Introduction

Françoise Daucé, Benjamin Loveluck, Francesca Musiani

▶ **To cite this version:**

Françoise Daucé, Benjamin Loveluck, Francesca Musiani. Introduction. Genèse d'un autoritarisme numérique. Répression et résistance sur Internet en Russie, 2012-2022, Presses des Mines, pp.13 - 32, 2023, 10.4000/books.pressesmines.9058 . halshs-04139487

HAL Id: halshs-04139487
https://shs.hal.science/halshs-04139487v1

Submitted on 23 Jun 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Françoise Daucé, Benjamin Loveluck et Francesca Musiani (dir.)

Genèse d'un autoritarisme numérique

Presses des Mines

Introduction

Françoise Daucé, Benjamin Loveluck et Francesca Musiani

DOI : 10.4000/books.pressesmines.9058
Éditeur : Presses des Mines
Lieu d'édition : Paris
Année d'édition : 2023
Date de mise en ligne : 1 juin 2023
Collection : Sciences sociales
EAN électronique : 9782385424244

OpenEdition Books

http://books.openedition.org

Référence électronique
DAUCÉ, Françoise ; LOVELUCK, Benjamin ; et MUSIANI, Francesca. *Introduction* In : *Genèse d'un autoritarisme numérique* [en ligne]. Paris : Presses des Mines, 2023 (généré le 07 juin 2023). Disponible sur Internet : <http://books.openedition.org/pressesmines/9058>. ISBN : 9782385424244. DOI : https://doi.org/10.4000/books.pressesmines.9058.

Introduction

Françoise Daucé, Benjamin Loveluck et Francesca Musiani

Le 24 février 2022, l'offensive militaire russe contre l'Ukraine s'accompagne d'un renforcement immédiat de la censure sur les médias ainsi que des contrôles et blocages de l'Internet en Russie. Le processus d'enrôlement d'Internet au service de la politique belliciste de l'État russe s'accélère brusquement et rend possible la mise au pas de l'espace public dans le contexte de la guerre. Celle-ci justifie le resserrement brutal du réseau d'emprises et de contraintes qui pesait déjà, tant sur les acteurs que sur les infrastructures numériques. D'un côté, la loi est amendée dans un sens plus restrictif, interdisant toute critique de l'armée ou toute évocation du terme « guerre » (qualifiée d'« opération militaire spéciale »). Elle conduit de nombreux médias à renoncer à leurs publications. Des poursuites pénales sont engagées contre les journalistes indépendants et les opposants à la guerre tandis que le registre des « agents de l'étranger », tenu par le ministère de la Justice, s'étoffe considérablement. De l'autre, le pouvoir bloque les plateformes de médias sociaux internationaux (Facebook, Instagram) et renforce son contrôle sur les acteurs numériques locaux (VKontakte, Yandex). Ces décisions interviennent alors que, sous l'effet des sanctions, des opérateurs numériques étrangers quittent le pays et déconnectent leurs infrastructures du réseau russe.

Comment cette dynamique autoritaire est-elle devenue possible dans un espace numérique qui fut libre à ses débuts ? Cette question se pose aussi dans d'autres pays comme l'Iran, la Turquie, le Pakistan, la Thaïlande, certains pays d'Asie du Sud ou d'Asie centrale, du Moyen-Orient et de l'Afrique, mais aussi des pays occidentaux où des traits de l'autoritarisme numérique sont discernables. Le cas de la Chine est particulier, dans la mesure où le développement numérique fut fortement encadré dès l'origine. La Russie présente aussi une trajectoire singulière, dans la mesure où les débuts de l'informatique connectée grand public ont été marqués dans les années 2000 par une forte activité entrepreneuriale, de nombreux opérateurs locaux répartis sur le territoire ainsi qu'un taux de pénétration d'Internet très rapide[1], dans un contexte de relatif laissez-faire. L'objectif de cet ouvrage est de comprendre la politique d'encadrement de l'Internet russe en la resituant dans une perspective historique qui remonte au début des années 2010, et de proposer une sociologie politique du numérique à partir des acteurs qui ont investi cet

1 Celui-ci passe de 15% à près de 60% entre 2005 et 2011 selon les données de l'International Telecommunication Union (https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=RU).

espace pour faire entendre leurs voix ou valoir leurs droits : fournisseurs d'accès, développeurs, journalistes, militants, professionnels du web, citoyens mobilisés. Alors que le réseau russe, né des initiatives plurielles et décentralisées des inventeurs du numérique, a longtemps porté les espoirs de démocratisation de la sphère publique russe, comment les emprises se sont-elles constituées dans le temps long, s'ajustant aux spécificités du web[2] et à l'inventivité de ses défenseurs ?

Autoritarisme et numérique

Avant même le début de la guerre en Ukraine, mais plus encore après, la tournure prise par le régime politique russe relance les débats sur sa qualification. La notion d'autoritarisme semble datée pour le décrire, comme le constatent Sergei Guriev et Daniel Treisman [2022] qui proposent d'en renouveler l'analyse par la notion de « *spin dictators* » pour décrire des régimes politiques fondés sur la manipulation du débat public et la simulation des mécanismes démocratiques plutôt que sur la peur et la violence directe. Cependant, après les destructions commises par l'armée russe en Ukraine, à partir de février 2022, et face à la brutalité de la répression sur le plan domestique, la notion d'autoritarisme peut sembler faible, certains observateurs n'hésitant plus à qualifier le régime de fasciste. Cette position est notamment défendue par des intellectuels comme Alexander Motyl [dès 2016] ou Timothy Snyder [2022] qui estiment que le fascisme peut être ici défini comme un système autoritaire populaire fondé sur une dictature personnelle et le culte du leader mais aussi sur le culte des morts et le mythe de l'âge d'or du passé impérial. Cette position ne fait pas l'unanimité. Marlène Laruelle [2021 et 2022] considère ainsi que la Russie n'est pas fasciste car le pouvoir ne s'appuie pas sur la mobilisation des masses mais profite plutôt de l'atomisation de la société. La dynamique impérialiste a cependant été ouvertement réactivée et s'est focalisée sur l'Ukraine, déjà lors de l'intervention dans le Donbass et l'annexion de la Crimée en 2014 et de manière plus brutale encore lors de l'invasion lancée en février 2022.

