurs, les lignes Maginot sont précaires : impossible de se dire que ce qu'on a construit l'est pour l'éternité, parce que tout change constamment, et très vite. C'est pour cette raison qu'il est vital

que les décideurs politiques [20], sans être des spécialistes, aient une meilleure culture numérique, une bonne connaissance de cet environnement, de manière à éviter les effets d'annonce caducs quelques semaines plus tard. La fluidité bienvenue du numérique ne doit pas nous conduire, par ignorance, à perdre la maîtrise de nos intérêts stratégiques et nos libertés individuelles.

* *
*

20. « L'Homo numericus devra être technologue, juriste et féru d'économie », Nicolas Arpagian, *Les Echos*, 9 octobre 2019.

Questions de la salle

Henri Cukierman [21] **:** *La lutte contre les réseaux pédophiles sur Internet a été, me semble-t-il, un grand succès. En revanche, j'ai l'impression que ça n'a pas marché pour d'autres causes, comme la lutte contre le terrorisme ou les discours de haine. Il m'intéresserait d'essayer de comprendre pourquoi ça marche dans un cas et pas dans d'autres.*

Nicolas Arpagian : Ce qui a fonctionné, c'est la production d'un texte, cette Convention de Budapest de 2001. Mais même là, il s'est passé plusieurs années, parfois plus de dix, avant que les États transposent l'accord dans leur droit national [22]. Cela, par crainte de perdre un peu de souveraineté puisqu'une fois le traité ratifié, il faut répondre aux sollicitations et partager du renseignement.

21. Président de la chambre de commerce France-Israël.

22. https://www.coe.int/fr/web/conventions/full-list?module=signatures-by-treaty&treatynum=185

Le problème, au niveau de l'Union européenne, c'est que les États restent concurrents entre eux dans de nombreux domaines, comme l'emploi ou la fiscalité. Ce qui les incite à conserver leur expertise IT/cyber en interne et à en limiter la mutualisation à l'échelle des 27. C'est le cas avec les agences nationales de cybersécurité (ANSSI, BSI…) tandis que l'échelon européen de l'ENISA ne dispose encore que de moyens très limités. Il y a certes Europol, mais ce n'est pas du tout un FBI européen, comme disent parfois les journalistes. Aux États-Unis, un policier fédéral est compétent sur l'ensemble des 50 États, avec un même système juridique, une même langue et une capacité d'intervention judiciaire du *Department of Justice*. Europol, c'est de la coopération, uniquement un lieu de coordination. Or le problème, c'est que les cybercriminels bénéficient, eux, de toute la fluidité, de toute la réactivité du numérique. Déplacer leurs activités d'un pays à un autre se fait en quelques minutes, c'est très fluide, tandis que les États, qui respectent leur Code de procédure pénale, sont obligés de formuler des demandes de coopération, qui doivent être traduites, acceptées, etc. Il y a donc une prime de réactivité et de mobilité en faveur des délinquants.

En matière de terrorisme, les États ont intensifié leur coopération, mais là encore, on est avant tout dans de la coopération internationale et pas dans de l'intégration de services opérationnels. Ce qui explique qu'il n'y a pas les mêmes capacités de réactivité, de performance, de fluidité que les organisations criminelles.

Il y a eu, cependant, des résultats sur des pratiques ciblées, par exemple les retraits de contenus. Des États, notamment européens, ont réussi à peser davantage que dans d'autres domaines auprès des grandes plateformes, afin, par exemple, de retirer des contenus faisant l'apologie du terrorisme. Ce sur quoi on a buté, c'est que, jusqu'à présent, le corpus juridique était trop faible. En clair, les plateformes étaient considérées, jusqu'à présent, comme des hébergeurs avec un rôle seulement technique, sans responsabilité sur la nature de ce qui est diffusé. Vous ne pouvez alors pas demander d'intervenir aussi rapidement que pour un éditeur, et il faut reconnaître que les grandes plateformes ont utilisé des trésors de lobbying pour surtout ne jamais être considérées comme des éditeurs. Car un éditeur, journal, radio, télévision, est responsable du contenu, et peut être poursuivi devant la XVII[e] chambre correctionnelle du Tribunal de Paris qui est spécialisée en la matière. Alors que quand vous n'êtes qu'hébergeur, il faut des signalements documentés, concordants, en nombre suffisant, etc. C'est comme ça qu'il y a eu des discussions surréalistes entre le ministère de l'Intérieur et une grande plateforme concernant des vidéos de décapitation. Ladite plateforme plaidant l'absence de musique valorisant l'acte et de commentaire faisant l'apologie de la mise à mort. Elle le qualifiait donc de simple information. Cependant, le *Digital Service Act* (DSA) et le *Digital Market Act*[23] (DMA), deux textes européens adoptés en 2023, même s'ils ne qualifient pas les plate-

23. https://www.bercynumerique.finances.gouv.fr/numerique-que-sont-le-dma-et-le-dsa-les-projets-europeens-de-regulation-dinternet

formes d'éditeurs au même titre qu'un média, donnent désormais des moyens à la famille européenne pour obtenir des retraits avec un renforcement considérable de la responsabilité de ces acteurs. Les discours d'appel à la haine devraient être plus facilement attaquables et surtout résorbables par l'entrée en vigueur de ce DSA et de ce DMA européens.

Jean-Louis Gergorin [24] : *Vous avez très justement signalé la remarquable audition parlementaire du général Aymeric Bonnemaison. Dans cet exposé, celui-ci décrit très bien la doctrine américaine de* cyber threat hunting, *qui consiste à préempter de futures attaques en étant présent dans les réseaux, qu'il s'agisse des réseaux des alliés qu'on protège ou ceux de l'adversaire dont on s'attend à ce qu'ils attaquent. Cette stratégie consiste notamment à repérer les implants, ces maliciels prépositionnés à l'avance. Or la doctrine américaine, comme celle du Royaume-Uni, du reste, semble évoluer. Le Cyber Command américain, conjointement avec le FBI, semble maintenant estimer tout à fait légitime de neutraliser les groupes criminels, principalement basés en Russie, d'ailleurs, au moyen d'attaques offensives. Ce n'est pas le cas du commandement cyber français, ni d'ailleurs d'aucun commandement cyber européen jusqu'à présent. Devons-nous évoluer sur ce point ? Dans le cas contraire, n'allons-nous pas perdre notre souveraineté numérique déjà mise*

24. Ancien chef du Centre d'analyse et de prévision du Quai d'Orsay, consultant en stratégie, spécialiste des enjeux cyber.

