

La souveraineté numérique sans l'État : y a-t-il une souveraineté individuelle pour « l'homo numericus » ?

Par Pierre NORO

Enseignant à Sciences Po Paris, au Learning Planet Institute (Université Paris-Cité), chercheur et entrepreneur

La « souveraineté numérique » est un concept habituellement décliné à l'échelle des États et parfois à celle des « géants du numérique » dont ils dépendent pour répondre à leurs besoins. Mais, dans les discours de nombreux pionniers d'Internet et activistes des droits numériques comme dans les pratiques de certaines communautés (logiciel libre, chiffrement, technologies *blockchain*...), les outils numériques permettraient avant tout de revendiquer une souveraineté au niveau individuel.

Cet article a pour but d'esquisser les contours de cette idée, d'en questionner le sens et la légitimité historique. Par-delà une définition limitée d'une souveraineté « de fait », la création d'outils pour positiver des valeurs et des libertés universelles met en lumière une souveraineté numérique individuelle articulée autour des communs numériques et tirant sa légitimité de leur gouvernance, créant une concurrence ou des points de convergence avec celles des États et des entreprises plateformes.

La « souveraineté numérique » est un concept régulièrement invoqué dans les discours des politiques et les feuilles de route stratégiques produites par la puissance publique. Néanmoins, cette notion recouvre souvent des intentions et des réalités différentes et imprécises : la définition de la « souveraineté numérique » est encore, à bien des égards, un chantier en construction (Blandin, 2016 ; Bômont 2018 ; Danet et Desforges, 2020 ; Noro, 2021 ; Glasze *et al.*, 2022). Mais si cette nouvelle forme de souveraineté se décline au niveau des États et qu'elle s'accorde parfois aussi aux entreprises plateformes qui contestent leur pouvoir, est-il possible de la définir à l'échelle individuelle, celle de l'utilisateur numérique, de « l'homo numericus » ?

La notion de souveraineté individuelle a une longue histoire derrière elle. Elle est habitée de l'héritage intellectuel de Locke¹ puis notamment de celui des philosophes anarchistes libertaires, reconnaissant aux individus une souveraineté « naturelle » déléguée – et souvent maltraitée – par les gouvernements². Néanmoins, lorsqu'elle s'entrechoque avec celle des États ou des « géants du numérique », la souveraineté numérique individuelle se

¹ "Every man has a Property in his own Person" écrivait-il dans ses *Deux traités de gouvernement* en 1690.

² Particulièrement dans le courant anarchiste individualiste, avec l'égoïsme Max Stirner (*L'Unique et sa propriété*, 1844) mais aussi les libertariens et anarcho-capitalistes, notamment américains, de Josiah Warren (*Manifesto*, 1841) jusqu'à Robert Nozick (*Anarchy, state, and utopia*, 1974).

révèle être un amalgame complexe, le résultat de revendications diverses, d'une culture variée et d'enjeux numériques particuliers qui invitent à une cartographie originale de ce concept³. Pour ce faire, nous allons explorer les contours de cette souveraineté au travers de prises de positions, de documents et de projets à forte portée symbolique, identifiant une première définition « négative » dont les limites manifestes seront complétées par une appréhension des valeurs défendues par les communautés numériques se réclamant d'une forme de souveraineté et surtout des outils qui les positivent. Au croisement de ces deux notions apparaît une souveraineté individuelle essentiellement collective, fondée sur la défense des libertés numériques et sur la pratique de communs numériques qui méritent d'être valorisés.

LA SOUVERAINÉTÉ INDIVIDUELLE PAR-DELÀ LES ÉTATS

Avec l'émergence puis la démocratisation de l'informatique personnelle et d'Internet⁴, le rapport aux espaces numériques se développe hors des institutions de recherche et militaires à l'origine du réseau ARPAnet et du monde de l'entreprise. De la même façon que l'imprimerie, en facilitant l'accès aux livres et en décloisonnant l'accès à la connaissance, a permis à la fois la naissance d'un nouveau lecteur individuel tout en soutenant l'expansion du mouvement humaniste à l'échelle européenne, les années 1980 et surtout 1990 sont le berceau de nouveaux utilisateurs du numérique qui font l'expérience d'un nouveau « cyberspace ».

