SciencesPo
CEVIPOF

Juin 2025

LA RÉSILIENCE DE L'ÉTAT FACE AUX MENACES INFORMATIONNELLES

La clé de l'État n'est pas l'organisation bureaucratique et politique, ce n'est pas le palais de Tauride, ni le palais Marie, ni le palais d'Hiver, mais l'organisation technique, c'est-à-dire les centrales électriques, les chemins de fer, le téléphone, le télégraphe, le port, les gazomètres, les aqueducs.

Giuliano Da Empoli, L'heure des prédateurs, Gallimard, 2025, pp. 104-105.

Virginie Tournay
Directrice de recherche CNRS
Centre de recherches politiques de Sciences Po (CEVIPOF)
virginie.tournay@sciencespo.fr

Cette note porte sur les menaces informationnelles susceptibles d'éprouver la résilience nationale. Elle met en évidence l'urgente nécessité de réformer en profondeur les organisations publiques et sociales impliquées dans la lutte contre les manipulations de l'information (LMI). En effet, l'attention portée au *design institutionnel* conditionne l'efficacité des contre-mesures en renforçant la résilience de l'État. S'engager dans cette voie suppose de déplacer le curseur depuis les autorités institutionnelles garanties par le droit, pour placer l'analyse à un niveau plus pragmatique : les données et leur dynamique circulatoire. Ce déplacement de l'échelle d'observation permet d'intégrer les problématiques de cybersécurité dans la LMI ; les deux partageant un même objectif de surveillance des activités du cyberespace.

La conséquence de ce rapprochement est double :
Premièrement, la notion de résilience doit être précisée. Le projet de loi qui vise à harmoniser le dispositif de sécurité des activités d'importance vitale, avec le droit européen, marque le passage d'une logique de protection des infrastructures à une approche plus globale axée sur la résilience face à tout type de menaces, qu'elles soient d'origine cyber, physique ou hybride. On passe ainsi d'une vision essentialiste à une conception relationnelle des prérogatives de Défense où le maintien de la cohésion nationale s'inscrit dans une dynamique de négociations ininterrompues. Le modèle du jeu d'échecs théorisé par John Searle constitue une métaphore efficace pour rendre accessible au plus grand nombre la notion complexe de cyber-résilience.
Deuxièmement, la rencontre entre la cybersécurité et la LMI marque un véritable séisme dans la logique institutionnelle de découpage thématique des organisations dédiées à la détection des alertes au sein du cyberespace. Ainsi, la séparation instituée entre les organisations luttant contre la désinformation scientifique, les mouvements sectaires ou le cyberharcèlement, n'a plus de réelle pertinence dans une monde où la résilience est désormais inséparable des dynamiques du cyberespace.

D'une conception essentialiste a une conception relationnelle des prérogatives de Défense

Le projet de loi *relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité*[1] du gouvernement Barnier, actuellement en première lecture à l'Assemblée nationale, consacre la notion de *résilience* dans les dispositifs de sécurité des activités d'importance vitale et de lutte contre les menaces du cyberespace. Il augure un changement majeur de paradigme en ce qui concerne la sécurisation nationale. Une approche dynamique et adaptative, axée sur la continuité des activités d'importance vitale remplace une grille de lecture plus statique et institutionnelle, fondée sur le paradigme de la *protection* face aux menaces. Cette notion sous-tend l'idée de veiller et de préserver le cœur du régalien face à des menaces externes, tandis que la *résilience* admet le caractère inévitable des atteintes. Elle interroge la capacité de rebond des infrastructures critiques et leurs stratégies pour prendre des mesures appropriées. Ainsi, une appréhension co-évolutive des activités du cyberespace et de la Défense nationale se substitue à un regard mécaniste des dynamiques du cyberespace. L'inconvénient majeur de ce dernier modèle qui a prévalu jusqu'à maintenant, était de considérer les activités au sein du cyberespace d'une part, et la Défense nationale d'autre part, comme des variables indépendantes réunies par les seuls liens de cause à effet[2].

Le paradigme de la *résilience* change la donne en soulignant le caractère interdépendant de ces deux variables et leur relatif enchevêtrement. Les pratiques du cyberespace sont duales. Elles peuvent être facilement arsenalisées, comme en témoigne l'importance croissante des influenceurs (« prédicateurs 2.0 ») quand ils sont susceptibles de « porter atteintes aux valeurs de la République », notamment par le biais du secteur éducatif, par le financement illicite d'activités cultuelles[3] ou l'embrigadement radical de jeunes publics aux motivations diverses. La dynamique du cyberespace participe aussi à la continuité des États, quels que soient le système politique, depuis les démocraties libérales jusqu'aux régimes autoritaires. Cela va de la lutte informatique d'influence, c'est-à-dire des opérations militaires conduites dans la couche informationnelle du cyberespace, jusqu'aux expressions plurielles des formes de cyber-banditisme d'État mobilisant des organisations mercenaires diversement instituées. Par exemple, le régime de la Corée du Nord forme des hackers depuis une quinzaine d'années - le groupe Lazarus étant le plus connu - spécialisés dans le vol massif de cryptomonnaies et l'espionnage technologique avec menace de paralysie des infrastructures critiques. Cette logique cyber-offensive impacte l'équilibre international de dissuasion nucléaire[4]. On passe ainsi d'une *conception essentialiste* des prérogatives de Défense de l'État, définie par la « protection des installations d'importance vitale », à une *conception relationnelle* de ces mêmes prérogatives. Elle sous-tend la capacité des États à absorber des attaques informationnelles menaçant la cybersécurité. Avec ce modèle, la maitrise des perturbations doit permettre à la puissance publique de retrouver une stabilité pouvant être différente de la situation initiale, mais l'atteinte de ce nouvel équilibre ne peut avoir pour effet de modifier substantiellement la cohésion sociale.

1.
Le projet de loi réfère à la transposition de trois directives européennes publiées le 14 décembre 2022. La première, dite « REC » sur la résilience des entités critiques, concerne l'élaboration de standards européens pour préparer et répondre aux risques qui pèsent sur ces infrastructures ; la deuxième dite « NIS 2 » fixe des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union Européenne, et la troisième concerne le secteur financier. Elle accompagne le règlement *Digital Operational Resilience Act* (DORA)

2.
Impact des réseaux sociaux sur la Défense Nationale, présentée en ouverture des premières journées de l'Agence du Numérique de Défense le 16 octobre 2024. Ce travail en cours de publication propose une modélisation de la Défense Nationale en rupture avec une vision mécaniste. Elle est envisagée suivant une logique de système complexe

3.
Frères Musulmans et islamisme politique en France, Rapport de la République Française, mai 2025

4.
Edwin Barancira, « Les menaces cyber de la Corée du Nord », Portail de l'Intelligence Économique, le 30/05/2025. https://www.portail-ie.fr/univers/2025/les-menaces-cyber-de-la-coree-du-nord/ Consulté le 31 mai 2025

Intégrer la notion de résilience amène au constat difficile « *que l'on ne pourra jamais se protéger contre toutes les menaces. L'enjeu consiste donc à identifier les moyens d'assurer la continuité des activités essentielles* »[5] en cas d'incident. Un consensus doit être établi autour de ce qui constitue « *le sanctuaire de nos activités régaliennes* »[6], c'est-à-dire sur ce qui doit à tout prix être préservé dans la poursuite des activités essentielles, souligne le Général Patrick Perrot, conseiller IA du Comcyber du ministère de l'intérieur, dans un débat consacré aux problématiques de souveraineté numérique. Sera-t-il acceptable, par exemple, que la plateforme Google apporte son expertise dans le marché des logements sociaux, telle que le profilage des habitudes d'une population cible, croisé à une estimation des risques territoriaux de criminalité ou de pollution ? Si elle ne s'adresse pas directement aux contenus informationnels[7], la notion de résilience interroge leur autorité légitime et concourt activement à la LMI. Le défi démocratique porte sur la démarcation à établir entre les données dont la circulation doit rester entre les mains de l'État, celles qui ne doivent, à aucun prix, être déléguées à une instance supranationale ou à des consortiums privés, et celles qui peuvent relever d'une subsidiarité européenne. En filigrane, c'est le noyau dur de la cohésion sociale qui exige d'être clarifié à travers la numérisation des sociétés et la démocratisation de l'intelligence artificielle.