Comme le souligne David Lewis [2020], pendant longtemps la Russie a été présentée comme un « régime hybride » associant des éléments issus d'un passé autocratique et totalitaire (persécution des dissidents, censure des médias, violations de la loi par les élites) avec cependant des caractéristiques relevant de

2 Soulignons ici la différence entre « Internet » et « Web », bien que les deux termes soient trop souvent utilisés de manière interchangeable dans le discours quotidien. Internet est le système mondial de réseaux informatiques interconnectés qui utilisent un « langage commun » – à savoir la suite de protocoles Internet – pour communiquer entre eux. Le Web, ou World Wide Web (WWW), est un ensemble particulier d'applications construites au-dessus d'Internet, l'une des plus largement utilisées par les utilisateurs finaux (avec, par exemple, le partage de fichiers et les applications de messagerie électronique).

l'ordre libéral international (intégration à l'économie mondialisée, pénétration des normes libérales, adoption des nouvelles technologies). Mais selon Lewis, le poutinisme est ancré avant tout dans un paradigme schmittien, qui a d'abord vu l'émergence d'une forme spécifique de « démocratie illibérale », où les normes juridiques peuvent être transgressées par le pouvoir en place si cela permet de maintenir « l'ordre ». Cette logique bien connue conduit à établir une distinction ami/ennemi, où la population russe est sans cesse présentée comme menacée par les critiques et par les minorités, identifiées comme une « cinquième colonne » œuvrant pour des puissances étrangères et visant à saper à la fois les « valeurs traditionnelles » russes et la sécurité de l'État. Depuis plus d'une dizaine d'années, cette distinction est allée croissant et a permis de jeter un voile de suspicion de plus en plus marqué sur toutes les voix discordantes – en particulier les journalistes indépendants, les militants des droits de l'Homme, les opposants politiques.

Les formes plus établies de l'espace public – notamment les médias audiovisuels mais aussi les manifestations physiques – ont été les cibles premières de l'emprise répressive exercée par le pouvoir, comme cela a été bien documenté. Dans ce contexte, l'espace numérique a semblé offrir des opportunités pour tous ceux qui cherchaient à comprendre, à s'exprimer et à s'organiser mais qui ont dû, pour ce faire, imaginer des détours techniques et emprunter des chemins de traverse numériques. Ils ont été aidés par de nombreux acteurs moins visibles : informaticiens, développeurs, techniciens des réseaux, professionnels du web qui ont constamment inventé de nouvelles parades, permettant de ruser à la fois avec la législation et les contraintes techniques. Pour ces derniers, s'il s'agissait parfois avant tout de permettre à leur activité économique de perdurer, nombreux sont ceux qui se sont politisés à l'épreuve des frustrations, des entraves et des intimidations.

Ce sont ces voix discordantes mais aussi leurs nombreux porte-voix numériques, avec leur savoir-faire et leurs outils, qui sont au cœur de cet ouvrage. Nous avons cherché à saisir à la fois les contraintes pesant sur l'information et la communication en Russie et les pratiques concrètes des acteurs cherchant à s'en défaire. Pour tous ceux-là, les « libertés numériques » sont devenues un enjeu palpable, quel que soit leur bagage technique et quel que soit leur degré d'engagement politique. Il leur a fallu composer avec une législation de plus en plus complexe et délibérément ambivalente, permettant aux autorités de mettre en place – comme dans l'espace physique – une forme d'arbitraire destiné à intimider et contraindre à l'auto-censure en ligne. Celle-ci est allée de pair avec l'installation de dispositifs technologiques visant à censurer automatiquement les publications et à surveiller les communications personnelles.

Le détour par le monde numérique permet de sortir de la dialectique opposant la dictature personnelle du chef au peuple atomisé car il offre l'opportunité de penser l'oppression en réseau [Lokot, 2020]. La guerre favorise le resserrement des nombreux nœuds du web pour mettre en péril l'intégrité numérique et physique des citoyens critiques. Les contraintes distribuées et plurielles qui quadrillent l'espace numérique s'articulent à diverses échelles et en divers lieux au service du projet belliciste et impérialiste de l'État russe. Ni « verticale du pouvoir », ni « horizontale de la soumission », la contrainte s'installe dans l'articulation entre dispositifs numériques et dispositifs sécuritaires. Elle se joue dans les milieux intermédiaires de la surveillance de proximité, de l'autonomie des services locaux, des interprétations arbitraires de la loi, des incitations économiques à obéir, des voisins qui surveillent… Au-delà de la Fédération de Russie, ce maillage oppressif s'étend progressivement aux territoires et zones de guerre sous domination de l'État russe hors de ses frontières (Crimée et autres zones occupées en Ukraine, territoires dominés de Transnistrie, d'Abkhazie, d'Ossétie…) Pour ceux qui dénoncent l'oppression, les interstices de liberté et les compromis discrets se réduisent encore. Dès le début de la guerre, de nombreux militants, activistes, journalistes et citoyens qui s'y opposaient ont été contraints de quitter la Russie pour retrouver, à l'étranger, leur intégrité physique et numérique. Ils croisent en exil les millions de citoyens ukrainiens chassés par l'agression militaire contre leur pays.