Cet espace, plutôt difficile d'accès puisqu'il requiert des compétences et des équipements spécifiques, apparaît comme résolu transnational et hors d'atteinte de la puissance publique. L'information y circule selon de nouvelles règles, de manière relativement ouverte, soumise à des contraintes techniques mais encore libre de normes juridiques, faute non seulement de législation *ad hoc* mais aussi de juridiction claire.

L'espace numérique est à la fois issu et structuré par des idéologies post-hippies, libertaires et libertariennes, où l'individu, hors des juridictions des États peut s'émanciper et exister dans de nouvelles communautés articulées autour de logiques de marché (anarcho-capitalisme), de coopération libre (développement des projets et communautés *open source* et de la philosophie Unix) (Stallman, 2015) et d'initiative individuelle, créative et parfois subversive (la culture *hacker*) (Turner, 2006 ; Cardon, 2019 ; Chen, 2022). Pour compléter le tableau, il faut aussi ajouter l'idéal « connectionniste » des pionniers et des industriels du numérique qui espèrent, avec des motifs variés mais convergents, étendre ce nouvel espace en connectant toujours plus de nouveaux foyers. Ce territoire a donc vocation à s'agrandir, ignorant les frontières nationales, mettant toujours plus d'individus en réseau, les connectant sans recourir à l'État comme intermédiaire.

La première forme de souveraineté numérique individuelle serait donc essentiellement « négative » : le cyberspace apparaît d'abord « a-national », hors des juridictions traditionnelles, au-delà de la souveraineté des États. L'*homo numericus* y serait donc souverain « par défaut », un principe pleinement aligné avec de nombreuses idéologies prévalentes dans les communautés responsables de nombreuses innovations techniques de l'époque, de la Silicon Valley californienne au CERN européen.

John Perry Barlow, artiste militant et cofondateur de l'Electronic Frontier Foundation (EFF), dans sa fameuse *Déclaration d'indépendance du cyberspace* de 1996, présente

³ Bien que certains auteurs n'hésitent pas à se revendiquer de l'héritage anarcho-libéral, comme par exemple Davidson et Rees-Mogg dans leur *The sovereign individual* (1997).

⁴ Avec notamment le déploiement des protocoles TCP/IP en 1982, puis DNS en 1985 et HTTP en 1991.

une revendication claire de cette nouvelle souveraineté numérique individuelle. S’adressant aux « Gouvernements du monde industriel, géants fatigués de chair et d’acier », il proclame : « Vous n’avez aucun droit de souveraineté sur nos lieux de rencontre. [...] je m’adresse à vous avec la seule autorité que donne la liberté elle-même lorsqu’elle s’exprime. Je déclare que l’espace social global que nous construisons est indépendant, par nature, de la tyrannie que vous cherchez à nous imposer⁵. ». Si ni le territoire, ni les usagers du cyberspace ne relève des États, il faut bien que l’*homo numericus* y soit souverain.

Cette souveraineté « naïve » n’est toutefois pas appréhendée de manière homogène et présente déjà des paradoxes. L’émergence d’une société inclusive, horizontale et libérée de l’arbitraire des États se heurte déjà aux barrières techniques et à une vision méritocratique et élitiste très affirmée dans certaines communautés. Elle résulte aussi souvent d’une vision déracinée de la réalité matérielle de l’écosystème numérique, dépendant des infrastructures et des technologies (*hardware* et *software*) financées, entretenues et/ou administrées par la puissance publique (Mazzucato, 2013), et bientôt rattrapée par l’extension des juridictions et des intérêts stratégiques.