À cette prospective des menaces informationnelles qui porte autant sur les contenus que sur l'autorité légitime apte à les gouverner, doit être ajouté l'usage massif, continu et personnalisé d'agents conversationnels tels que *ChatGPT*, *DeepSeek* ou *Mistral AI*. Nul doute que ces pratiques sociales auront un impact considérable sur la cohésion sociale et la légitimité de la puissance publique à moyen et long terme. Préciser la notion de résilience face à ces nouveaux défis suppose de déplacer le curseur des autorités instituées à la dynamique des données du cyberespace.

I. Une grille de lecture basée sur la donnée plutôt que sur les autorités instituées

La résilience des États face au tsunami numérique ne peut pas être évaluée en prenant uniquement pour référence l'échelle institutionnelle dont l'autorité s'apprécie au regard de la hiérarchie des normes. En effet, la souveraineté en matière cyber est moins tributaire du caractère légalement instituée d'une autorité, que de son architecture organisationnelle, comme en témoigne la nécessité stratégique de disposer d'un cloud français en matière de Défense afin de ne pas dépendre d'acteurs extérieurs[8]. Dès lors, la légitimité politico-légale des autorités nationales et européennes ne constitue pas un critère *per se* de résilience ; le droit et les valeurs européennes fixent le cadre de protection mais ils n'empêchent pas les ingérences encouragées par la fluidité du cyberespace. Le web, ainsi que les objets connectés et les outils de l'intelligence artificielle sont accessibles à tous et peuvent être diversement arsenalisés[9] par une large palette d'acteurs en partenariat, en opposition ou en situation d'indifférence vis-à-vis des États-nations. Face au caractère protéiforme des acteurs susceptibles d'intervenir dans le cyberespace (en termes de taille, structure, motivation et visibilité), il convient de s'appuyer sur une conception *relationnelle* des institutions souveraines basée sur la circulation des données, plutôt que sur une vision *essentialisée* de leur autorité. Cela va du fonctionnement classique des organisations impliquées, par exemple, dans le traitement et la compilation des données fiscales jusqu'aux politiques transactionnelles de Trump conduisant à un autodafé numérique des bases de données publiques.

5.
Propos de M. Hugues Saury, rapporteur du projet de loi, dans le cadre de l'examen du rapport MM. Michel Canévet, Patrick Chaize, et Hugues Saury, fait *au nom de la commission spéciale sur le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité*, n°393, Sénat, 4 mars 2025. https://www.senat.fr/rap/l24-393/l24-39324.html. Document consulté le 5 mai 2025

6.
Propos du général Patrick Perrot, conseiller IA du Comcyber du ministère de l'intérieur dans le cadre du débat avec Laure Sibony, enseignante et autrice, *L'IA face aux enjeux de souveraineté*, Alliancy - numérique et business, 15 mai. https://www.linkedin.com/events/7315744798915645441/about/ Consulté le 9 mai 2025

7.
Les règlements européens DMA (*règlement sur les marchés numériques*) et DSA (*règlement sur les services numériques*) abordent plus spécifiquement les problématiques reliées aux abus de position dominante des très grandes plateformes et des contenus en ligne : haine, désinformation, contrefaçon. En France, cette régulation est renforcée par la loi du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique

8.
Clotilde Bômont, - *« La souveraineté numérique », pilier et défi pour la construction du cloud défense français* -, *Revue Défense Nationale*, n°878, 2025/3, p. 81-87. Amaël Cattaruzza, « Vers une géopolitique numérique », *Constructif*, n°60, 2021/3, p. 46-50

9.
Débat entre le général Patrick Perrot, conseiller IA du Comcyber du ministère de l'intérieur et Laure Sibony, enseignante et autrice, *op. cit.*

L'économie circulatoire des données : un élément clé du soft-power

Les cybermenaces doivent être analysées de façon systématique à partir de l'économie circulatoire des données, ce qui suppose de porter attention aux logiques d'accès, de captation et de monopolisation des données. Le terme d'*incident* proposé par la commission spéciale s'inscrit dans cette échelle d'observation plaçant la donnée au centre du diagnostic de la cybersécurité. Il s'agit : « d'*un évènement compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement, ou des services que les réseaux et les systèmes d'information offrent ou rendent accessibles* ». L'étude des cybermenaces suppose une hybridation des déterminants techniques, organisationnels et géostratégiques[10]. Dès lors, le *soft power* acquiert une importance considérable dans l'univers numérique en raison du potentiel d'affirmation de stratégies d'influence à grande échelle (propagande, guerre des hashtags)[11] et de techniques frauduleuses incitant l'internaute à communiquer ses données personnelles (phishing).

L'adoption du paradigme de *résilience* du point de vue de la cybersécurité a pour conséquence sociologique d'élargir le périmètre des activités numériques constitutives d'une menace, ainsi que les entités de la puissance publique concernées par l'exigence de résilience. Avec l'adoption du projet de loi, la réglementation en cybersécurité passerait de 500 infrastructures critiques à 15 000 entités dites « essentielles » et « importantes ». Des administrations publiques et des entreprises pour la plupart, auxquelles s'ajouteraient 1500 collectivités locales et groupements de collectivités. Il ne s'agit plus uniquement de sécuriser ces organisations contre les cyberattaques, mais de renforcer la résilience de l'ensemble de leurs systèmes d'information en réponse à des menaces grandissantes, de plus en plus diversifiées et mobilisant des groupes criminels protéiformes (annexe I).

Dans cette approche relationnelle, la confiance des citoyens accordée aux institutions républicaines constitue une forte variable d'ajustement de la force de frappe des cyber-ingérences, notamment informationnelles.

II. La confiance des citoyens dans les institutions républicaines : une variable d'ajustement dans la force de frappe des cyber ingérences informationnelles

Les activités numériques *menaçantes* pour la puissance publique concernent les incidents susceptibles de porter atteinte à la continuité des services essentiels au fonctionnement de la société et de l'économie.

Une qualification ex-ante impossible

Bien que les procédés numériques malveillants soient inventoriés (annexe I), la reconnaissance du caractère *menaçant* d'activités susceptibles de porter atteinte à la résilience nationale soulève une double difficulté sociologique.