à mal, puisque nous risquons de devenir dépendants de la cyber protection plus offensive des Américains ?

Une deuxième question que je voudrais vous poser concerne les instruments juridiques. Vous avez très justement parlé du RGPD et des nouvelles directives qui sont en train de sortir. Mais en réalité, cela gêne de plus en plus certains acteurs auxquels nous sommes attachés, la presse française, par exemple, notamment de la presse régionale, pour qui la publicité ciblée est un élément majeur de son équilibre économique, tandis que les GAFAM n'en ont rien à faire. Pour les GAFAM, c'est très simple : d'un côté, elles obtiennent votre consentement dans les Conditions générales d'utilisation, que vous ne pouvez pas négocier et auxquelles vous souscrivez, sans les lire, parce que de toute façon vous ne pouvez pas vous passer du service ; et de l'autre, si elles subissent des amendes, ce qui arrive régulièrement maintenant, les montants sont dérisoires par rapport à leur puissance financière. Google a été récemment condamné à un million d'euros, mais même dix, c'est marginal pour eux, et pour y arriver il faut surmonter leurs armées d'avocats et toutes les procédures. Au final, les GAFAM sont toujours gagnants. Ne faudrait-il pas penser à développer des outils technologiques de protection, plutôt que de croire uniquement à ces instruments juridiques que les GAFAM ont toujours la possibilité de circonvenir ?

Nicolas Arpagian : À mon sens, l'affaire Colonial Pipeline en mai 2021 a été un tournant. Environ un quart de la distribution de pétrole, essence, mais aussi

kérosène, a été alors rendue inaccessible sur la côte Est des États-Unis, à cause d'un rançongiciel dont a été victime cette société. Face à la montée de la colère dans l'opinion publique, nous avons assisté à deux beaux cas de *deus ex machina* : l'administration américaine a tout d'un coup déclaré avoir retrouvé les pirates et récupéré l'essentiel de la rançon que la compagnie avait payée. On n'a jamais su comment. Je pense que le droit n'a pas été très sollicité dans cette affaire. Mon analyse, qui n'engage que moi, est que les États-Unis se sont affranchis de toutes les règles de droit et qu'on a utilisé les services de renseignement – parce que le président Biden a dit qu'il fallait régler la question tout de suite au nom de l'intérêt supérieur de la Nation. Je pense que c'est un modèle qui est difficilement duplicable et impossible à rendre public. Il y a eu un problème similaire avec Apple qui ne voulait pas ouvrir son téléphone à la requête des services judiciaires américains, dans le cas de l'attaque terroriste de San Bernardino. Et puis, un beau jour, on a appris, autre *deus ex machina*, que le FBI avait déniché une entreprise israélienne capable de pirater l'iPhone du terroriste. Résultat, tout le monde était content, le FBI avait ses éléments de procédure et Apple pouvait dire qu'elle n'avait pas enfreint la vie privée de ses utilisateurs. Je pense qu'on a juste sauvé les apparences.

Contre le prépositionnement, la réponse première est l'expertise. Le moyen essentiel de s'en prémunir, c'est d'avoir des têtes de femmes et d'hommes bien faites pour être capables de comprendre une situation et se demander si, tiens, cet élément-là est bien normal, juste un bug

ou une pièce prépositionnée. Même si on met des outils de détection, qui vont balayer les infrastructures, il faut des femmes et des hommes, et c'est là où l'investissement initial dans la formation, dans l'entretien de cette formation, est vital. La France, pour sa part, doit surinvestir ce champ pour rattraper un certain retard. Ce n'est pas tant un problème de nombre de formations, elles existent mais ne font pas le plein. Le prépositionnement est d'autant plus un sujet, que l'on doit composer avec une certaine habitude de mettre en place les fameuses *back doors*, ces « portes arrière » facilitant un accès discret aux systèmes. De grands industriels du numérique ont officialisé, à l'occasion du conflit en Ukraine, le fait qu'ils peuvent parfois être des bras armés de l'administration américaine. Le général Bonnemaison, dans son audition parlementaire de la fin 2022, a déclaré qu'on avait envisagé un *Pearl Harbor* numérique à un moment, qui n'a pas eu lieu et c'est tant mieux. Mais je crois que cela s'explique clairement par le fait que le conflit n'oppose pas la Russie à la seule Ukraine, mais, en tout cas du point de vue numérique, avec l'implication de toute la puissance du *Cyber command* américain et de plusieurs géants du numérique.