DE L’ESQUIVE À L’AFFRONTEMENT : LA SOUVERAINETÉ INDIVIDUELLE CONTRE CELLE DES ÉTATS (ET DES GAFAM)

La souveraineté individuelle face aux États et le capitalisme de surveillance

La déclaration d’indépendance de Barlow relève néanmoins à la fois de l’esquive que de la mise en place d’un conflit de souveraineté. Elle est une réponse à l’adoption du Telecommunications Act de 1996, perçue comme une « invasion » du cyberspace par des autorités publiques incompétentes et illégitimes. L’extension de la juridiction américaine sur le « cyberspace » et le rapport de force qui en résulte vient donc progressivement « positiver » la définition de la souveraineté numérique individuelle.

Cette souveraineté individuelle ne peut donc pas résulter que du constat d’un « ailleurs » hors de portée de l’État. Elle se définit aussi contre l’État parce qu’elle s’enracine dans des valeurs menacées par celui-ci. La « civilisation de l’Esprit » dont Barlow revendique l’indépendance fonde sa légitimité sur sa culture et ses valeurs résolument anarchistes, universalistes, égalitaires, libertaires, rejetant la propriété intellectuelle au profit d’une protection absolue de la liberté d’expression individuelle et de la libre circulation de l’information. Ces valeurs étant irréconciliables avec le droit et donc l’État américain⁶, il faut bien que le cyberspace fasse sécession et affirme une souveraineté propre.

La question de la propriété intellectuelle n’est pas le seul point d’achoppement dans ce rapport de force. Mues par une intuition visionnaire des risques que la numérisation, lorsqu’elle est aux mains d’États, surtout illibéraux, ou d’entreprises dominantes et quasi-monopolistiques, puisse normaliser un contrôle sans précédent sur la société, certaines communautés se rallient autour du droit à la vie privée, à la confidentialité des communications, notamment par l’utilisation d’outils de chiffrement. C’est le cas des cypherpunks, dont Eric Hughes écrivit en 1993 le manifeste, affirmant la nécessaire protection de la vie privée comme garante d’une « société ouverte ». Le manifeste des

⁵ Traduction issue de *Libres enfants du savoir numérique : Une anthologie du Libre* (2000) de Florent Latrive et Olivier Blondeau.

⁶ L’EFF est d’ailleurs née à la suite des premières vagues d’investigations contre le piratage aux États-Unis.

cyberpunks n'est pas qu'un acte de militantisme : en proclamant « les cyberpunks écrivent du code » Hughes affirme que la souveraineté individuelle à l'ère numérique passe par la contribution au développement d'outils partagés qui protègent la souveraineté des individus et le droit universel à une vie privée face aux « gouvernements, entreprises, ou autres grandes organisations sans visage ». La participation à l'élaboration et l'utilisation d'infrastructures logicielles *open source* est donc une autre manière de « positiver » la souveraineté numérique, Hughes reliant déjà le droit individuel à un effort collectif.

L'intuition des cyberpunks se confirme surtout après le tournant que constitue les attentats du 11 septembre 2001, à la suite duquel un mouvement politique transpartisan, mené par les États-Unis entraînant avec eux de nombreux États européens, invoquant la sécurité des citoyens pour surveiller les communications d'une large partie de la population mondiale. Après les premières victoires des activistes numériques durant la décennie 1990⁷, ce retour en force de la « Raison d'État » qui prime sur les libertés individuelles a abouti à l'adoption de réglementations remettant en cause le droit au chiffrement, à la vie privée, à la neutralité du Net et à l'accès à l'information, ainsi qu'au déploiement de dispositifs de surveillance numérique de masse, du Patriot Act⁸ de 2001 jusqu'au CLOUD Act⁹ de 2018, et même à la mise en place de programmes outrepassant ces cadres juridiques, comme ceux révélés par Edward Snowden en 2013 puis de nombreux lanceurs d'alerte par la suite.