Premièrement, les aspects de cybersécurité ne sont pas toujours détachables du volet informationnel. Par exemple, la préservation de l'intégrité des processus démocratiques exige de protéger les infrastructures électorales critiques des cyberattaques[12]. L'annulation du premier tour de l'élection présidentielle roumaine en novembre 2024[13] est un exemple patent de la

10.
Jean-Yves Marion, « Ransomware: Extortion is My Business », *Communications of the ACM*, Vol. 68, n°5, 2025, p. 36-47

11.
Sur l'histoire et la substance des luttes informationnelles, voir les travaux de David Colon, *Les Maîtres de la manipulation - Un siècle de persuasion de masse* (Tallandier, 2ème édition, 2023), et *La guerre de l'information - les États à la conquête de nos esprits* (Tallandier, 2ème édition, 2025)

12.
Brunessen Bertrand, « Désinformation : quels enjeux ? quels effets systémiques ? », Libre Blanc du Pôle d'Excellence Cyber – *Lutte contre les manipulations de l'information. Regards croisés de spécialistes et d'acteurs du domaine*, ministère des Armées, Région Bretagne, Mai 2023, p. 10-12

13.
Rapport Viginum, *Manipulation d'algorithmes et instrumentalisation d'influenceurs - Enseignements de l'élection présidentielle en Roumanie & risques pour la France*, février 2025

porosité des frontières entre la désinformation politique et une atteinte portée à la matérialité de l'ingénierie démocratique. Ainsi, l'amplification artificielle de contenus visant à surreprésenter un candidat, parce qu'elle contrevient à la réglementation en matière de publicité et de concurrence électorale, constitue une cyberattaque qui porte atteinte à la continuité du processus électoral. Dans ce cas de figure, la contrefaçon d'un mouvement d'opinion (*astroturfing*) éprouve directement la résilience nationale.

Deuxièmement, seule une faible partie des ingérences informationnelles est susceptible de porter atteinte à la continuité de l'État, et à ce titre, d'être qualifiée de menaçante pour la résilience nationale. Les perturbations de la concurrence électorale engendrées par la manipulation coordonnée de l'algorithme de recommandation *tik-tok* sont directement liées à ce mode opératoire. Mais dans la plupart des cas, il est impossible d'évaluer l'étendue des atteintes de façon *ex-ante*. En effet, le degré de réceptivité du public cible peut difficilement être anticipé. Or, il constitue très souvent la variable déterminante de l'efficacité des modes opératoires malveillants. Un exemple pour montrer son importance : pendant la pandémie de covid, l'amplification des contenus antivax et le refus des pass sanitaires ont diminué la qualité du débat démocratique. Mais cette désinformation n'a pas constitué, en tant que tel, une menace relevant de la Défense Nationale. Dans un scénario où les populations auraient été plus perméables à la promotion infondée de l'hydroxychloroquine et plus défiantes vis-à-vis des mesures prises par les autorités, la force de frappe de tels contenus aurait constitué une menace de santé publique et la gestion de cette situation aurait exigé sa catégorisation dans le champ de la Défense Nationale, voire militaire. Aussi, la perméabilité des populations entre en ligne de compte dans la reconnaissance du caractère ou non menaçant, des manipulations informationnelles, pour la continuité de l'État.

De même, l'absence d'attention malveillante de l'émetteur ne suffit pas à éliminer la dimension menaçante des manipulations informationnelles. Des contenus faux peuvent être émis sans que l'individu ou le groupe n'ait réellement conscience du caractère désinformateur (*Mésinformation*). On se souvient du statut controversé de la trithérapie il y a une vingtaine d'années pour lutter contre le VIH. En rendant indétectable le virus dans le sang, cette médication permettait de conclure que les risques de transmission par voie sexuelle étaient négligeables. Certains en avaient déduit que la trithérapie n'était pas seulement un outil thérapeutique mais aussi un outil de prévention qui ne supposait pas d'autres précautions. Contrairement à la *désinformation* où les contenus sont artificiellement amplifiés par des outils manuel ou algorithmique de propagandes à base de faux comptes (*bots*) ou de vidéos mensongères (*deep fakes*) conduisant des malversations d'opinions, la mésinformation ne s'accompagne pas d'une quelconque volonté de porter préjudice, mais peut aboutir à des dommages collatéraux. En outre, le vrai peut aussi être détourné pour nuire à un individu, un groupe ou à une institution (*Malinformation*). Sont mobilisées des méthodes de divulgation d'informations sensibles ou d'usurpation d'identité par le piratage de comptes personnels visant à décrédibiliser une personnalité ou une institution. À côté de ces outils qui intensifient certains contenus, le harcèlement en ligne ayant pour objectif de museler la parole est aussi présent[14]. Ces procédés sont susceptibles d'amener ou de participer à des troubles de l'ordre social.

14.
Lutte contre la manipulation de l'information, site DGSI mis à jour le 26/11/2024, consulté le 4/05/2025. https://www.dgsi.interieur.gouv.fr/decouvrir-dgsi/nos-missions/cyberdefense/lutte-contre-manipulation-de-linformation

Des effets insidieux à moyen terme sur la cohésion sociale

Si la capacité à intervenir sur la viralité est une composante majeure de la manipulation informationnelle, la génération de contenus à l'aide des outils de l'intelligence artificielle[15] constitue une autre dimension à prendre en compte. La menace pour la continuité des activités de la puissance publique peut se présenter à court terme, par l'amplification des effets relatifs aux procédés de manipulation informationnelle mentionnés ci-dessus. Cela se traduit par une augmentation quantitative des contenus disponibles de mésinformation et de désinformation[16], lesquels peuvent être plus ou moins sophistiqués, et adaptés aux profils individuels. Par ailleurs, la ligne entre le contenu produit entièrement par l'*humain* et le *contenu* créé avec l'aide de l'intelligence artificielle tend à s'estomper. Cela interroge la notion de véracité de l'information traditionnellement fondée sur la source, et plus largement, le statut social et culturel à donner aux outils de l'IA dans la description de la réalité.

De façon plus insidieuse, la menace liée à l'usage des modèles de langage d'IA génératifs intervient aussi à moyen et long terme car leur entrainement soulève des défis majeurs pour la mémoire collective. La généralisation des agents conversationnels déplace les lieux traditionnels de construction de la mémoire, assurés historiquement par des institutions telles que les archives, bibliothèques et musées, vers les grandes entreprises technologiques. On assiste à une extraction massive des archives numériques par ces acteurs privés, souvent sans cadre réglementaire clair, ce qui leur permet de constituer une base d'entrainement de leurs modèles. En étant progressivement administré par ces entités, le patrimoine matériel commun devient une ressource commerciale. Ce processus d'appropriation silencieuse des données constitue une menace majeure pour la cohésion nationale, en particulier lorsque les entreprises concernées sont étrangères. En rendant accessibles gratuitement leurs algorithmes génératifs, ces entreprises imposent peu à peu leurs logiques de hiérarchisation des contenus et leurs filtres culturels, reconfigurant sans grand bruit, le rapport au passé des usagers du web ainsi que leurs traditions culturelles.