Concernant la réglementation, celle-ci a quand même un avantage : elle pose des obligations, fixe aux parties prenantes un agenda de mise en conformité et crée un régime de sanctions et de responsabilité. La réglementation a du bon, parce que là où un dirigeant d'entreprise pourrait invoquer la conjoncture pour se défausser ou son manque d'envie, il est amené à répondre à des questions

importantes : vos données sont-elles caractérisées et localisées ? Quelles sont les mesures de protection mises en œuvre ? On s'est moqué un peu facilement de l'Union européenne, où la France et l'Allemagne ont été très motrices en matière de réglementations. Il n'empêche que la Californie a produit un équivalent du RGPD, et que les États-Unis et la Chine se sont dotés à leur tour de législations sur les infrastructures critiques. Mais il est évident que là où l'Europe est défaillante, c'est en termes d'offres applicatives ou logicielles : un internaute chinois peut vivre sa vie numérique – se faire livrer ses repas, avoir des interactions sociales, trouver un job ou l'âme sœur – avec une palette d'applications ou de services totalement chinois. Pareil pour un citoyen russe ou américain. L'Europe, elle, est essentiellement un consommateur de services numériques développés par d'autres. Et n'a pas encore su créer d'offres, soit parce qu'on n'a pas donné les moyens financiers à ces entités, soit parce que les technologies existaient, mais que les utilisateurs européens ne s'en sont pas saisis. Ce qui peut s'avérer mortel pour celles-ci. Pour prendre l'exemple d'un moteur de recherche : il n'est performant qu'à partir du moment où il a de nombreux utilisateurs qui nourrissent l'algorithme et lui permettent de devenir meilleur et d'attirer encore plus d'usagers. Sans quoi, au contraire, il est pris dans une spirale descendante car considéré comme peu pertinent et satisfaisant. Il en va de même avec le fameux ChatGPT dont tout le monde parle : en l'utilisant exclusivement, les Européens le renforcent et ne donnent pas les moyens à un équivalent européen d'émerger. Idem pour ces applications ludiques qui vous promettent de vous donner

le visage que vous aurez dans 10, 20, 30 ans, si vous leur transmettez votre portrait. Outre la captation de votre image, vous contribuez à entrainer leur logiciel d'intelligence artificielle. Sous prétexte de faire une activité amusante, vous acceptez leurs conditions générales et cédez la propriété de votre figure en format haute définition, voire son utilisation commerciale. Ce qui fait que votre visage peut très bien, demain, agrémenter une campagne publicitaire pour des céréales ou autres. Chacun, par une méconnaissance du droit et des conséquences, a offert gratuitement la montée en gamme de ces algorithmes, parce qu'on a fourni gratuitement la masse de données dont ces outils ont besoin pour être de plus en plus performants et peut-être dominer le marché de demain, compliquant l'arrivée de nouveaux entrants.

Jean-Louis Gergorin : *Dans le cas de Colonial Pipeline, ils ont récupéré l'argent parce qu'il existe des outils. Il y a trois ou quatre start-ups (ou même ex start-ups, parce qu'elles se développent très vite), deux américaines et une britannique, Elliptic, qui sont bien connues et qui permettent de tracer tout ce qui se passe sur les cryptomonnaies. Parce que toutes ces rançons sont payées en cryptomonnaies – essentiellement en bitcoins. C'est comme cela que Colonial Pipeline, qui a évidemment donné au FBI les informations, a pu récupérer son argent. L'Europe réfléchit sérieusement à se doter des mêmes outils de récupération…*

Nicolas Arpagian : Oui, mais pour Colonial Pipeline, ce que je voulais souligner, c'était l'affranchissement d'un

certain nombre de règles de droit, les délais très courts dans lesquels ça s'est fait…

Jean-Louis Gergorin : *Le texte en cours de préparation aux États-Unis, qui sera une directive présidentielle, va légitimer tout ce que vous avez décrit, c'est-à-dire la capacité d'intervention offensive, telle qu'elle est pratiquée, y compris face à des attaques criminelles, pas simplement face à des attaques étatiques. Tout ceci va être écrit, va être officialisé, et donc accentuera encore le déséquilibre stratégique entre l'Europe et les États-Unis.*

Benoit Grandin [25] : *Je voulais savoir quelle était votre opinion par rapport à la doctrine publique française de cybersécurité qui sépare de façon assez stricte, quoique pas nécessairement étanche, le défensif de l'offensif, avec le défensif attribué quasi exclusivement à l'ANSSI, et l'offensif à la fois au commandement cyber, à la DGSE et à quelques autres acteurs.*

Nicolas Arpagian : Vous avez raison, c'est un vrai choix doctrinal, que par exemple n'ont pas fait nos voisins britanniques, où le GCHQ est à la fois agence gouvernementale, service de renseignement et dispositifs d'écoute. L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), créée en 2009, était la succession de la Direction centrale de la sécurité des systèmes d'information, sous l'autorité du SGDSN, le Secrétaire général de

25. Conseiller référendaire à la 4e chambre de la Cour des comptes.

la Défense et de la Sécurité nationale. En clair, vous avez le Premier ministre qui a en dessous de lui le SGDSN, qui a dans son champ d'intervention l'ANSSI. Ce placement auprès du SGDSN correspond totalement à ce que vous décrivez. Le SGDSN, c'est le gestionnaire de crise, c'est le spécialiste de l'anticipation et du pilotage de crise, depuis la crue centennale à Paris à des pandémies ou un accident nucléaire. Son travail, c'est notamment de préparer des plans, des exercices, des moyens en sorte de répondre à des crises de toute nature au sens large. L'une des raisons de ce placement de la DCSSI puis de l'ANSSI auprès du Premier ministre, par l'intermédiaire du SGDSN, était aussi de ne pas effrayer les entreprises en les mettant face à une structure de la Défense, et de leur dire que le risque n'est pas uniquement militaire, mais concerne bien tous les acteurs civils. Pour le clin d'œil, c'est le même type de raisonnement qui m'a conduit à insister auprès des Presses Universitaires de France (PUF) pour ne pas intituler mon « Que sais-je ? », *La cyberguerre*, mais bien *La cybersécurité*. Parce que la guerre, cela semble dans l'esprit de beaucoup devoir ne concerner que les militaires, tandis que la sécurité, c'est clairement le problème de tous. Il est toujours plus simple de faire venir les militaires à des sujets civils, que l'inverse. Même si Guillaume Poupard, le premier directeur, était ingénieur général de l'armement, que l'ANSSI était assez de culture militaire, le rattachement au Premier ministre était quand même un moyen d'aborder les entreprises en leur disant qu'il s'agit de réalités économiques, de leur monde et pas uniquement d'un domaine réservé à l'univers militaro-industriel.