Le développement des nouvelles technologies de l'information et de la communication a d'abord suscité l'espoir d'un passage à la « démocratie Internet » [Cardon, 2010] et a été investi d'un pouvoir de « libération » [Diamond, 2010], qui a culminé au moment des « révolutions arabes » où le numérique a largement été présenté comme un vecteur de démocratisation [Howard & Hussain, 2013]. Internet a également longtemps été perçu comme l'incarnation même des valeurs libérales d'autonomie individuelle, de transparence, d'ouverture et d'organisation collective distribuée, le modèle du réseau venant s'opposer aux paradigmes hiérarchisés et stato-centrés [Loveluck, 2015a, 2015b] – avant que l'inquiétude et la déception ne s'installent face à de nombreuses menaces nouvelles associées au numérique (collecte et exploitation des données personnelles, capitalisme de surveillance, manipulation et déstabilisation des processus démocratiques, etc.) mais aussi une ré-affirmation plus générale des prérogatives de l'État dans sa gouvernance [Tréguer, 2019 ; Haggart et al., 2021].

Certains travaux avaient déjà tempéré l'optimisme dominant en montrant que les régimes autocratiques pouvaient tout à fait s'accommoder d'internet voire le mettre à leur service [Kalathil & Boas, 2003 ; Boas, 2006 ; Morozov, 2011]. Mais c'est seulement dans la période plus récente, et dans le contexte d'un recul démocratique global [Diamond et al., 2016; Waldner & Lust, 2018], que la notion d'« autoritarisme

numérique» s'est imposée pour décrire l'usage des technologies de l'information par les régimes autoritaires pour surveiller, réprimer et manipuler les sociétés [Glasius & Michaelsen, 2018]. Le fait que les pouvoirs répressifs cherchent à interférer directement avec les flux d'information et de communication à travers des actions de censure, de surveillance arbitraire et de désinformation n'a rien d'inédit. Cependant, exercer un contrôle sur ces nouveaux espaces d'information, d'expression et de mobilisation demande de s'adapter à leurs spécificités, exige un certain nombre de ressources et de compétences – et offre également de nouvelles opportunités répressives [Keremoğlu & Weidmann, 2020 ; Feldstein, 2021]. Les plateformes de médias sociaux par exemple, qui ont un temps symbolisé le pouvoir émancipateur du numérique, se présentent désormais sous un jour beaucoup plus ambivalent, non seulement en raison de leurs dérives propres (circulation des discours de haine, politiques de modération de contenus, biais algorithmiques, captation de données personnelles, etc.) mais aussi parce qu'elles sont vulnérables à des formes de cooptation et de manipulation qui peuvent renforcer la mainmise des pouvoirs autocratiques sur leurs populations [Gunitsky, 2015 ; Deibert, 2019].

La Chine fait figure d'exemple le plus abouti d'autoritarisme numérique, à travers l'immixtion des services de l'État dans les infrastructures et les services, le filtrage des accès, la sophistication des dispositifs automatisés de censure, les ressources techniques et humaines mobilisées pour manipuler les discours et l'opinion (*wǔmáo dǎng* ou «parti des 50 centimes») ainsi que l'efficacité de la surveillance et de la répression [Han, 2018 ; Roberts, 2018 ; Liang et al., 2018]. Cependant la notion est aussi employée pour décrire les usages répressifs d'Internet au Moyen-Orient [Jones, 2022], au Pakistan [Jamil, 2021] ou encore au Zimbabwe [Mare, 2020]. Certains éléments d'autoritarisme numérique sont parfois également manifestes au sein des démocraties libérales à travers les pratiques de surveillance de masse ou certains cas de censure [Hintz & Milan, 2018], ainsi que par l'autorisation accordée à des entreprises privées de vendre des solutions techniques de filtrage et de surveillance à des acteurs violant les droits humains[3].

À la différence de la Chine, l'autoritarisme numérique en Russie a initialement pu être qualifié de *low-tech* et *low-cost* car ne s'appuyant pas sur des capacités de filtrage automatisé très poussées [Morgus, 2018 ; Lamensch, 2021]. Il reposerait davantage sur l'instrumentalisation du droit ainsi que sur l'auto-censure et l'intimidation des fournisseurs d'accès Internet et téléphonique, des entreprises privées et de la société civile [Polyakova & Meserole, 2019], sans être pour autant moins efficace. Comparé au modèle chinois, le contrôle exercé par le pouvoir russe sur Internet s'est développé de manière plus réactive et *ad hoc*, mais se présente aussi comme plus

3 Ce fut le cas des français Amesys et Nexa vers l'Egypte et la Libye [Tesquet, 2020], ou encore de l'israelien NSO vers de nombreux acteurs tels le régime saoudien mais aussi les cartels de la drogue mexicains [Marczak et al., 2018].

décentralisé, plus flexible et moins coûteux [Howells & Henry, 2021]. Les méthodes employées pourraient bien, à l'avenir, servir de canevas pour d'autres pays.