Ce mécanisme inédit de *soft law* redéfinit les modalités d'accès, de transmission et de valorisation du patrimoine culturel, sans possibilité évidente d'ouverture à un débat public, ni de contestation. Contrôler et résister collectivement à une redéfinition matérielle des mémoires collectives, est complexe à mettre en œuvre. D'une part, la gratuité et la disponibilité des agents conversationnels aux populations sont perçues, de prime abord, comme un véritable pas en avant démocratique. D'autre part, l'opacité des mécanismes d'entrainement et les règles implicites de sélection des données rendent impossible toute critique ou réglementation adaptée. On assiste donc à une reconfiguration profonde de la culture, avec cette interrogation : la façon dont la communauté nationale se rapporte à son passé constitue-t-elle une mission de l'État ? Les institutions publiques doivent-elles conserver le monopole matériel et symbolique des mémoires collectives ou la souveraineté culturelle (« mémorielle ») peut-elle être déléguée à d'autres entités privées, étrangères ou supranationales ? Dans la mesure où ces prérogatives doivent restées rattachées à l'État car constitutives du nation-building, les interrogations doivent être intégrées dans les défis de la LMI car elles interviennent sur la capacité à maintenir l'intégrité du noyau dur de la cohésion sociale.

15.
Journée d'étude du CNRS, Axe 1 – Génération de contenu, *Lutte contre la manipulation de l'information (LMI)*, 24 mars 2025. Mes remerciements à Émilie Bonnefoy de m'avoir communiqué ce document

16.
Ce constat a motivé la mise en place d'une initiative commune CNRS-Ministère des armées pour établir des stratégies de LMI. La présente note se concentre sur les LMI ayant un impact sur la résilience nationale

Trouver une manière accessible de décrire la complexité du concept de résilience fait partie de ces défis. Le jeu d'échec, modélisé par le philosophe John Searle constitue une puissante métaphore pour rendre compréhensible au plus grand nombre la complexité du concept de résilience appliquée aux institutions à l'épreuve du tournant numérique.

III. Le jeu d'échec de John Searle, une métaphore de la cyber résilience nationale

Le degré de réceptivité des publics cibles est une composante déterminante de la force de frappe des manipulations informationnelles. Une population résiliente suppose un certain niveau de confiance dans les institutions républicaines. Si les institutions assurant la protection sont bien acceptées dans la société française, on observe en revanche une perte nette d'autorités multiformes aboutissant à « l'État sans qualités ». Ainsi, le rapport des Français à la justice ou aux impôts est devenu compliqué. C'est pourquoi, la transformation de la confiance collective dans les expressions régaliennes devra être minutieusement suivie ces prochaines années[17].

17.
Les enquêtes annuelles du baromètre de confiance politique menées au CEVIPOF fournissent une traçabilité et des informations clés sur l'évolution du rapport de confiance des citoyens français et européens : https://www.sciencespo.fr/cevipof/fr/etudes-enquetes/barometre-confiance-politique/

Une perméabilité accrue des citoyens à d'autres offres cognitives

Le champ des institutions de la connaissance n'est pas épargné par les transformations de l'opinion publique : la crédibilité sociale des données scientifiques parait de moins en moins liée aux organisations qui les produisent. Les enquêtes sondagières font régulièrement état d'un contraste entre une confiance marquée dans la culture scientifique et une défiance relative vis-à-vis du travail scientifique. La baisse d'adhésion dans les institutions de la puissance publique rend les citoyens plus perméables à d'autres offres cognitives, et en particulier à des mouvances sectaires basées sur le développement personnel ou la quête collective de sens. De même, l'importance contemporaine des conflits mémoriels valorise des récits alternatifs sans que l'écueil du relativisme culturel et du révisionnisme historique ne soit véritablement traité. Le socle d'une histoire commune est fragilisé, il devient la proie d'algorithmes entrainés par des puissances étrangères à partir du socle des archives nationales. Ce processus est susceptible de porter atteinte à la cohésion nationale.

La résistance des populations aux ingérences informationnelles exige, au niveau individuel, un esprit critique acéré, une culture critique des algorithmes fondée sur des acquis scolaires pour pouvoir argumenter, contre-argumenter et utiliser les outils numériques interactifs avec le recul nécessaire. Pour autant, la résilience des États face à la diversité des menaces informationnelles reste indissociable de la garantie que les populations accepteront toujours de déléguer en priorité la prise en charge de leur santé, sécurité et alimentation à des organisations certifiées par l'État. Une contribution libre publiée dans le cadre des travaux de la commission Bartolone-Winock en 2015 faisait déjà état de cette intuition d'un bouleversement sans précédent (annexe 2). La fidélisation des populations repose sur la croyance collective dans la capacité des institutions publiques à administrer les données liées à la protection collective. Cela englobe la dimension subjective de sécurité, c'est-à-dire le sentiment collectif d'être en sécurité, et pas uniquement le fait de l'être. La résistance à la menace informationnelle est intimement liée à la cybersécurité.

Le jeu d'échec, une métaphore efficace de la résilience des États

Le modèle du jeu d'échec du philosophe John Searle est une métaphore pertinente de la résilience des États car il intègre la symbolique politique dans les conditions d'existence d'une institution. Elle fonde la raison d'être des institutions. Contrairement aux *faits bruts* qui sont indépendants de la croyance des observateurs, l'existence des institutions en est largement dépendante. Ainsi, « *l'altitude du Mont Blanc est un fait, que nous le croyions ou non ; en revanche, que ce morceau de papier gris soit un billet de cinq euros n'est un fait que parce que nous croyons qu'il s'agit d'un billet de cinq euros* ». Le fait institutionnel est donc ontologiquement subjectif[18], il est entaché des ambivalences de l'intentionnalité. C'est pourquoi le philosophe mobilise le jeu d'échec pour décrire de façon métaphorique la réalité sociale des institutions. En effet, le jeu n'existe que par ses règles constitutives collectivement reconnues, telles que les possibilités de déplacement des pièces qui sont fixées une fois pour toute. Elles définissent la condition d'existence du jeu. Cet exemple peut être contrasté avec le code de la route dont les règles correspondent à des contraintes apposées à une circulation automobile préexistante. Dès lors, elles ne constituent pas l'activité qu'elles régulent : la circulation automobile existerait même s'il y avait d'autres règles. Ainsi, la validation d'un État démocratique est indissociable de ses règles constitutives telles que l'existence des droits et devoirs des citoyens. Pour Montesquieu, le dévouement du citoyen à la Res Publica est la condition *sine qua non* à la pérennité du régime républicain. Si on supprime ce contrat social, la nature même de l'État démocratique disparait. La résilience s'appuie donc sur un sous-ensemble minimal de règles constitutives garantissant le maintien de la cohésion nationale.

Avec le tournant numérique, les règles constitutives doivent être traduites à l'échelle de la donnée, et plus seulement au niveau des institutions. Ce changement de focale n'est pas évident à intégrer dans les représentations collectives car les rapports de force politiques sont abordés et vécus sous l'angle des négociations entre États, par la voie diplomatique ou guerrière. Néanmoins, la donnée comme objet du droit est de plus en plus présente. La jurisprudence illustre des liens marqués entre leur circulation dans le cyberespace et les atteintes à la résilience nationale. La décision de la cour constitutionnelle roumaine précédemment évoquée en donne une illustration emblématique : une campagne de promotion agressive, articulée à une multitude d'attaques informatiques contre les infrastructures de support du processus électoral, met en péril la sincérité du scrutin[19]. Elle aboutit, entre autres, à fausser *le caractère libre et équitable du vote des citoyens et l'égalité des chances des candidats aux élections*. L'opération d'influence, appuyée sur la manipulation de l'algorithme TikTok constitue une atteinte qui va au-delà de la régularité du processus électoral. Elle éprouve l'intégrité des valeurs fondamentales de la démocratie constitutionnelle comme en témoigne l'annulation judiciaire du processus électoral dans sa totalité, et pas seulement du candidat ayant bénéficié d'une promotion agressive[20].