Concernant le partage entre l'offensif et le défensif, un avantage du cyber, c'est qu'à la différence de l'armement, l'offensif et le défensif ne sont pas des mondes en opposition. À la question de comment on attaque, la doctrine française, pendant plusieurs années, a été muette. Mais quand je dis muet, on vous réprimandait si vous ne faisiez ne serait-ce qu'aborder le sujet, en disant qu'il vaut mieux laisser les adversaires dans le flou concernant votre capacité d'action. Mais je pense que quand vous avez des géants en face de vous, vous avez beau dire que vous avez un super arsenal dans la poche, il faut être sacrément crédible pour être craint. À l'époque, c'était essentiellement la DGSE qui était responsable de la fonction offensive. Ensuite, a été créé le Commandement cyber en tant que tel, au même titre que les états-majors de la Marine, de la Terre ou de l'Air et de l'Espace. Il y a toujours un fort besoin de recrutement. Aujourd'hui quand vous allez dans les salons destinés aux étudiants au sujet des carrières professionnelles, vous avez au milieu des entreprises un stand de la DGSE, de la Direction du renseignement militaire (DRM), de la Sécurité militaire (DRSD)… parce que ce sont des organismes qui ont besoin de trouver des recrues. Ils font des événements, des « hackathons » pour détecter les talents et faire connaître leurs offres d'emplois. On est dans un domaine où le diplôme n'est pas le plus important ; ce qui compte c'est votre capacité opérationnelle, et des gens sans être très diplômés peuvent avoir des savoir-faire intéressants. Grâce à la cooptation et à des tests concrets on peut apprécier la valeur d'un(e) candidat(e). Mais ce sont des profils qui sont encore

largement en pénurie sur le marché, car tout le monde les recrute : administrations civiles de l'État, administrations militaires de l'État, grands groupes industriels, prestataires privés et monde cybercriminel. Les services de l'État (principalement l'ANSSI et la DGSE) ont deux avantages pour les jeunes diplômés : les salaires d'entrée ne sont pas si déconnectés de la réalité du marché et la mise en responsabilité est beaucoup plus rapide que dans beaucoup d'entreprises commerciales. Avec des postes très intéressants confiés à de jeunes diplômés. En revanche, avec la montée dans la hiérarchie intermédiaire, la séniorité, il y a souvent un effet ciseaux sur les rémunérations par rapport au privé. Donc le vrai défi aujourd'hui des administrations est aussi de garder leurs personnels, de les fidéliser. Le recours à des réservistes est également une possibilité pour compléter les ressources des effectifs permanents.

Jean-Michel Besnier [26] : *Vous avez magnifiquement décrit les trois valeurs qui ont longtemps été considérées comme émancipatrices : la dérégulation, la fragmentation, et la déterritorialisation. Ce sont ces trois valeurs qui, depuis la contre-culture américaine, sont considérées comme la condition pour éviter les États totalitaires, pour éviter la prise de pouvoir centralisée. La question que je me pose après vous avoir écouté, est celle-ci : est-ce que la culture d'émancipation qui a été celle de l'Occident pendant des décennies, dont vous avez souligné certains effets pervers, n'appelle comme alternative que l'État autoritaire, que la transformation, comme en*

Chine et en Russie, de leur cyberespace en Intranet ? Peut-on forger une utopie, une vision, qui permettrait d'échapper aux inconvénients de la culture d'émancipation néo soixante-huitarde, d'un côté, et, de l'autre, aux méfaits de l'État autoritaire, même adouci ?

Nicolas Arpagian : L'univers numérique présente une particularité par rapport aux grands groupes du XXe siècle : il ne s'agit plus simplement d'inonder le monde avec ses produits, mais aussi de déployer un projet philosophique et politique. Le mantra de Sergey Brin et Larry Page, quand ils ont créé Google, était « Don't be evil ». Avant, c'était essentiellement améliorer les marges, faire de l'optimisation fiscale... bref : doper la profitabilité. Là, on a des gens qui disent qu'ils ont un projet de société, un projet d'organisation du monde. C'est très clair avec des gens comme Jimmy Wales, pour Wikipédia, ou Elon Musk qui vient de prendre le contrôle de Twitter. Nombre de ces firmes ont aussi des projets politiques, des projets de société (technomédecine, corps augmentés, monnaies virtuelles…) avec une ambition d'implication inédite et mondiale sur les populations.

André Comte-Sponville : *Une question pour rebondir sur l'intervention de Jean-Michel Besnier. Ces nouvelles technologies, symbolisées par le smartphone, sont le triomphe de l'individu – en tant qu'individu, j'accède à de nouveaux pouvoirs, de moins en moins coûteux ;*

26. Professeur émérite de philosophie à l'Université Paris-Sorbonne.

je n'y comprends rien techniquement, mais je l'utilise. D'un côté, donc, triomphe de l'individu, de plus en plus puissant. Mais dans le même temps, les libertés individuelles s'en trouvent menacées. Le triomphe de l'individu, pour ne pas dire de l'individualisme, finit par menacer les libertés individuelles. Cela m'inquiète beaucoup. Car la démocratie a deux ennemis principaux : les dictateurs et la mafia – les deux pouvant fonctionner ensemble, comme on le voit notamment en Russie. On a le sentiment que le numérique renforce la menace que représentent ces deux ennemis pour nos démocraties. Quelles armes la démocratie peut-elle et doit-elle utiliser pour combattre, bien sûr, les dictatures, mais aussi cette mafia dont le pouvoir est considérablement augmenté par les nouvelles technologies ?

Nicolas Arpagian : L'hyperpersonnalisation est en effet une pièce à deux faces : elle peut être émancipatrice, mais elle conduit aussi à morceler les ripostes et les coalitions de défense. Gommant le sentiment d'appartenance à une collectivité, qui souderait des opposants à même de proposer une option alternative. Sur un autre plan, un certain nombre de grands acteurs économiques ont bien compris l'importance d'entretenir les rivalités entre les interlocuteurs. En jouant par exemple de la compétition fiscale et sociale entre les 27 pays de l'UE. Ainsi on constate que les grandes multinationales mettent constamment en concurrence les États membres pour héberger leurs activités ou domicilier leur comptabilité. Le Luxembourg et l'Irlande sont assez exemplaires de ce genre de pratiques en formulant des offres très (trop ?) compétitives.