Le maillage coercitif de l'Internet russe

Contrairement au grand *Firewall* en Chine, l'Internet russe s'est d'abord développé librement, laissant l'initiative à de nombreux acteurs publics ou privés, dotés d'un bagage technique ou simple citoyens expérimentant et inventant des outils numériques ajustés à leurs usages. Dans les années 1990, le pays a connu une période de dérégulation économique brutale, qui a durement affecté le niveau de vie de la population mais qui a laissé libre cours aux premiers innovateurs de l'Internet russe (fournisseurs locaux d'Internet, importateurs d'ordinateurs, premiers éditeurs en ligne…). À l'époque, le contexte politique reste ouvert aux collaborations internationales, permettant la circulation des personnes et des biens numériques. La Russie est déjà en guerre (contre son propre parlement en 1993, contre la Tchétchénie en 1994 et à nouveau en 1999) mais l'espace public médiatique est peu régulé, voire laissé aux dérives des groupes oligarchiques qui possèdent les principaux médias d'information. En regard, l'espace numérique porte les promesses d'une démocratisation vertueuse, fondée sur la participation horizontale des citoyens et susceptible d'échapper aux jeux de pouvoir et d'argent.

La première décennie du siècle, après l'élection de Vladimir Poutine à la présidence russe en 2000, est marquée par le paradoxe politico-numérique de « demi-liberté d'expression » [Gelman, 2010], avec d'un côté le développement rapide d'un Internet libre et de l'autre le renforcement d'une gouvernance politique verticale et autoritaire. Au début des années 2000, le web russe et son ouverture sur le monde suscitent des espoirs de démocratisation et de mobilisation *offline* [Gladarev & Lonkila, 2012 ; Etling et al., 2010]. Le large mouvement de protestation contre les fraudes lors des élections parlementaires et le retour de V. Poutine à la fonction présidentielle (après un jeu de chaises musicales avec son ancien premier ministre Dmitri Medvedev), à l'hiver 2011-2012, représente un tournant. Il incarne le potentiel civique du web, permettant aux manifestants de coordonner leurs actions, de diffuser leurs slogans et de structurer le mouvement. Il bénéficie du développement des applications mobiles des médias sociaux internationaux (LiveJournal, Facebook, Twitter) et nationaux (Odnoklassniki, VKontakte).

À cette époque, le Runet (à comprendre comme l'Internet « russophone ») est ouvert sur le monde. Par sa plasticité, cet espace numérique dépasse les frontières nationales. Il est lu et consulté par les citoyens dans l'ensemble du pays mais aussi par les populations russophones vivant hors des frontières (ex-citoyens soviétiques des États devenus indépendants, étudiants et expatriés installés en

Europe ou en Amérique du Nord, autres voyageurs circulant à travers le monde). Dans l'« étranger lointain », le Runet relie les communautés russes émigrées, notamment aux États-Unis, en Israël et en Europe [Fialkova & Yelenevskaya, 2005 ; Morgunova, 2012]. La richesse et la qualité des contenus numériques mettent en lumière la diversité des idées, des projets et des groupes qui alimentent l'Internet russe, des plus conservateurs aux plus révolutionnaires. Cependant, la notion même de Runet traduit un repli progressif sur un imaginaire national imposé par les élites au pouvoir [Asmolov & Kolozaridi, 2017]. Le Runet, en s'adressant à tous les publics du « monde russe », devient un outil parmi d'autres du projet politique impérial des autorités russes dans son étranger proche et lointain, voire même un outil du « cyber impérialisme » [Uffelmann, 2014]. Au-delà du Runet et des publics russophones, les programmes en langues étrangères de RT ou Spoutnik [Audinet, 2021] témoignent également de l'expansionnisme médiatique de l'État russe, appuyé sur les outils numériques.

Au début des années 2010, les réglementations de plus en plus strictes imposées par le gouvernement mettent à mal les libertés en ligne [Oates, 2013 ; Konradova & Schmidt, 2014 ; Soldatov & Borogan, 2015]. La législation russe s'alourdit, illustrant la volonté du gouvernement d'établir un contrôle national sur une arène numérique qui lui avait jusqu'alors échappé. La réélection de V. Poutine pour un troisième mandat, en 2012, puis pour un quatrième, en 2018, s'accompagne d'un durcissement politique proportionnel au déclin de la légitimité démocratique du chef de l'État. Les institutions du pays (parlement, autorités régionales, partis politiques, élections) sont vidées de leur substance dans le cadre du projet de « démocratie souveraine » porté par le pouvoir. Les citoyens sont incités à se rallier au discours patriotique et réactionnaire des autorités, ou réduits à la marginalisation aux confins de l'espace public pour exprimer leur mécontentement ou leurs critiques.

Les mesures de régulation nationale du web démontrent les réponses coercitives choisies par les autorités face aux défis que l'Internet pose à la souveraineté. Cette politique de recentrage national du Runet, appuyée notamment sur un arsenal législatif au service des objectifs du pouvoir, a été bien documentée [Nocetti, 2015 ; Stadnik, 2021]. Roskomnadzor (RKN), l'organisme de contrôle des communications instauré en 2008, a vu sa juridiction et sa portée s'étendre rapidement à des domaines aussi variés que le contrôle des contenus en ligne, un droit de blocage des sites web et l'enregistrement des sites bloqués sur des listes noires, avec une possibilité de censure sensiblement accrue. Ce contrôle repose sur son important réseau de relations et de collaborations avec l'ensemble des institutions de sécurité de l'État à toutes les échelles du pouvoir, fédéral et régional. Le ministère de l'Intérieur (MVD), le Service fédéral de sécurité (FSB), les institutions judiciaires, le Parquet et les diverses agences de contrôle (de la

santé, de la consommation, de la jeunesse, des impôts, etc.) constituent le tissu régalien qui quadrille la société et relaie les directives élaborées au sommet de l'État. Il peut également être soutenu, au niveau local, par les associations conservatrices de citoyens mobilisés au service du maintien de l'ordre, en ligne et hors ligne (cyberpatrouilles, mouvements de vigilantisme, « patriotes », cosaques – voir [Daucé et al., 2019]).