La résilience de l'État définie par son monopole sur les données régaliennes

La circulation des données dessine la cyber-résilience. À la différence de la circulation routière qui existerait même si la signalisation obéissait à d'autres règles, la résilience de l'État est structurellement définie par son *monopole* sur les données régaliennes. Cette caractéristique ne constitue pas uniquement un

18.
Éric Monnet et Pierre Navarro, « Les institutions sont-elles dans la tête ? Entretien avec John Searle », *Tracés*, 17, 2009. https://journals.openedition.org/traces/4270. Consulté le 25 mai 2025

19.
Alexandre Riou, *Roumanie : le séisme du premier tour de l'élection présidentielle*, Fondation Jean Jaurès, 05 décembre 2024

20.
Natasa Danelciuc-Colodrovschi, « Retour sur l'annulation des résultats de l'élection présidentielle par la cour constitutionnelle roumaine : les juges ont-ils sauvé la démocratie ? », dir. Romain Rambaud, *Blog du droit électoral*, 10 avril 2025. https://blogdudroitelectoral.fr/2025/04/retour-sur-lannulation-des-resultats-de-lelection-presidentielle-par-la-cour-constitutionnelle-roumaine-les-juges-ont-ils-sauve-la-democratie-par-une-nouvelle-autrice-natasa-danelciu/ Consulté le 25 mai 2025

symptôme mais elle définit son essence. Tenir un monopole sur les données du cyberespace, c'est avoir la capacité de collecter, de centraliser et de contrôler – tant la circulation, la transformation et l'agrégation – des données, qui acquièrent un statut « public » quand l'entité agit pour le compte de l'État (données de recensement, d'imposition, de la couverture sociale etc.). Ces règles de circulation sont constitutives d'un État résilient, plutôt que régulatives. On peut rapporter métaphoriquement les ingérences portant atteintes aux règles de circulation des données au bouleversement des règles du jeu d'échec. Il n'est pas possible de changer le nombre de cases sur l'échiquier, ni de modifier les règles de déplacement de chaque type de pièce, de les autoriser à franchir les bords de l'échiquier sans porter atteinte à l'intégrité même du jeu. La manipulation des algorithmes, les techniques de leurre, d'emprise psychologique telles que l'usurpation d'identité, l'extorsion de fonds, l'embrigadement ou l'exfiltration de données confidentielles peuvent, dans certains cas, fausser les règles du jeu, et être qualifiées d'atteintes portées à l'État. Il en est de même pour la désinformation issue, par exemple, de médias étrangers. Ces manipulations peuvent créer du trouble sans nécessairement porter préjudice à la raison d'être de l'État. Dans quelle mesure les manipulations informationnelles sont-elles susceptibles de porter atteinte aux règles constitutives, exigeant la répression ? Le délit d'outrage en ligne[21], disposition amendée par le Sénat, avant d'avoir été censurée par le Conseil constitutionnel en raison des risques d'atteinte de la liberté d'expression, témoigne des difficultés d'un tel arbitrage.

Le défi pour la puissance publique consiste à définir son cadre du jeu, à poser une partition claire entre le noyau des règles constitutives de la cyber-résilience et les règles régulatives susceptibles d'être modulées dans le débat démocratique. En continuant de filer la métaphore, la forme des pièces et la matière de l'échiquier peuvent faire l'objet de conventions différentes sans que cela ne modifie les principes du jeu. Pour autant, la catégorie de « règle régulative » doit aussi être appréhendée avec prudence. En effet, un pas de côté trop grand vis-à-vis des conventions régulatives peut fragiliser les règles constitutives. Par exemple, si la forme des pièces du jeu est radicalement transformée de sorte qu'elles dépassent le périmètre des cases, ou que leur motif ne soit plus aisément identifiable, la pratique de l'échec s'en trouve nécessairement impactée. Avec cette image, on peut se demander à partir de quel seuil, une promotion électorale en ligne, dépendant des systèmes d'apprentissage automatiques des réseaux sociaux (par exemple l'algorithme de Facebook, Twitter/X etc.) impacterait la cyber-résilience de l'État ? Jusqu'où les données produites et stockées par les organisations publiques peuvent-elles être utilisées par les plateformes sans porter atteinte à l'essence même du noyau régalien ? Avec des logiques algorithmiques favorisant la viralité de propos clivants, les entrepreneurs communautaires (les influenceurs islamistes par exemple) peuvent surreprésenter des contenus idéologiques incompatibles avec les valeurs républicaines[22]. Par le jeu du *soft power*, un seuil de dérégulation du marché informationnel peut définir un point de bascule menaçant la cohésion nationale. Les pratiques numériques d'influence présentent un risque systémique car leur organisation repose sur l'hybridation de données privées massivement collectées avec des profils de vulnérabilités individuelles établis par les historiques de navigation. Cela favorise les diverses formes de captation de l'attention, allant de la manipulation des consommateurs dans les univers du loisir jusqu'à des formes d'emprises sectaires plus ou moins sophistiquées.

22.
Hugo Micheron, *La Colère et l'Oubli. Les démocraties face au jihadisme européen*, Gallimard, 2023

IV. Recommandations : conserver le monopole des données régaliennes contre la tentation du néofédoalisme numérique

Les législations ne sont pas adaptées aux défis posés par le développement de l'intelligence artificielle, et plus largement par les transformations structurelles du marché informationnel qui résultent du tournant numérique. Cette inadaptation n'est pas uniquement la conséquence d'un retard de mise à jour du cadre législatif. La fabrique de la loi ne constitue pas en tant que tel un levier suffisant pour une double raison. D'une part, les manipulations informationnelles se situent sur le terrain de la *soft law*, et d'autre part, les organisations traditionnelles sont confrontées à des techniques de captation de l'attention des populations déployées par les plateformes. Les espaces numériques constituent des lieux où s'affrontent différentes propositions cognitives de services - provenant d'entités publiques comme privées - dont l'objectif affiché est d'améliorer, voire de prendre en charge le quotidien des individus à des degrés divers. En cela, les dynamiques du web confrontent les États et les sociétés à un changement drastique du paysage civique, c'est-à-dire des relations réciproques du citoyen et de la puissance publique. À travers le déploiement d'un large panel d'offres de service, les seigneurs du numérique renforcent les liens de dépendance de leur population, exposant de fait, à un néoféodalisme numérique[23]. La LMI se joue non seulement au niveau du contrôle des contenus informationnels et de leur viralité. Elle implique aussi de déterminer l'économie circulatoire des données régaliennes. Pour les institutions républicaines, cela suppose une capacité à collecter, à centraliser et à contrôler - tant la circulation, la transformation, les barrières à l'entrée que les formes d'agrégation - de données susceptibles d'acquérir un statut « public ».