L'hyperindividualisation est donc forcément un vecteur de fragilisation, parce qu'on ne peut compter que sur ses propres ressources. Ensuite, quelle attitude avoir face à ces deux dimensions antagonistes ? On dit que c'est un optimiste qui a inventé l'avion et un pessimiste qui a inventé le parachute. Il faut les deux. Et ne pas minimiser les périls. L'un d'entre eux, c'est la béatitude et le technosolutionnisme. Tout récemment encore, nous en avons eu l'illustration avec ceux qui s'imaginent que pour régler le problème politique et culturel entre chasseurs et promeneurs, il suffit de sortir une application sur un smartphone pour éviter que des gens se fassent tuer en allant en promenade. Il faut plus que jamais hausser les droits de l'*homo numericus* que nous sommes devenus, trop longtemps négligés, et bien les faire connaître à tous les citoyens.

Il ne faut pas non plus oublier qu'une entreprise est un corps social mortel. Rappelez-vous des services comme *MySpace* ou *Second Life*, dont tout le monde parlait il y a quelques années, dont il fallait être, et qui maintenant ne sont plus que l'ombre d'eux-mêmes. Les utilisateurs, à un moment, ont considéré que les fonctionnalités n'étaient pas satisfaisantes, qu'il y avait mieux ailleurs, qu'ils n'en avaient pas pour leur argent, même si c'est gratuit… Et bien, plus vous pourrez discuter une technique, plus vous pourrez la contester, plus vous pourrez aller voir ailleurs et finalement remettre en question les entreprises non respectueuses des droits individuels, plus vous aurez des citoyens autonomes.

Un mot sur le terme de *hacker*[27] : celui-ci est souvent assimilé à un pirate, au sens de gangster, or c'est un tempérament que je nous souhaite dans nos organisations. Car qu'est-ce qu'un *hacker* ? C'est quelqu'un qui, quand il regarde une technologie, veut comprendre comment elle fonctionne et ensuite la personnaliser en fonction de ses besoins ou envies. Il va donc se demander pourquoi, au juste, telle fonctionnalité existe, si elle est utile ou légitime. Pour, le cas échéant, l'améliorer ou la supprimer. Il faut donc miser sur l'éducation, l'éducation, l'éducation. Faire en sorte que nous soyons des consommateurs-citoyens-électeurs exigeants et informés.

Les administrations françaises devraient aussi se porter davantage qu'elles ne le font vers les entreprises hexagonales. Les Américains ont une expression : *Drink your own Champagne*, qui signifie qu'il faut se méfier d'une société dont les collaborateurs ne consomment pas les produits. Un peu comme un restaurant dont les employés iraient systématiquement manger ailleurs : c'est suspect pour le client qui se met à table… Une compagnie française est forcément désavantagée à l'étranger si elle ne peut pas dire que son propre gouvernement ou ses leaders nationaux utilisent ses produits. Pourquoi des décideurs étrangers feraient-ils confiance à cette entreprise si son propre écosystème domestique n'en veut pas ? Malheureusement, en France, des entreprises ne deviennent trop souvent légitimes qu'au moment où des investisseurs

27. « Les entreprises doivent se mettre au *hacking* », Nicolas Arpagian, Les Echos, 21 août 2013.

étrangers en prennent le contrôle… Nous sommes dans une période charnière où des usages sont en train de se structurer et où, si des entreprises n'atteignent pas bientôt une taille critique, elles risquent de ne plus pouvoir le faire, une fois que d'autres solutions auront été déployées à grande échelle. Car les clients ne déménageront pas si facilement. La commande publique peut donc jouer un rôle structurant et surtout très symbolique.

Richard Deville [28] : *Comment recruter dans la cyberdéfense ? Et comme individu, que puis-je faire, que nous recommandez-vous de faire concrètement ?*

Nicolas Arpagian : Dans le domaine du cyber, le salarié a nettement la main. Il faut le cajoler, d'autant plus que maintenant, avec les réseaux sociaux comme LinkedIn, elle ou il va recevoir plusieurs offres dans le mois, avec des majorations de salaire entre 15 et 20 %. Le taux de rétention, la fidélisation est donc un problème et demande des évolutions de mentalité chez les managers. Il n'est plus possible d'asseoir son autorité en clamant que le chef a toujours raison. Ça oblige à beaucoup plus de pédagogie et d'humilité de la part des équipes d'encadrement. Le salarié s'attend à ce que le chef sache faire quelque chose que lui ne sait pas faire, et qu'il lui apprenne à le faire. Sauf que le chef qui ne sait faire qu'une chose ne souhaite peut-être pas l'enseigner pour ne pas perdre son élément différenciateur. D'où l'importance de faire constamment

28. Institut des actuaires

progresser son savoir par de la formation continue. Et, troisièmement, le chef doit être en mesure de participer à la résolution du problème afin de gagner le respect de ses troupes. Elles seront ainsi d'autant plus respectueuses de son autorité. Dans le domaine du cyber, vus la rapidité des évolutions et les talents qui peuvent exister chez chacun indépendamment de son âge, ce n'est pas forcément le plus ancien dans le grade le plus élevé qui a toujours raison. Ça oblige les managers à jouer sur d'autres valeurs, à développer de grandes qualités humaines : ce qui est bien venu. Mais tout le monde n'est pas capable de faire cela.