Dans l'espace numérique, le contrôle s'exerce avant tout à travers les acteurs qui maintiennent et font fonctionner l'Internet, et qui proposent des solutions de connectivité aux utilisateurs (opérateurs de télécommunication, fournisseurs d'accès à Internet, hébergeurs de sites web, moteurs de recherche, plateformes de réseaux sociaux, entreprises de services numériques, développeurs et techniciens, concepteurs d'algorithmes…) [DeNardis, 2012 ; 2014]. Ceux-ci se voient imposer sans cesse de nouvelles contraintes juridiques et techniques. S'agissant de la censure par exemple, il s'agit de contraindre ces intermédiaires à implémenter la politique voulue par les autorités en les tenant pour responsables en cas d'infractions. Cette démarche, connue sous le nom de *intermediary liability* [MacKinnon et al., 2014]), n'est pas propre à la Russie et s'est même généralisée dans le contexte de la modération de contenus sur les plateformes [Gillespie, 2018], mais à la différence d'autres pays le contexte juridique russe est mouvant, aisément instrumentalisé et laissant peu de place aux contre-pouvoirs (contrôles constitutionnels) et aux possibilités de recours (bien qu'ils existent). Cependant, les utilisateurs eux-mêmes, en particulier sur les plateformes de réseaux sociaux telles que Twitter ou VKontakte, peuvent aussi être aisément et directement incriminés en vertu des lois permettant de sanctionner sur le plan pénal de simples partages (*reposts*) ou « j'aime » (*likes*) de publications en ligne [Van der Vet, 2020].

Pour mieux encadrer ces services, au cours des dernières années, les autorités russes se sont activement orientées vers une autonomisation et une « souverainisation » du Runet par l'adoption de nouvelles lois visant à contrer l'influence des entreprises étrangères, à mieux contrôler les échanges de données avec l'extérieur et à isoler le réseau russe en cas de « menace ». Cette tendance est illustrée par la loi sur l'Internet souverain, adoptée en 2019 dans le but officiel de protéger le pays contre les cyberattaques [Musiani et al., 2019], et la « loi contre Apple », adoptée en 2020 contraignant les constructeurs à pré-installer des applications « de fabrication russe » sur les smartphones. La démarche de « souverainisation » de l'Internet russe – anticipant peut-être les fractures que l'expansionnisme russe ne manquerait pas de provoquer – prévoit notamment un contrôle accru des interconnexions vers les autres pays et une possibilité d'isoler le segment russe du reste d'Internet, ainsi que le déploiement auprès des opérateurs et fournisseurs d'accès de systèmes plus aboutis de filtrage automatisé (systèmes d'inspection de paquets dits TSPU ou « Moyens techniques

de lutte contre les menaces » permettant de bloquer ou de ralentir le trafic en ciblant des protocoles, des services ou des adresses spécifiques). Cette volonté de faire coïncider les frontières géographiques avec les frontières numériques s'accompagne d'une centralisation croissante du réseau et d'une concentration des opérateurs [Limonier, 2021]. Au fil des contraintes légales, techniques et économiques, qui s'accumulent, les acteurs d'Internet, initialement très divers et relativement indépendants, se trouvent enrôlés bon gré mal gré dans la genèse de l'autoritarisme numérique.

Cependant, cette politique de contrôle ne doit pas nécessairement être considérée comme parfaitement verticale, cohérente et hiérarchique. Les lois s'appliquant à l'activité en ligne sont nombreuses, variées, en constante adaptation : initialement dirigées contre le terrorisme, la pédopornographie, ou encore l'apologie du suicide, puis contre les activités « extrémistes » ou les appels à manifester, elles ont rapidement vu leur périmètre s'élargir tout en demeurant vaguement définies. Leur application est souvent aléatoire ou arbitraire. L'examen attentif de la législation et de son application ne montre pas une domination centralisée d'Internet mais plutôt une multiplicité de types de contrôle, partiels, fluctuants et parfois contradictoires. Les contrôles juridiques peuvent s'ajuster de diverses manières aux dispositifs techniques (algorithmes) ou aux caractéristiques économiques (profilage) de l'activité en ligne, mais ils demeurent toujours imparfaits, laissant des espaces limités d'action pour les opposants numériques et leur agilité technique. Les pouvoirs publics échouent même, parfois, à mettre en œuvre leur propre politique répressive sur Internet, comme en témoigne, en 2018, leur incapacité à bloquer l'application Telegram sur le sol national [Ermoshina & Musiani, 2021].