23.
Virginie Tournay et Guy Saez, Dynamique du cyberespace : vers un néoféodalisme numérique, *The Conversation*, 10 avril 2025

À partir de quel seuil la mise en œuvre de procédés tels que les ingérences médiatiques étrangères, le contrôle, la manipulation des opinions publics, et les cyberattaques menace-t-elle la cohésion sociale ? S'il n'est pas toujours possible de fixer le curseur ou d'évaluer l'impact des incidents de façon *ex-ante*, une réflexion doit être menée pour adapter le design des institutions républicaines aux logiques des rapports de force régissant l'économie circulatoire des données, de sorte qu'elles puissent conserver le monopole des données *régaliennes*. Avec une grille de lecture située à l'échelle de la donnée, quelques pistes peuvent être envisagées pour réformer le design institutionnel :

1. Le réseau associatif impliqué dans la LMI au niveau français et européen est une constellation très riche, diversifiée mais fragmentée. Les structures d'éducation populaire, celles qui sont engagées contre les dérives sectaires, les embrigadements religieux et la cybermalveillance, sont confrontées à la nécessité d'alerter, voire d'intervenir dans le cyberespace pour limiter au maximum les propagandes et les atteintes à la personne incompatibles avec les valeurs d'un État de droit. Une culture de résistance et d'intervention en ligne commune à ce vivier associatif devrait être encouragée par la puissance publique. Comme le soulignait le chef de la Miviludes, Donatien le Vaillant, le 4 avril dernier dans le cadre de la rencontre organisée à l'hôtel de ville de Paris pour les cinquante ans de l'Association traitant du phénomène sectaire (ADFI), ce sont les bénévoles qui font la chair des politiques publiques. Une culture commune de la résistance numérique doit être partagée et soutenue par les pouvoirs publics. Cela suppose, dans un premier temps, de favoriser le

rapprochement d'organisations sociales confrontées aux mêmes enjeux de sécurité informationnelle (éducation, famille, sécurité intérieure…).

2. La LMI va bien au-delà des politiques sociales et éducatives. C'est un défi systémique et transversal à tous les domaines d'action publique qui éprouve l'État jusque dans ses fonctions les plus régaliennes puisque l'objectif est la préservation du monopole de ses données. Au-delà d'une prise de conscience interministérielle, c'est le découpage sectoriel des domaines d'action publique qui est à reconsidérer, ce qui engage tout le design organisationnel de l'État.

3. Les plateformes privées sont des instances de captation de l'attention capables de susciter un fort sentiment de proximité, bien davantage que les portails émanant de la puissance publique. Une concurrence de services entre les offres publiques et les offres privées s'affirme. Aussi, le *design* des services publics en ligne doit être intégralement repensé en privilégiant un rapport de proximité tout en préservant l'idée d'intérêt général. La montée en puissance de portails publics marquée par des pronoms possessifs n'est sans doute pas la meilleure solution (« Ma prime Rénov » ; « Ma retraite ») puisqu'en bout de ligne, cela encourage la personne utilisatrice de telles « services » à se reconnaître comme client plutôt qu'usager d'un service public. En outre, la personnification des services ne va pas nécessairement de pair avec le sentiment de proximité. La réintroduction d'interlocuteurs humains dans les services publics parait incontournable, et plus largement au niveau de l'ensemble des terminaisons de l'action publique (Contribution libre au rapport Bartolone-Winock, annexe II).

4. Les agents conversationnels exercent un fort pouvoir de séduction et de persuasion, notamment auprès des jeunes générations. Si les grandes plateformes entraînent leurs algorithmes en continu, la puissance publique gagnerait à mettre en place des contre-algorithmes aisément appropriables par les populations. L'objectif serait de diminuer leur perméabilité aux manipulations informationnelles. C'est le sens de la proposition du président de l'ADFI, Daniel Sisco, qui serait de mettre en place un outil conversationnel permettant à chaque citoyen de faire lui-même son autodiagnostic d'emprise sectaire basé sur les données de la Miviludes. La grille de lecture serait basée sur les critères de dangerosité et d'emprise psychiatrique. Le doute étant présent à différents moments du parcours d'embrigadement, cet outil pourrait jouer un rôle considérable dans la prise de conscience du sujet, voire intervenir comme lanceur d'alerte.

5. La puissance publique dispose d'un atout que n'ont pas les plateformes privées : la capacité institutionnelle à resynchroniser les temporalités collectives[24]. Le tournant numérique s'est accompagné d'un délitement des cérémonies audiovisuelles (par exemple, des émissions telles que Sept sur sept ou Cinq colonnes à la une) qui réunissaient tous les Français le même jour, à la même heure. La puissance publique pourrait tenter de resynchroniser les temporalités individuelles à travers de grands évènements, au-delà des cérémonies sportives telles que les jeux olympiques, impliquant des médiations numériques afin de recréer un sentiment de commun.

24.
Virginie Tournay, La confiance dans les institutions républicaines, *Les 50 ans de l'ADFI*, 4 avril 2025

ANNEXES

Annexe 1

Un catalogue diversifié des principaux types de cyberattaques[25] contre lesquelles la directive NIS2 entend lutter :

Les rançongiciels (ransomware) : logiciels malveillants chiffrant les données des victimes et exigeant une rançon pour leur restitution.

L'hameçonnage (phishing) : technique frauduleuse visant à récupérer des données sensibles en usurpant l'identité d'un tiers de confiance.

Les attaques sur internet : exploitation des failles des applications et des services en ligne

Les attaques sur la chaîne d'approvisionnement : ciblage des vulnérabilités des logiciels et services fournis par des tiers.

- Les attaques par déni de service distribué (DDoS) : saturation des infrastructures informatiques pour les rendre inopérantes.
- Les attaques à caractère social : utilisation des techniques de manipulation psychologique pour obtenir un accès aux systèmes.

25.
Commission spéciale Résilience Cybersécurité, « Renforcer la cybersécurité et la résilience des infrastructures critiques », *Sénat*, 14 mars 2025. https://unitae-rgpd.fr/wp-content/uploads/2025/03/RAPPORT-PROJET-LOI-CYBERSECURITE.pdf. Document consulté le 5/05/2024

Annexe 2

Virginie Tournay, *Effets de la numérisation de nos sociétés sur la vie politique*, Contribution libre - Rapport commission Bartolone-Winock sur l'Avenir des institutions, La documentation française, 3 octobre 2015, pp. 187-192.

Je souhaiterais apporter un approfondissement de ma contribution du 26 juin 2015, présentée lors de la dernière séance de restitution de nos travaux. Si les dysfonctionnements de la machine représentative, de nos partis politiques et de notre justice contribuent à la crise des institutions politiques, ces aspects ne constituent qu'une dimension du problème de la défiance des citoyens vis-à-vis de leurs élus. Quand on parle de « crise » des institutions, il est avant tout question du ressenti des citoyens, notamment d'une perte de croyance collective dans la capacité de nos institutions à résoudre leurs problèmes concrets, du quotidien. Dès lors, la relation de cause à effet entre la mécanique interne de nos institutions et la perception citoyenne de leur fonctionnement n'est pas directe. **Il faut donc braquer le projecteur de l'analyse au niveau de ce qui touche directement le quotidien des citoyens, c'est-à-dire les terminaisons de l'action publique qui assurent le relais du pouvoir politique jusqu'aux espaces publics. Selon moi, ce niveau est à souligner dans la hiérarchie des variables explicatives de la défiance politique.** J'ai insisté sur quatre courroies de transmission institutionnelle : le travail et les guichets administratifs, le champ associatif, les institutions de mémoire, les politiques culturelles et scientifiques. Dans le cadre de cette contribution libre, je voudrais mettre l'accent sur les changements liés à la culture numérique qui s'adressent à une fraction croissante de nos concitoyens d'une part et, qui s'intègrent, d'autre part, au cœur même du fonctionnement de nos institutions politiques, depuis la machine représentative jusqu'aux terminaisons administratives.