La nature de la mission peut jouer un rôle pour attirer les talents vers les formes militaires de la cyberdéfense. Par exemple, après les attentats de 2015, des jeunes sont venus candidater au Ministère des Armées. La motivation est d'autant plus grande, dans ce secteur, qu'on va alors plus loin que des exercices pour éprouver la robustesse des systèmes d'information. Avec des actions tant défensives qu'offensives auprès d'organisations ennemies. Des femmes, des hommes peuvent apprécier de servir une politique qui correspond à leurs valeurs, dans un cadre maîtrisé.

Pour ses usages personnels, la première chose à faire est déjà d'interroger ses choix d'applications. Je prends un exemple très simple : votre messagerie. Combien d'entre vous ont recours à un service de messagerie payant ? Au passage, combien d'entre vous aussi ont acheté leur nom de domaine, pour sécuriser leur identité numérique ? Je

reviens aux emails : il est évident qu'un système gratuit de messagerie comme Yahoo, Gmail, etc., a une contrepartie, en l'occurrence l'exploitation de vos données personnelles et du contenu de vos messages. Autrement dit, en échange de la gratuité d'un service, vous offrez le profilage de votre activité. Pareil pour les moteurs de recherche : commandez à Google, vous en avez le droit, vos cinq ans de résultats de recherche. Google va vous envoyer quasiment par retour de mail un petit fichier contenant tout ce que vous lui avez demandé ces cinq dernières années. Regardez, c'est passionnant, et cinq ans, c'est long, surtout que maintenant on demande tout à Google dès qu'on a une question. Ces informations dessinent bien entendu un profil de votre personnalité, comme c'est le cas avec les données de vos courriels. Viennent s'ajouter à cela votre historique de navigation, vos déplacements ainsi que votre consommation de vidéos sur une plateforme comme Youtube.

De la même manière, il faut être très vigilant sur la géolocalisation. L'historique des géolocalisations ne se limite pas à dire que vous êtes à Paris le 19 janvier à 10 h du matin, mais que vous êtes au 27 de la rue de Londres avec un minutage à la seconde près. C'est un jeu d'enfant de croiser ces informations avec celles de quelqu'un d'autre afin de savoir qui vous avez rencontré, où, quand, pendant combien de temps, etc.

Autrement dit, le point de départ, c'est de faire attention à ses usages : se méfier des petites applications gratuites, désactiver la géolocalisation lorsqu'elle n'est pas absolu-

ment nécessaire, peut-être prendre un service de messagerie payant, avoir différents profils de courriels pour différents usages, afin de disséminer l'information vous concernant.

Ces comportements vertueux peuvent avoir un effet sur les velléités des grandes entreprises. Je prends l'exemple des « Google glasses ». Ces lunettes permettaient d'avoir des informations en temps réel sur ce que vous voyez, par exemple l'identité de la personne en face de vous. Techniquement, ça fonctionnait. Mais devant les critiques en matière de respect de la vie privée, Google a arrêté le projet. Si chacun d'entre nous fait l'effort de s'informer et d'agir en tant que consommateur, si aussi en tant qu'électeurs nous faisons pression sur nos élus, il sera possible de lutter contre ces dispositifs par trop intrusifs.

André Comte-Sponville : *Orange et Qwant scannent-ils comme Google ?...*

Nicolas Arpagian : Orange fonde l'essentiel de son activité commerciale sur un abonnement payant. C'est important de comprendre le modèle économique de son prestataire afin de pouvoir lui demander des comptes. Orange n'a donc pas a priori vocation à scanner les messageries de ses clients comme le fait un fournisseur gratuit de service, financé par le profilage publicitaire.

André Comte-Sponville : *Et Qwant ?*
Nicolas Arpagian : Qwant est un moteur de recherche

français, qui s'appuie quand même beaucoup sur l'infrastructure de Bing, donc de Microsoft. Son grand défaut est de ne pas avoir suffisamment d'utilisateurs, donc de requêtes. Avec par conséquent des résultats considérés comme moins performants, ce qui semble-t-il n'incite pas les internautes/mobinautes à le fréquenter suffisamment. Cela illustre la responsabilité individuelle de chaque consommateur dans le choix des services numériques qu'il emploie au quotidien. Il n'y a certainement pas de fatalité, mais l'avancée technique de grands acteurs du numérique est difficile à rattraper. D'autant qu'ils ont acquis l'aisance financière leur permettant de recruter les meilleurs experts, d'acheter les compétiteurs émergents, et de conduire de nombreux chantiers simultanés avec la possibilité d'en interrompre certains sans mettre en péril leur puissance globale. Les situations ne sont pas figées cependant : l'intégration de ChatGPT dans l'activité de recherche d'informations sur la Toile pourrait être de nature à pénaliser le leader Google au profit du challenger Microsoft dans ce marché des moteurs de recherche et des liens sponsorisés. Sous réserve évidemment d'une riposte technologique à venir de la part du géant de Mountain View, Google. Ou d'un autre acteur, pas encore identifié !

Retrouvez l'intégralité du débat en vidéo sur
www.institutdiderot.fr

Les publications de l'Institut Diderot

Dans la même collection

- L'avenir de l'automobile - Louis Schweitzer
- Les nanotechnologies & l'avenir de l'homme - Etienne Klein
- L'avenir de la croissance - Bernard Stiegler
- L'avenir de la régénération cérébrale - Alain Prochiantz
- L'avenir de l'Europe - Franck Debié
- L'avenir de la cybersécurité - Nicolas Arpagian
- L'avenir de la population française - François Héran
- L'avenir de la cancérologie - François Goldwasser
- L'avenir de la prédiction - Henri Atlan
- L'avenir de l'aménagement des territoires - Jérôme Monod
- L'avenir de la démocratie - Dominique Schnapper
- L'avenir du capitalisme - Bernard Maris
- L'avenir de la dépendance - Florence Lustman
- L'avenir de l'alimentation - Marion Guillou
- L'avenir des humanités - Jean-François Pradeau
- L'avenir des villes - Thierry Paquot
- L'avenir du droit international - Monique Chemillier-Gendreau
- L'avenir de la famille - Boris Cyrulnik
- L'avenir du populisme - Dominique Reynié
- L'avenir de la puissance chinoise - Jean-Luc Domenach
- L'avenir de l'économie sociale - Jean-Claude Seys
- L'avenir de la vie privée dans la société numérique - Alex Türk
- L'avenir de l'hôpital public - Bernard Granger
- L'avenir de la guerre - Henri Bentegeat & Rony Brauman
- L'avenir de la politique industrielle française - Louis Gallois
- L'avenir de la politique énergétique française - Pierre Papon
- L'avenir du pétrole - Claude Mandil
- L'avenir de l'euro et de la BCE - Henri Guaino & Denis Kessler
- L'avenir de la propriété intellectuelle - Denis Olivennes
- L'avenir du travail - Dominique Méda
- L'avenir de l'anti-science - Alexandre Moatti
- L'avenir du logement - Olivier Mitterrand
- L'avenir de la mondialisation - Jean-Pierre Chevènement