Ce basculement est pleinement aligné avec l'émergence d'entreprises plateformes fondant leur activité sur la capture d'un maximum de données des utilisateurs et la publicité ciblée, tout particulièrement les « Gafam ». La souveraineté individuelle numérique est donc amenée à se concrétiser face à une double-menace, celle du retour des États qui étendent leur juridiction au cyberspace, dont la conception de la sécurité collective bat en brèche les libertés revendiquées par les activistes numériques, conjuguée à celle des entreprises qui construisent brique par brique le « capitalisme de surveillance » (Zuboff, 2019).

La souveraineté par le code

L'accélération du conflit entre la souveraineté des États, la souveraineté individuelle et celles des entreprises plateformes présente presque une dimension dialectique en ce qu'elle force les communautés numériques à se structurer. Pour « positiver » leurs souverainetés naissantes, « l'*homo numericus* » et les entreprises usent d'un outil qui leur est propre, le code informatique, dont Lawrence Lessig avait déjà identifié le pouvoir normatif puisqu'il définit des « architectures de contrôle social » qui régissent les interactions entre utilisateurs et orchestrent une concurrence avec le droit traditionnel (Lessig, 1999, 2006). En fervent défenseur des modèles coopératifs et de l'*open source*, Lessig affirme aussi la nécessité pour les communautés numériques transnationales d'appréhender le caractère politique de leurs architectures, les valeurs défendues par le code qui leur donne corps et

⁷ Par exemple, l'*executive order* 13026 signé le 11 novembre 1996 qui amène au déclassement des logiciels de chiffrement à l'export, considérés jusqu'alors comme matériel militaire, ou la décision *Junger v. Daley* (6th Cir. 2000) qui aboutit à l'extension de la protection fournie par le 1^{er} amendement aux codes sources informatiques.

⁸ Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA PATRIOT Act), Acte de 2001 (H.R. 3162, Pub. L. 107-56), repéré à <https://www.govinfo.gov/content/pkg/PLAW-107publ56/html/PLAW-107publ56.htm>

⁹ Clarifying lawful overseas use of data (CLOUD Act), Acte adopté en tant que section V du Consolidated Appropriations Act de 2018 (H.R. 1625, Pub. L. 115-141), repéré à <https://www.govinfo.gov/content/pkg/BILLS-115hr1625enr/html/BILLS-115hr1625enr.htm>

d'adopter des modèles de gouvernance plus démocratiques afin de légitimer leur souveraineté dans la dialectique qui les oppose aux États¹⁰.

Parmi ces architectures de code, les technologies *blockchain* apparaissent comme des « outils de souveraineté » qui incarnent à la fois l'héritage des cypherpunks et de Lessig. L'ambition du système *Bitcoin*, décrit en 2008 par Satoshi Nakamoto¹¹, et des autres protocoles qui l'ont suivi, est de déployer des réseaux en pair-à-pair ayant pour but de permettre des transactions entre les membres pseudonymes d'une communauté ouverte. Le code, bien entendu *open source*, prévoit un « protocole de *consensus* » qui permet, sous certaines conditions, aux membres du réseau de s'accorder sur un ensemble d'informations (le registre constitué en chaîne de blocs) sans dépendre d'un tiers de confiance ni craindre la censure, mais aussi des règles de gouvernance décentralisée inspirées par les communautés du logiciel libre pour permettre l'évolution du code source.

Les technologies *blockchain* présentent donc à la fois les particularités des « communs numériques » (gouvernance décentralisée, *open source*, réseau pair-à-pair maintenu par les participants et accessible à tous...) et un ADN profondément anarcho-capitaliste (logique de marché libre, garantie absolue de la propriété privée contre la coercition, collaboration fondée sur l'alignement des incitations économiques et la maximisation des espérances de gains, qui va jusqu'à la marchandisation de la participation à la gouvernance...). Elles remettent radicalement en cause les pouvoirs régaliens, en premier lieu celui du contrôle de la monnaie¹², contournent le système financier traditionnel et ses réglementations, tout en contrecarrant les systèmes de surveillance, puisqu'elles implémentent des technologies de chiffrement par défaut qui redéfinissent la notion d'identité en ligne (Clippinger et Bollier, 2014)¹³.