Formes et limites des résistances numériques

Il est essentiel de comprendre la diversité et l'imperfection des contraintes qui s'appliquent au web et à l'Internet russes pour saisir les nombreuses formes de résistance, d'évasion et de contournement qui se sont développées en réaction à ces contraintes. Au cours des années 2000, lors de la construction de l'Internet russe, les potentielles restrictions techniques sont restées le plus souvent invisibles pour ses utilisateurs [Deibert & Rohozinski, 2010]. Depuis les années 2010, les répressions qui ont surgi en réponse au développement de l'activisme citoyen [Clément et al., 2010] ou aux grandes manifestations contre la fraude électorale en 2011 et 2012 [Gabowitsch, 2017] ont favorisé l'émergence de savoirs critiques concernant les usages d'Internet. Des initiatives et des compétences militantes se sont développées, y compris avec l'aide de formateurs à la sécurité numérique [Bronnikova & Zaytseva, 2021], contribuant à la diffusion de savoirs alternatifs dans la société pour contourner les barrières qui s'érigent en ligne. Les militants

d'opposition et les journalistes indépendants ont appris à moissonner les données ouvertes ou fuitées pour mener leurs enquêtes et dénoncer la corruption des élites. Les citoyens mécontents ont créé des boucles de discussion sur les applications sécurisées (Telegram, Signal) pour coordonner leurs actions. Confrontés progressivement au tournant oppressif à partir du début des années 2010, les opérateurs techniques, les défenseurs des libertés d'Internet, les militants, les journalistes, mais aussi des citoyens ordinaires, se sont heurtés aux multiples contraintes qui enserrent l'Internet russe mais ont élaboré des critiques et des contournements qui, sans cesse, par leurs usages numériques hétérodoxes, viennent défier les codes de l'autoritarisme.

Cet ouvrage propose une sociologie de l'Internet russe qui s'appuie sur un ensemble d'enquêtes, menées entre 2018 et 2022 auprès des mouvements, des organisations et des citoyens mobilisés qui constituent un public engagé face aux atteintes aux libertés numériques. Il met l'accent sur les multiples objets numériques au cœur des controverses politiques et des tensions d'usage dans l'espace virtuel russe dans la période récente. Il montre les processus de construction de l'oppression numérique, au fil des critiques, conflits et contournements qui mettent aux prises tant les acteurs publics que privés, tant les partisans de l'ordre du net que les défenseurs de ses libertés. Les travaux académiques sur la « désobéissance » et la « résistance » à la domination sont prolifiques, en histoire, en sciences politiques et en sociologie, et ont montré que l'ordre institutionnel ne peut être imposé sans un certain arrangement dans la distribution des rôles prescrits [Hmed & Laurens, 2011]. S'il s'avère souvent difficile d'identifier une « résistance » cohérente et organisée, les chercheurs ont montré comment celle-ci peut prendre la forme de compétences et d'arts de faire [de Certeau, 1990], d'actions de basse intensité, discrètes ou souterraines qui relèvent de l'« infra-politique » [Scott, 2009], ou encore d'évitements, de contournements, de piratages [Keucheyan & Tessier, 2008].

Sur Internet, de nouvelles formes de protestation en ligne se sont développées contre les politiques gouvernementales de surveillance du réseau [Best & Krueger, 2008 ; MacKinnon, 2012]. Certaines peuvent impliquer des voix publiques visibles et un « médiactivisme » ostensible [Cardon & Granjon, 2013], d'autres au contraire l'anonymat et l'obscurcissement [Brunton & Nissenbaum, 2015]. Elles renvoient aussi bien à des multitudes d'actions individuelles à bas bruit, qu'à des initiatives visant à transformer le paysage numérique en Russie, en prise directe avec les autorités – comme l'illustre la trajectoire du cofondateur de VKontakte Pavel Dourov : celui-ci dirigea le réseau social jusqu'en 2014 avant de quitter le pays face à une pression croissante, ayant entre-temps fondé la plateforme Telegram qui, en vertu de ses spécificités techniques et de son extra-territorialité, fait valoir une plus grande résistance à l'interventionnisme du pouvoir [Maréchal, 2018].

Les modèles dérivés des mouvements hors ligne et ceux façonnés par les technologies en réseau coexistent et s'hybrident. Ainsi en septembre 2021 lors des élections législatives, le mouvement de Navalny propose aux électeurs une application de *smart voting* (vote utile) permettant d'identifier, dans chaque circonscription, le candidat le plus à même de battre le représentant du parti présidentiel Russie Unie : une vive bataille technique les oppose aux autorités essayant par tous les moyens de neutraliser l'application, qui aboutit même à une injonction inédite faite à Google et Apple – leurs représentants étant menacés de poursuites pénales et les bureaux du premier investis par des huissiers armés – pour qu'ils la retirent de leurs *app stores*[4]. Il est donc important de comprendre la résistance du net en tenant compte également de ses dimensions techniques, matérielles et logicielles, de l'infrastructure en constante évolution qui anime l'Internet, le maintient ensemble ou le fragmente, et qui est le lieu d'intenses batailles de gouvernance [DeNardis, 2014].

Plusieurs des enquêtes présentées dans ce livre s'intéressent de près aux infrastructures, dispositifs techniques et interfaces impliqués dans la surveillance et la censure, tels que les boîtiers de filtrage du trafic Internet, les algorithmes de classement des nouvelles, ou encore les caméras de surveillance. Ces outils de contrôle, souvent invisibles aux yeux des utilisateurs, sont dévoilés par les militants et les citoyens confrontés à leur usage répressif. Les conflits autour du développement de ces technologies et de leurs usages montrent que les stratégies de résistance et de contournement passent aussi « par l'infrastructure » [Daucé & Musiani, 2021]. En effet, face à l'emprise croissante du gouvernement russe, la confrontation politique directe est devenue de plus en plus difficile et risquée.