Au cours de nos travaux, les effets de la numérisation des sociétés sur la vie politique ont été abordés suivant un triple regard. Tout d'abord, ce sont les préoccupations de *l'open data* et de *l'open gouvernement*, c'est-à-dire l'émergence de stratégies institutionnelles fondées sur les données numériques au service de la prise de décision politique qui a été discutée (*Audition Henri Verdier ; 30/01/2015*). Ensuite, la commission s'est penchée sur l'utilisation des nouvelles technologies pour améliorer la proximité entre les représentants et les citoyens dans le cadre des campagnes électorales (*Audition Guillaume Liegey ; 13/02/2015*). Enfin, les articulations entre les temporalités médiatique et politique ont été appréhendées à l'aune de la saturation informationnelle des espaces de nos sociétés numériques (*Audition Géraldine Muhlmann ; 10/04/2015*). Indispensable, l'examen de ces aspects par la commission renvoie aux procédures internes de nos institutions politiques (Audition 1), à la communication électorale (Audition 2) et médiatique (Audition 3). Globalement, les nouvelles technologies numériques ont été appréhendées comme des opérateurs instrumentaux dont l'impact sur nos institutions politiques est essentiellement d'ordre fonctionnel. Je voudrais plutôt questionner ici l'impact du développement brutal de ces nouvelles infostructures (GAFAM)[1] sur la nature même de nos institutions politiques. Les GAFAM sont-elles en mesure de conduire à des modifications substantielles de nos institutions politiques, c'est-à-dire de transformer à la fois les ***systèmes d'acteurs impliqués***, leur ***matérialité*** et leur ***logique symbolique*** ? Jouent-elles un rôle dans les perceptions que peuvent avoir les citoyens de leurs institutions politiques ?

En dépit de l'omniprésence de ces technologies numériques dans le quotidien des français et des européens, l'horizon prédictif de leurs effets politiques est très difficile à envisager compte tenu de leur irruption brutale dans nos sociétés (quelques années) et du fait que leurs manifestations régaliennes commencent seulement à se faire sentir[2]. Plutôt que de laisser cette problématique en suspens dans nos réflexions sur l'avenir des institutions, il m'apparaît indispensable de la soumettre à l'examen de nos concitoyens tout en étant conscient qu'il subsiste un grand nombre de points aveugles en raison du fait que nous nous situons au tout début de cette innovation de rupture[3]. À défaut de trouver de solides repères dans la trajectoire à venir de ces technologies digitales, l'approche sociohistorique des techniques constitue un angle d'attaque possible pour aborder cette problématique. Aussi, doit-on considérer que l'impact des GAFAM sur nos institutions politiques, est de même portée que ne l'a été celui de la radio et de la télévision dans la première moitié du vingtième siècle ? Les GAFAM se situent-ils dans la continuité de la révolution informationnelle rattachée au développement des médias modernes ? Si tel est le cas, faut-il uniquement penser l'impact des GAFAM sur nos institutions politiques en termes de nature, de quantité et de cinétique des flux d'informations traversant nos institutions politiques et la société civile ?

Pour apporter des éléments de réponse à cette interrogation, les propriétés technologiques des GAFAM seront brièvement rappelées dans la perspective de leurs effets politiques, notamment sur la perception citoyenne des

institutions politiques (1), puis mises en relation avec certains résultats de l'enquête d'opinion « les fractures françaises » de la Fondation Jean-Jaurès[4] afin de discuter ce « pouvoir horizontal » (2) et de proposer quelques pistes pour accompagner le développement numérique dans la vie politique (3).

1. Les effets politiques des GAFAM

Pour ***l'utilisateur***, les caractéristiques visibles des outils numériques sont de deux ordres. La première, la plus évidente, est liée à la capacité à rechercher, à stocker et à échanger d'énormes quantités de données sur une interface dématérialisée (le « cloud »). Outre le fait que ces produits évoluent très vite, le nombre d'utilisateurs en fait un phénomène mondial. En 2015, 42% de la population mondiale est connectée dont deux milliards d'inscrits sur les réseaux sociaux. Au niveau de la France, 83% de sa population utilisent internet et 68%, les réseaux sociaux. Dans cette économie informationnelle, il n'y a plus de récepteur « passif » au sens classique du terme mais des utilisateurs dont on peut suivre les traces numériques, et auxquelles les entreprises participant à cette économie des « big data » sont en mesure de proposer des anticipations de leurs besoins. Ainsi, cette révolution numérique modifie le *système organisateur des perceptions*[5] individuelles en plaçant continûment la condition humaine dans une situation interactive généralisée. En particulier, les modalités d'acquisitions culturelles sont en cours de reformatage compte tenu du fait que l'information devient accessible en un clic. Cela a pour effet une montée en puissance de revendications de connaissance plurielles qui se situeraient toutes sur un même plan de légitimité, avec le risque d'accentuer la confusion entre ce qui relève de l'opinion et ce qui relève d'un savoir produit par des institutions scientifiques. La deuxième caractéristique de cette révolution numérique est la forte croissance de l'internet des objets connectés dans le secteur de la santé marqué par une ambition prédictive à partir du recueil de renseignements personnels. Est-il possible que la santé mobile et connectée soit prise en charge par l'Assurance maladie ? Comment ces bénéfices seront-ils mesurés et quantifiés ?

Les institutions politiques sont touchées de plein fouet par cette révolution digitale. On assiste à une multiplication des objets numériques dans les débats parlementaires depuis que les salles de commission et l'hémicycle permettent un accès libre à internet. L'inflation de la communication électronique assigne aux regards extérieurs le statut de « publics vivants » au point que l'usage de Twitter est devenu une norme chez les députés[6]. En outre, le rapport des citoyens aux administrations devient de plus en plus dématérialisé et déterritorialisé, simplifiant ainsi le quotidien des administrés. Cette libération des données administratives, également en cours dans les collectivités territoriales, engendre des remaniements dans la manière administrative de travailler les données afin de les constituer en bien public. Elle bouleverse les conceptions de la *street-level bureaucracy* et distend les contacts entre citoyens et fonctionnaires. Le risque étant que ces derniers ne s'inscrivent plus dans un rapport situé, vivant avec leurs administrés et qu'ils n'incarnent plus les terminaisons de l'action publique. Les technologies digitales retentissent

donc sur la ***territorialité de l'État***. Un portail dédié à l'Open Data « data.assemblee-nationale.fr » a été récemment mis en ligne. Ces nouveaux modes d'archivage en voie de généralisation, plus exhaustifs, vont impacter sur la façon dont les citoyens de demain appréhenderont le passé de leurs institutions politiques. Les technologies digitales retentissent également sur la ***mise en mémoire de l'État***, susceptible de faire l'objet d'histoires concurrentielles.