Les technologies *blockchains* sont d'ailleurs plus que des alternatives aux institutions étatiques et aux plateformes centralisatrices des GAFAM. Elles donnent aux utilisateurs des outils pour créer de nouvelles communautés dotées d'un ensemble de règles de gouvernance inscrites dans le code d'un *smart contract*¹⁴ revêtant un caractère normatif, permettant de prendre des décisions collectives et d'administrer un trésor constitué de cryptoactifs, sans entité juridique ni juridiction prédéfinie (Hassan, 2021). Grâce à cette structure technique, les communautés numériques peuvent alors se constituer en « organisations décentralisées et autonomes » (DAO) poursuivant un objectif commun (Buterin, 2014). Puisqu'elles reposent sur une infrastructure ouverte, en pair-à-pair et un modèle de gouvernance décentralisé positivé par un code *open source* capable de s'exécuter de manière autonome, de nombreuses DAO se revendiquent d'une souveraineté de fait (de Filippi, 2018, 2021) et forment un écosystème émergent, bouillonnant d'expérimentations en matière de gouvernance et couvrant des réalités très diverses, de petites communautés

¹⁰ À même de refléter ce qu'il appelle les "citizen-sovereign values" plutôt que les intérêts commerciaux des entreprises qui composent et régulent déjà l'écosystème numérique ("merchant-sovereign").

¹¹ Satoshi Nakamoto est lui-même un-e auteur-e pseudonyme dont l'identité n'a jamais été révélée.

¹² Pourtant identifié dès le XVI^e siècle par Jean Bodin comme l'un des fondements de la souveraineté de l'État.

¹³ Les transactions sur les principaux réseaux *blockchain*, *Bitcoin* compris, sont pseudonymes et non anonymes. Elles peuvent aujourd'hui être tracées au moyen de technologies d'analyse avancées, mais de nouveaux outils sont régulièrement développés pour renforcer la confidentialité des transactions et contourner ces techniques d'analyse (« mixeurs », nouveaux protocoles comme Monero, Zcash, DarkFi...).

¹⁴ Les *smart contracts* sont des petits programmes informatiques déployés sur un réseau *blockchain*, capables de s'exécuter de manière décentralisée et automatisée.

constituées autour d'enjeux clairs et locaux, jusqu'à des tentatives de constitution de nouvelles entités souveraines alternatives¹⁵.

Si elles constituent des exemples symptomatiques d'une souveraineté numérique ancrée dans une culture alternative et des valeurs structurées autour des droits de l'*homo numericus*, les technologies *blockchain* actuelles présentent de nombreuses limites¹⁶ et sont loin d'être les seuls outils opérés par des communautés numériques, souvent de manière participative et ouverte, afin de garantir leur souveraineté¹⁷. Cette diversité et le constat évident qu'aucune de ces technologies n'est le fruit du travail d'un seul individu ni qu'elle pourrait opérer sans reposer sur un collectif organisé doit nous amener à questionner la nature « individuelle » de l'élan de souveraineté qui anime tous ces mouvements et projets.

LA SOUVERAINÉTÉ NUMÉRIQUE, UNE AFFAIRE DE COMMUN

Bien que la préservation de la vie privée prônée par les cypherpunks et par de nombreuses organisations de défense des libertés numériques¹⁸ repose sur l'utilisation par chacun d'outils de chiffrement appropriés, le développement de ces outils est évidemment le résultat d'un long travail collectif¹⁹, tout comme le droit de les utiliser en dépit de velléités politiques appelant à toujours plus de surveillance²⁰. Cette protection est d'ailleurs souvent perçue comme une pratique nécessairement collective, un bien commun où l'augmentation du nombre d'utilisateurs contribue à augmenter marginalement la sécurité de tous²¹.