- L'avenir de la lutte contre la pauvreté - François Chérèque
- L'avenir du climat - Jean Jouzel
- L'avenir de la nouvelle Russie - Alexandre Adler
- L'avenir de la politique - Alain Juppé
- L'avenir des Big-Data - Kenneth Cukier & Dominique Leglu
- L'avenir de l'organisation des Entreprises - Guillaume Poitrinal
- L'avenir de l'enseignement du fait religieux dans l'École laïque - Régis Debray
- L'avenir des inégalités - Hervé Le Bras
- L'avenir de la diplomatie - Pierre Grosser
- L'avenir des relations Franco-Russes - S.E Alexandre Orlov
- L'avenir du Parlement - François Cornut-Gentille
- L'avenir du terrorisme - Alain Bauer
- L'avenir du politiquement correct - André Comte-Sponville & Dominique Lecourt
- L'avenir de la zone euro - Michel Aglietta & Jacques Sapir
- L'avenir du conflit entre chiite et sunnites - Anne-Clémentine Larroque
- L'Iran et son avenir - S.E Ali Ahani
- L'avenir de l'enseignement - François-Xavier Bellamy
- L'avenir du travail à l'âge du numérique - Bruno Mettling
- L'avenir de la géopolitique - Hubert Védrine
- L'avenir des armées françaises - Vincent Desportes
- L'avenir de la paix - Dominique de Villepin
- L'avenir des relations franco-chinoises - S.E. Zhai Jun
- Le défi de l'islam de France - Jean-Pierre Chevènement
- L'avenir de l'humanitaire - Olivier Berthe - Rony Brauman - Xavier Emmanuelli
- L'avenir de la crise du Golfe entre le Quatar et ses voisins - Georges Malbrunot
- L'avenir du Grand Paris - Philippe Yvin
- Entre autonomie et Interdit : comment lutter contre l'obésité ? Nicolas Bouzou & Alain Coulomb
- L'avenir de la Corée du Nord - Juliette Morillot & Antoine Bondaz
- L'avenir de la justice sociale - Laurent Berger
- Quelles menaces numériques dans un monde hyperconnecté ? - Nicolas Arpagian
- L'avenir de la Bioéthique - Jean Leonetti
- Données personnelles : pour un droit de propriété ? Pierre Bellanger et Gaspard Koenig
- Quels défis pour l'Algérie d'aujourd'hui ? - Pierre Vermeren
- Turquie : perspectives européennes et régionales - S.E. Ismail Hakki Musa
- Burn-out - le mal du siècle ? - Philippe Fossati & François Marchand
- L'avenir de la loi de 1905 sur la séparation des Églises et de l'État. Jean-Philippe Hubsch
- L'avenir du bitcoin et du blockchain - Georges Gonthier & Ivan Odonnat
- Le Royaume-Uni après le Brexit Annabelle Mourougane - Fréderic de Brouwer & Pierre Beynet
- L'avenir de la communication politique - Gaspard Gantzer
- L'avenir du transhumanisme - Olivier Rey
- L'économie de demain : sociale, solidaire et circulaire ? Géraldine Lacroix & Romain Slitine
- La transformation numérique de la défense française - Vice-amiral Arnaud Coustillière
- L'avenir de l'indépendendance scientifique et technologique française Gérard Longuet
- L'avenir du Pakistan - Ardavan Amir-Aslani

- Le corps humain et sa propriété face aux marchés - Sylviane Agacinski
- L'avenir de la guerre économique américaine - Ali Laïdi
- Construire l'économie de demain - Jean Tirole
- L'avenir de l'écologie... et le nôtre - Luc Ferry
- La vulgarisation scientifique est-elle un échec ? - Étienne Klein
- Les trois utopies européennes - Francis Wolff
- L'avenir des Juifs français - Haïm Korsia
- Comment faire face à la pénurie et à la hausse des prix des matières premières ? Philippe Chalmin
- Changement climatique : comprendre et agir - Christian de Perthuis
- L'avenir du féminisme - Caroline Fourest