Le modèle régalien de justice sociale est déstabilisé par les technologies digitales, à travers les dispositions de droit du travail (la mise à mal de professions réglementées par les sociétés Uber, Airbnb…), les démarcations entre vie privée et espace public (affaire Snowden, les réseaux sociaux), les enjeux sécuritaires (traçabilité des déplacements avec les objets connectés, cybercriminalité, renseignements personnels sur la santé) et les formes d'e-activisme (allant de la constitution de contre-pouvoirs au sein du monde arabe jusqu'aux formes d'embrigadements terroristes sectaires). Parce que les GAFAM retentissent sur la vie des individus et leur système de relations, il est indéniable que la perception classique d'un État Providence territorialisé, marqué par certains équilibrages économiques et par des règles particulières au regard des lois du marché dans un souci de justice sociale, risque d'être sérieusement affaiblie dans les années à venir. Si l'arrivée des médias télévisuels avait grandement modifié la communication politique, on peut penser que le numérique impliquera un renouveau de notre modèle de l'État-nation puisqu'il retentit sur sa matérialité, son système d'acteurs et sa logique symbolique.

2. Les fractures françaises. Les effets du numérique sur la représentativité politique

Pour certains analystes et entrepreneurs de politiques publiques, l'open data intervient comme un facteur de capacitation des citoyens (*empowerment*) parce qu'il donne accès à des ressources leur permettant de contribuer de façon plus éclairée au débat public. Au niveau de l'accompagnement de la décision publique, il est certain qu'une politique d'ouverture des données publiques est en mesure de faciliter la concertation entre les différents acteurs territoriaux et d'articuler les échelles décisionnelles. Ainsi, la publication en open data de cartes géo-localisées des accidents de la route ou des itinéraires pour personnes en fauteuil roulant est susceptible de constituer la base d'une concertation entre associations locales et municipalités et conduire à de meilleurs aménagements routiers et améliorer des services de proximité. Cela étant, si la constitution de biens publics numériques peut s'avérer précieuse en termes d'action publique, il n'est pas certain que la mise à disposition publique des big data suivant cette logique de transparence se traduise par une amélioration de la représentativité politique, ni par un accroissement de la proximité entre le citoyen et l'élu susceptible de répondre à la crise des corps intermédiaire et des institutions de médiation (média, partis, syndicats).

On assiste à une profonde crise de la représentation politique mais l'interprétation à donner à cette crise est très complexe. Il est tentant de

déduire que cette crise résulte d'un écart trop important entre la représentativité politique et la représentativité sociale, ce que certains traduisent par un besoin irrépressible de démocratie participative. De fortes nuances doivent être apportées à ce constat. Si les aspirations à la démocratie « horizontale », plus participative, sont présentes au niveau local, de même qu'une demande accrue de libertés privées, Pascal Perrineau souligne la coexistence avec une demande de démocratie verticale plus rigoureuse : « On veut revenir au marbre gaullien. On veut un De Gaulle, mais un De Gaulle postmoderne »[7], couplé à une forte demande de protection économique, voire culturelle. Ce paradoxe trouve en partie réponse dans le fait que « plus les individus réclament une liberté privée, plus le besoin d'un principe de régulation centrale se fait sentir »[8]. Si bien que l'intervention des technologies numériques dans la machine représentative (e-vote, communication des élus via les réseaux sociaux) est susceptible de faciliter l'acquisition d'informations dans le cadre de campagnes électorales et de participer à la simplification administrative des actes civiques. Pour autant, ces technologies ne seront probablement pas en mesure de jouer un vecteur de médiation entre le monde des citoyens et celui des gouvernants. Elles n'interviendront probablement pas de façon déterminante dans l'amélioration de la machine représentative mais seront susceptibles de mieux accompagner les décisions politiques au niveau local et de jouer sur la proximité.

- Quelques pistes pour accompagner le développement numérique dans la vie politique

  Le projet de loi pour une « République numérique » comporte déjà plusieurs dispositions visant à réduire la fracture numérique (création d'un service public de la donnée accessible à tous) et à faire émerger de nouveaux droits pour les citoyens. Néanmoins, il subsiste un impensé, difficilement traductible dans le droit, lié aux effets de la numérisation de la société sur la nature même de nos institutions.
- Tout d'abord, les institutions politico-administratives (place, statut et symbole du fonctionnaire qui n'est plus directement accessible par ses administrés ; impacts de la déterritorialisation des services publics sur les représentations de l'État)
- Ensuite, les institutions scientifiques (la démocratisation accrue des affaires scientifiques et l'efficacité rhétorique de certains blogs conduisant à un affaiblissement de la distinction entre opinion et savoir ; la participation ne peut pas remplacer l'acquisition classique de connaissances)
- Enfin, les institutions culturelles (comment définir leurs rôles dans une société où le défi n'est plus l'accès à l'information mais celui d'apprendre à hiérarchiser les différentes sources par ordre d'importance avec un souci de véracité ; leur place dans la lutte contre les embrigadements sectaires)

  À côté de ce travail juridique, une réflexion sociologique et anthropologique doit s'engager sur le régime institutionnel de nos sociétés numérisées.

(0) *Virginie Tournay remercie Bruno Cautrès, pour leurs échanges autour de ce texte, où il souligne l'importance des clivages politiques liés à la numérisation dans un monde globalisé. Pour une analyse des relations entre l'Union Européenne et ses citoyens, voir Cautrès (Bruno), Les Européens aiment-ils (toujours) l'Europe ?, Paris, Documentation française, Réflexe Europe-Débats, juillet 2014.*

[1] L'acronyme GAFAM faire référence aux quatre grandes firmes informatiques américaines **G**oogle, **A**pple, **F**acebook, **A**mazon et **M**icrosoft qui dominent le marché du numérique depuis ces dernières décennies. Certains auteurs lui préfèrent l'acronyme GAFAY (**Y**ahoo).

[2] Conseil national du numérique, *Rapport Ambition Numérique – Pour une politique européenne et française de la transition numérique*, à la demande du Premier ministre, 18 juin 2015.

[3] Une technologie est dite de « rupture » lorsqu'elle remplace ou/et renouvelle un mode de production de biens ou de services amenant à de nouveaux marchés. Clayton M. Christensen, *The Innovator's Dilemma*, Harvard Business School Press, 1997.

[4] Gérard Courtois, Gilles Finchelstein, Pascal Perrineau et Brice Teinturier, *Fractures françaises (1)*, Fondation Jean Jaurès, septembre 2015.

[5] Stéphane Vial, *L'être et l'écran – Comment le numérique change la perception*, PUF, 2013.

[6] Jonathan Chibois, Twitter a-t-il bousculé le droit parlementaire ?, *Politics & social media*, Nov. 2014, Dijon, France, Formes et fonctions de participation politique dans un monde numérique <halshs-01153633>

[7] Enquête réalisée par Ipsos/Steria pour la Fondation Jean-Jaurès, *Le Monde* et Sciences Po (programme « vie politique »), avril 2015, p. 22.

[8] Pascal Perrineau, ibid. p. 9.

Édition : Florent Parmentier **Mise en forme :** Marilyn Augé

Pour citer cette note : TOURNAY (Virginie) « La résilience de l'État face aux menaces informationnelles », *Sciences Po CEVIPOF*, juin 2025, 17 p.