De plus, un certain nombre de conduites, que l'on peut qualifier de ruses juridiques, ou encore, de résistances par les pratiques et les usages, sont apparues en réponse à l'évolution de la législation. Les « résistants numériques » russes inventent de nouvelles astuces techno-juridiques qui défient le législateur. Au fil des enquêtes apparaissent des individus et des groupes, militants ou « simples » citoyens, qui, conscients des enjeux numériques des libertés publiques, mènent des actions de plaidoyer (critique des lois, élaboration de régulations alternatives), de défense des usagers réprimés (engagement d'avocats spécialisés, soutien aux militants poursuivis) ou encore de sensibilisation à la sécurité numérique (formateurs, webinars). Ils agissent cependant dans un contexte d'incertitude et leurs stratégies ne doivent pas nécessairement être interprétées comme suivant un modèle cohérent et durable.

4 « Google and Apple, under pressure from Russia, remove voting App », *The New York Times*, 17 septembre 2021 (https://www.nytimes.com/2021/09/17/world/europe/russia-navalny-app-election.html).

De multiples formes de désobéissance, de contournement, de piratage ou d'obfuscation traversent en effet l'espace numérique russe mais leur montée en généralité politique est généralement entravée. Parmi les usagers habiles qui savent accéder aux sites bloqués grâce à des réseaux privés virtuels (*virtual private networks* ou VPN), protéger leur correspondance privée par le chiffrement, sécuriser leur ordinateur par double authentification, tromper le censeur par des sites miroirs, rares sont ceux qui revendiquent un engagement politique dans la sphère publique. La plupart assurent au contraire « ne pas faire de politique ». Face aux entraves autoritaires, un processus d'évitement de la politisation est manifeste, à l'exemple du Parti pirate de Russie qui fonde en 2012 une association s'affichant comme « non politique », Roskomsvoboda[5], pour continuer à défendre légalement la liberté d'Internet en Russie [Daucé, 2022].

Euphémisation et détours sont de mise pour accéder à l'Internet libre sans éveiller l'attention des services de sécurité ou de la censure. Les outils et les pratiques de contournement n'ont d'ailleurs pas tous vocation à favoriser l'accès à des contenus politiques, ils permettent aussi de consommer sans payer des biens culturels comme la musique, les films ou les livres. Au point que l'on peut parfois se demander s'ils ne contribuent pas à l'acceptabilité de la censure et à l'affaiblissement du sentiment de révolte face aux atteintes aux libertés fondamentales. Ceux qui s'essayent à la résistance et à l'opposition, à l'instar de la Fondation de lutte contre la corruption (FBK) d'Alekseï Navalny, de la Société de défense d'Internet (OZI) [Klimarev, 2022] ou encore des citoyens mobilisés pour défendre l'environnement à Shies, dans le grand nord [Poupin, 2022], doivent affronter les multiples attaques du pouvoir. A. Navalny en fait cruellement les frais, d'abord empoisonné par les services de sécurité en 2020 puis emprisonné pour de longues années. Face aux menaces, nombre de ses partisans sont contraints à l'exil pour échapper aux poursuites criminelles. C'est depuis l'étranger qu'ils peuvent renouer avec la politique et mettre les outils numériques au service d'un projet d'opposition au pouvoir russe en place. Pour les citoyens mobilisés qui restent en Russie, le combat est difficile, les plaçant sous la menace permanente de la répression en ligne et hors ligne.

Présentation et structure de l'ouvrage

Le livre est nourri par les enquêtes de terrain réalisées dans le cadre du projet ANR ResisTIC (« Les résistants du net. Critique et évasion face à la coercition numérique en Russie, 2018-2022 »). Pendant cinq ans, l'équipe du projet a étudié la façon dont

5 Le nom de cette association est un détournement ironique du nom de l'Agence de surveillance des communications (Roskomnadzor), transformé en « Agence de la liberté des communications » (Roskomsvoboda)

différents acteurs du Runet résistent et s'adaptent aux réglementations autoritaires et centralisatrices. Le projet s'est intéressé particulièrement à la résistance en ligne et aux pratiques sociales et techniques moins connues déployées pour contourner les contraintes. Il a été initialement construit autour de trois axes de recherche : « Luttes expertes pour les libertés en ligne », « Professionnels du public à l'épreuve de la régulation du net » et « Migrations et résistances depuis l'étranger ». Ces axes ont évolué au fil du temps et des difficultés rencontrées sur le terrain (répressions, pandémie, guerre et exil). Les compétences multiples des membres de l'équipe ont permis de faire face collectivement à ces épreuves partagées pour parvenir au terme du projet.

Cet ouvrage offre un aperçu détaillé des différentes recherches menées, au carrefour des mobilisations critiques, de la souveraineté numérique, des données et des infrastructures – tant au niveau de leur développement que de leurs usages, souvent très créatifs et subversifs. Il offre une analyse des transformations de l'Internet russe à partir de différentes disciplines (la sociologie, la science politique, le droit et l'anthropologie), de différents acteurs (associations, entreprises, administrations, médias, éditeurs, militants…) et de différents objets (câbles, plateformes, algorithmes, données, réseaux sociaux, *posts*, *blogs*, *tchats*…). Il est complété par une frise chronologique (*timeline*) élaborée au fil du projet qui recense, sans prétention à l'exhaustivité, les nombreux événements qui, dans leur diversité et leurs contradictions, ont marqué les évolutions récentes de l'espace numérique russe. Disponible en accès ouvert (https://timeline.resistic.fr/), la frise offre, en complément de ce livre, une riche illustration des contraintes oppressives et des critiques pour la défense des libertés numériques qui se déploient tout au long des années 2010, jusqu'à l'invasion russe à grande échelle de l'Ukraine en février 2022.