Les Déjeuners / Dîners de l'Institut Diderot

- La Prospective, de demain à aujourd'hui - Nathalie Kosciusko-Morizet
- Politique de santé : répondre aux défis de demain - Claude Evin
- La réforme de la santé aux États-Unis : quels enseignements pour l'assurance maladie française ? - Victor Rodwin
- La question du médicament - Philippe Even
- La décision en droit de santé - Didier Truchet
- Le corps ce grand oublié de la parité - Claudine Junien
- Des guerres à venir ? - Philippe Fabry
- Les traitements de la maladie de Parkinson - Alim-Louis Benabib
- La souveraineté numérique - Pierre Bellanger
- Le Brexit et maintenant - Pierre Sellal
- Les Jeux paralympiques de Paris 2024 : une opportunité de santé publique ? Pr François Genet & Jean Minier - Texte écrit en collaboration avec Philippe Fourny
- L'intelligence artificielle n'existe pas - Luc Julia
- Cyber : quelle(s) stratégie(s) face à l'explosion des menaces ? Jean-Louis Gergorin & Léo Issac-Dognin
- La puissance publique face aux risques - François Vilnet & Patrick Thourot
- La guerre des métaux rares - La face cachée de la transition énergétique et numérique - Guillaume Pitron
- Comment réinventer les relations franco-russes ? - Alexandre Orlov
- La république est-elle menacée par le séparatisme ? - Bernard Rougier
- La révolution numérique met-elle en péril notre civilisation ? - Gérald Bronner
- Comment gouverner un peuple-roi ? - Pierre-Henri Tavoillot
- L'eau enjeu stratégique et sécuritaire - Franck Galland
- Autorité un «enjeu pluriel» pour la présidentielle 2022 ? - Thibault de Montbrial
- Manifeste contre le terrorisme islamiste - Chems-eddinne Hafiz
- Reconquérir la souveraineté numérique Matthieu Bourgeois & Bernard de Courrèges d'Ustou
- Le sondage d'opinion : outil de la démocratie ou manipulation de l'opinion ? Alexandre Dézé
- Le capitalisme contre les inégalités - Yann Coatanlem
- Franchir les limites : transitions, transgressions, hybridations - Claudine Cohen
- Migrations, un équlibre mondial à inventer - Catherine Withol de Wenden
- Insécurité alimentaire et changement climatique : les solutions apportées par les biotechnologies végétales - Georges Freyssinet

Les Notes de l'Institut Diderot

- L'euthanasie, à travers le cas de Vincent Humbert - Emmanuel Halais
- Le futur de la procréation - Pascal Nouvel
- La République à l'épreuve du communautarisme - Eric Keslassy
- Proposition pour la Chine - Pierre-Louis Ménard
- L'habitat en utopie - Thierry Paquot
- Une Assemblée nationale plus représentative - Eric Keslassy
- Où va l'Égypte ? - Ismaïl Serageldin
- Sur le service civique - Jean-Pierre Gualezzi
- La recherche en France et en Allemagne - Michèle Vallenthini
- Le fanatisme - Texte d'Alexandre Deleyre présenté par Dominique Lecourt
- De l'antisémitisme en France - Eric Keslassy
- Je suis Charlie. Un an après... - Patrick Autréaux
- Attachement, trauma et résilience - Boris Cyrulnik
- La droite est-elle prête pour 2017 ? - Alexis Feertchak
- Réinventer le travail sans l'emploi - Ariel Kyrou
- Crise de l'École française - Jean-Hugues Barthélémy
- À propos du revenu universel - Alexis Feertchak & Gaspard Koenig
- Une Assemblée nationale plus représentative - *Mandature 2017-2022* - Eric Keslassy
- L'avenir de notre modèle social français - Jacky Bontems & Aude de Castet
- Handicap et République - Pierre Gallix
- Réflexions sur la recherche française... - Raymond Piccoli
- Le système de santé privé en Espagne : quels enseignements pour la France ? Didier Bazzocchi & Arnaud Chneiweiss
- Le maquis des aides sociales - Jean-Pierre Gualezzi
- Réformer les retraites, c'est transformer la société - Jacky Bontems & Aude de Castet
- Vers un droit du travail 3.0 - Nicolas Dulac
- L'assurance santé privée en Allemagne : quels enseignements pour la France ? Arnaud Chneiweiss & Nadia Desmaris
- Repenser l'habitat. Quelles solidarités pour relever le défi du logement dans une société de la longévité ? - Jacky Bontems & Aude de Castet
- De la nation universelle au territoire-monde - L'avenir de la République dans une crise globale et totale - Marc Soléry
- L'intelligence économique - Dominique Fonvielle
- Pour un Code de l'enfance - Arnaud de Belenet
- Les écoles de production - Agnès Pannier-Runacher
- L'intelligence artificielle au travail - Nicolas Dulac Gérardot
- Une Assemblée nationale plus représentative ? - *Mandature 2022-2027* - Eric Keslassy

Les Colloques de l'Institut Diderot

- L'avenir du progrès (actes des Entretiens 2011)
- Les 18-24 ans et l'avenir de la politique
- L'avenir de l'Afrique

Les nouvelles lignes d'affrontement dans un monde numérisé : l'ère des frontières.com

Le monde se transforme, tout vacille et change sous nos yeux. Les pays se font la guerre autrement et la cyberguérilla précède parfois les chars d'assaut.

Après la Chine et l'Iran, la Russie construit son propre Internet, pour s'isoler un peu plus du monde occidental.

La monnaie, longtemps privilège d'État, est désormais initiée par des entités privées avec les cryptomonnaies.

La vie privée menace de disparaître. La parole des professionnels vaut autant que celle des amateurs. Les réseaux sociaux ne servent plus seulement à discuter entre amis, mais également à influencer les prochaines élections.

Bref, les séparations disparaissent entre des catégories qu'on croyait évidentes et pérennes.

Et péages et murailles remplacent peu à peu les frontières classiques qui distinguaient les environnements personnels, économiques et institutionnels.

Nicolas ARPAGIAN

Vice-Président du cabinet HeadMind Partners, Nicolas ARPAGIAN est chroniqueur au quotidien *Les Echos* et enseigne à l'École Nationale Supérieure de la Police (ENSP) ainsi qu'à Sciences Po Saint Germain. Auteur de nombreux ouvrages dont « La Cybersécurité » (PUF), « La Cyberguerre – La guerre numérique a commencé » (Éditions Vuibert), « Frontières.com » (Éditions de l'Observatoire) et « Innocence à crédit » (Mareuil Éditions), il est membre du Conseil d'orientation de l'Institut Diderot.

INSTITUT DIDEROT

ISBN 978-2-494240-10-0
9782494240100
ISSN 2496-4948 (en ligne)
ISSN-2608-1334 (imprimé)

Réalisation idcomm.fr - Imprimé sur papier issu de forêts gérées durablement.