De plus, il serait caricatural de limiter la défense des libertés numériques individuelles, notamment en matière de droit à la vie privée, aux seules communautés *open source* se revendiquant d'une souveraineté alternative. Lorsque leurs souverainetés s'entrechoquent, les États comme les entreprises s'appuient presque systématiquement sur la défense des droits individuels de leurs citoyens ou utilisateurs pour contrecarrer la souveraineté d'États rivaux et d'entreprises extraterritoriales (Noro, 2021)²². C'est en revendiquant la protection de la vie privée de ses citoyens que les États de l'Union européenne

¹⁵ Là encore, de l'adoption de ces technologies par des micro-nations ou la constitution de villes administrées par des DAOs (decentralized autonomous organization) jusqu'à la promesse de faire naître de nouveaux États transnationaux (Noro, 2022).

¹⁶ Voir notamment Fechtinger *et al.* (2023) et Rozas *et al.* (2021).

¹⁷ Ces outils ne se limitent d'ailleurs pas au logiciel mais comprennent également des infrastructures *hardware* (réseaux Wi-Fi et fournisseurs d'accès internet communautaires, stockage de fichiers décentralisés, mouvement *open hardware*...).

¹⁸ Quelques organisations particulièrement influentes en la matière : EFF, Privacy International, Center for Democracy & Technology, Quadrature du Net...

¹⁹ Il est parfois même financé plus ou moins directement par les États, au travers de la recherche, du développement militaire...

²⁰ À la suite des attentats ayant frappé la France en janvier 2015, le Premier ministre britannique David Cameron appelait même dans un discours du 12 janvier à l'interdiction de tout service de messagerie chiffrée auquel le gouvernement ne pourrait pas avoir accès, repéré à <https://www.bbc.com/news/technology-30794953>

²¹ Hughes intègre d'ailleurs la protection de la vie privée à une forme de « contrat social » auquel tous les utilisateurs d'outils de communication numérique devraient contribuer.

²² Comme par exemple avec l'adoption de la loi « Informatique et Libertés » du 6 janvier 1978, qui crée la CNIL en France.

adoptèrent le RGPD, renversant, au moins partiellement²³, le rapport de concurrence avec les États-Unis et leurs entreprises²⁴. Apple s’est opposé à l’État américain avec une rhétorique similaire en refusant de fournir au FBI les moyens de briser le chiffrement de l’un des téléphones des assaillants de San Bernardino. Si ces initiatives relèvent d’un mouvement vertical étranger à l’horizontalité qui caractérise les communautés numériques évoquées plus haut²⁵, leur efficacité est indéniable, d’autant que leur impact ne dépend pas exclusivement de l’adoption par chacun d’outils et de pratiques inégalement accessibles²⁶.

Que reste-t-il donc de l’idée même de souveraineté individuelle numérique ? D’une part, la définition « négative » d’une souveraineté par défaut s’avère insuffisante, voire naïve puisque déracinée des réalités matérielles, socio-économiques, politiques et juridiques du numérique. D’autre part, la définition « positive », celle qui émerge des faits, de la revendication de droits numériques centrés autour du droit à la vie privée, à la confidentialité des données et la libre circulation de l’information incarnée par le développement et l’adoption de technologies qui protègent ces libertés, est incompatible avec la fiction d’un « solipsisme » numérique, d’un *homo numericus* affirmant par et pour lui seul sa souveraineté, et n’exclut même pas l’exercice de la souveraineté des États et des entreprises lorsque celui-ci converge avec ces objectifs.

C’est à l’intersection de ces deux définitions que se dessinent les contours d’une souveraineté numérique singulière et mobilisable, celle de communautés numériques, transnationales, où les *homo numericus* s’associent librement selon un principe d’autodétermination et se saisissent de droits et libertés numériques qui émergent de l’unicité des dynamiques de l’information et de l’économie du savoir dans le « cyberspace ». Les « communs numériques » tirent alors leur légitimité à la fois des valeurs qu’ils défendent et de leur gouvernance collaborative, horizontale et ouverte (Peugeot, 2012 ; Fuster-Morell, 2014).

Comme les communautés qui les font vivre, les communs numériques forment un ensemble à la fois global et « kaléidoscopique », dont les effets sont cumulatifs et souvent interdépendants. Ils donnent corps à une souveraineté numérique « individuelle », non pas en ce qu’elle se résume à un projet anarchiste individualiste, ni ne recouvre que des pratiques atomisées, celles d’un *homo numericus* fantasmé, « seul souverain contre tous », mais qu’elle vise à protéger l’indépendance, à « encapaciter » les utilisateurs individuels dans un écosystème numérique où se déploient des asymétries de pouvoir et d’information qui provoquent des formes de domination nouvelles.

²³ La mise en conformité par rapport à de nouvelles normes s’avère souvent plus difficile pour les petits acteurs que pour les plateformes qui, pourtant ciblées, jouissent de davantage de ressources techniques et juridiques.

²⁴ La proclamation de la *Déclaration européenne sur les droits et principes numériques pour la décennie numérique* (2023/C 23/01) par l’Union européenne participe d’un même mouvement.

²⁵ Ces communautés peuvent néanmoins être indirectement associées à ce genre d’avancées, notamment au travers du travail de militantisme, d’éducation et d’influence des organisations de défense des droits numériques.

²⁶ Surtout lorsque l’on considère l’éventualité que des normes plus protectives s’étendent au-delà de leur juridiction, comme ce fut le cas avec le RGPD et le “Brussels effect” qui s’en est suivi (Bradford, 2012).

CONCLUSION

La « souveraineté numérique individuelle », revendiquée par des communautés voulant protéger les libertés numériques individuelles de chaque *homo numericus*, incarnée par des communs numériques accessibles à tous et gouvernés de manière ouverte, présente donc aujourd'hui un caractère « factuel » évident²⁷. Elle revêt aussi, comme c'est souvent le cas en matière de souveraineté, une dimension « fictive », celle d'un « mythe idéologique », puisqu'elle s'affirme par la concurrence avec des souverainetés des États et des entreprises du numérique dans lesquelles elle est encastrée (Wallerstein, 1999 ; Krasner, 2001 ; Agnew, 2005). Mais dans ce jeu de souverainetés, les superpositions et convergences sont possibles. Pour les États (ou même les entreprises) soucieux de préserver les libertés numériques individuelles, la reconnaissance de ces biens communs, le soutien à leur développement et la valorisation de leurs modèles de gouvernance, pour eux-mêmes et en tant que source d'inspiration potentielle, doivent devenir une priorité en matière de politiques publiques du numérique, que ce soit pour contrecarrer la domination de certains États ou d'entreprises qui mettent en péril les libertés individuelles, pour protéger le droit à la vie privée de chacun, pour renouer avec une partie de l'utopie libertaire du *web* ou pour concrétiser sa promesse d'une société de l'information plus égalitaire, démocratique et désirable.

BIBLIOGRAPHIE

- AGNEW J. (2005), "Sovereignty regimes: Territoriality and State authority in contemporary world politics", *Annals of the Association of American Geographers*, n°95, pp. 437-461.
- BÔMONT C. (2018), « Maîtriser le cloud computing pour assurer sa souveraineté » in Stéphane Taillat éd., *La Cyberdéfense : Politique de l'espace numérique*, pp. 91-97, Paris, Armand Colin.
- BLANDIN A. (dir.) (2016), *Droits et souveraineté numérique en Europe*, Bruylant, Coll. « Rencontres européennes ».
- BUTERIN V. (2014), "DAOs, DACs, DAs and more: An incomplete terminology guide", Ethereum Foundation Blog.
- CARDON D. (2019), *Culture numérique*, Presses de Sciences Po, Coll. « Les petites humanités ».
- CHEN C. (2022), *Work pray code: When work becomes religion in Silicon Valley*, Princeton University Press.
- CLIPPINGER J. & BOLLIER D. (dir.) (2014), *From Bitcoin to Burning Man and Beyond*, Amherst, ID3 & Off the Common Books.
- DANET D. & A. DESFORGES (2020), « Souveraineté numérique et autonomie stratégique en Europe : Du concept à la réalité géopolitique », *Hérodote*, pp. 177-178.
- DE FILIPPI P & WRIGHT, A. (2018), *Blockchain and the law. The rule of code*, Harvard University Press, 312 pages.
- HASSAN S. & DE FILIPPI, P. (2021), "Decentralized Autonomous Organization", *Internet Policy Review*, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, vol. 10, issue 2, pp. 1-10, <https://doi.org/10.14763/2021.2.1556>

²⁷ Au sens du « positivisme juridique » de Jellinek et de Malberg : la souveraineté existe *de facto*, l'État se constituant de lui-même avant de se doter de règles juridiques.

- FEICHTINGER, R., FRITSCH, R., VONLANTHEN, Y., & WATTENHOFER, R. (2023), “The hidden shortcomings of (D) AOs--An empirical study of on-chain governance”, pré-publication *arXiv*, arXiv:2302.12125.
- FUSTER MORELL M. (2014), “Governance of online creation communities for the building of digital commons: Viewed through the framework of the institutional analysis and development” in Frischmann B. *et al.* (dir.) *Governing Knowledge Commons*, Oxford University Press.
- GLASZE G., CATTARUZZA A. *et al.* (2022), “Contested spatialities of digital sovereignty” *Geopolitics*, pp. 1-40.
- KRASNER S. D. (2001), “Abiding Sovereignty”, *International Political Science Review*, vol. 22, issue 3, pp. 229-251.
- LESSIG L. (1999), *Code and other laws of cyberspace*, New York, Basic Books.
- LESSIG L. (2006), *Code: version 2.0*, New York, Basic Books.
- MAZZUCATO M. (2013), *The entrepreneurial State: Debunking Public vs. Private Sector Myths*, Londres, Anthem Press.
- NORO P. (2021), « Les enseignements des projets de cloud souverain pour la stratégie numérique de l'État français », Chaire Digital, Gouvernance et Souveraineté de Sciences Po.
- NORO P. (2022), « Gouvernement et Démocratie » in *Blockchain et développement durable*, rapport de l'association Blockchain for Good.
- PEUGEOT V. (2012), « Biens communs et numérique : l'alliance transformatrice » in CALDERAN *et al.* (dir.), *Le document numérique à l'heure du web*, ADBS, pp. 141-154.
- ROZAS D., TENORIO-FORNES A., DIAZ-MOLINA S., & HASSAN S. (2021), “When Ostrom meets blockchain: Exploring the potentials of blockchain for commons governance”, *Sage Open*, vol. 11, issue 1, pp. 1-14.
- STALLMAN R. (2015), *Free Software, Free Society: Selected Essays of Richard M. Stallman*, Boston, GNU Press.
- TURNER F. (2006), *From counterculture to Cyberculture*, Chicago, University of Chicago Press.
- WALLERSTEIN (1999), “States? Sovereignty? The dilemmas of capitalists in an age of transition” in SMITH D., SOLINGER D. & TOPIK S. (dir.), *States and sovereignty in the global economy*, Londres, Routledge.
- ZUBOFF S. (2019), *The age of surveillance capitalism: the fight for a human future at the new frontier of power*, Londres, Profile Books.