Les analyses présentées dans les chapitres qui suivent s'appuient sur des données originales, tant quantitatives que qualitatives. Une centaine d'entretiens au total ont été menés, ainsi que de nombreuses observations participantes, ethnographies en ligne, collectes de données numériques, etc. Outre les études de cas elles-mêmes, un point d'attention récurrent a consisté à évaluer les méthodes d'enquête de manière réflexive, compte tenu notamment de la situation de vulnérabilité de certains enquêtés. S'engager sur le terrain en Russie présentait des difficultés en raison des contraintes pesant sur les chercheurs et de la nécessité de ne pas mettre en difficulté – voire en danger – les personnes interrogées. Le caractère sensible de nos enquêtes n'a pu que s'accroître au fil des années, avec des bouleversements profonds qui ont bien sûr eu lieu à partir de février 2022. Tout au long de la recherche, une vigilance permanente a été portée à la sécurité des données collectées, à la fiabilité des réseaux de communication utilisés et à la protection des sources archivées. Les membres du projet ont eux-mêmes suivi

une formation à la sécurité numérique pour s'ajuster à un contexte d'enquête en permanente évolution. Cette expérience collective a permis de montrer que, au-delà d'une vision normative et protocolaire de la sécurité numérique, cette dernière résulte d'abord d'un dialogue permanent avec les acteurs concernés pour négocier ensemble les règles d'une sécurité partagée.

Le livre débute par une présentation du cadre normatif et législatif qui encadre l'Internet russe et qui grossit au fil des années, au prix d'une inflation de règles qui régulent de multiples aspects des activités numériques, des plus matérielles (les câbles) aux plus volatiles (les données) (chapitre 1). L'analyse se développe ensuite à partir de deux observatoires qui permettent de saisir l'autoritarisme numérique au concret : les boîtiers de filtrage des contenus et de surveillance de trafic imposés aux Fournisseurs d'accès Internet (chapitre 2) et les algorithmes de classement des nouvelles comme celui de Yandex (chapitre 3).

En regard des contraintes déployées, des savoirs émergent pour se protéger de la surveillance et des contrôles sur le Runet, grâce notamment aux formations dispensées par les spécialistes de la sécurité numérique aux militants critiques (chapitre 4). De leur côté, les journalistes apprennent à travailler avec les données numériques pour mener leurs investigations alors que les contrôles sur les médias se renforcent (chapitre 5). Les éditeurs et les libraires, quant à eux, découvrent à la fois les contraintes et les opportunités de la diffusion en ligne des livres, face aux usages politiques de la lutte contre le piratage (chapitre 6). Ces expériences fondent des apprentissages qui s'éloignent du déterminisme technologique pour renouer avec les subtilités de savoirs socialement situés.

Dans cet environnement fait de contraintes et de libertés croisées, les militants critiques et les citoyens mobilisés sont confrontés à des épreuves complexes, les conduisant à faire le choix d'outils numériques ajustés à leurs engagements (chapitre 7). Quand les risques numériques viennent menacer la sécurité physique des personnes, notamment à partir de l'agression militaire de la Russie contre l'Ukraine, seul l'exil permet de retrouver une intégrité physique et numérique qui peut donner lieu à de nouveaux engagements militants depuis l'étranger (chapitre 8).

Références bibliographiques

[Asmolov & Kolozaridi, 2017] Asmolov, Gregory, & Kolozaridi, Polina, « The imaginaries of RuNet: the change of the elites and the construction of online space », *Russian Politics* vol. 2, n° 1, p. 54-79.

[Audinet, 2021] Audinet, Maxime, *Russia Today (RT). Un média d'influence au service de l'État russe*, INA.

[Best & Krueger, 2008] Best, Samuel J., & Krueger, Brian S., « Political conflict and public perceptions of government surveillance on the Internet: an experiment of online search terms », *Journal of Information Technology & Politics* vol. 5, n° 2, p. 191-212.

[Boas, 2006] Boas, Taylor C., « Weaving the authoritarian web. The control of Internet use in nondemocratic regimes », in Zysman, John & Newman, Abraham (dir.), *How Revolutionary Was the Digital Revolution? National Responses, Market Transitions, and Global Technology*, Stanford, CA, Stanford University Press, p. 361-378.

[Bronnikova & Zaytseva, 2021] Bronnikova, Olga & Zaytseva, Anna, « 'In Google we trust'? The Internet giant as a subject of contention and appropriation for the Russian state and civil society », *First Monday* vol. 26, n° 5.

[Brunton & Nissenbaum, 2015] Brunton, Finn & Nissenbaum, Helen, *Obfuscation. A User's Guide for Privacy and Protest*, Cambridge, MA and London, MIT Press.

[Cardon, 2010] Cardon, Dominique, *La Démocratie Internet. Promesses et limites*, Paris, Seuil.

[Clément et al, 2010] Clément, K., O. Miriasova, & Demidov, A., *Ot obyvatelei k aktivistam: zarožda ûšiesiâ sotsial'nye dviženia v sovremennoj Rossii*, Moscou, Tri Kvadrata.

[Daucé, 2022] Daucé, Françoise, « Pirater l'autoritarisme. Trajectoires de lutte pour les libertés numériques dans la Russie de V. Poutine (2009-2022) », *Terminal* n° 134-135.

[Daucé et al, 2019] Daucé, Françoise, Loveluck, Benjamin, Ostromooukhova, Bella, & Zaytseva, Anna, « From citizen investigators to cyber patrols: volunteer Internet regulation in Russia », *Laboratorium* vol. 11, n° 3, p. 46-70.

[Daucé & Musiani, 2021] Daucé, Françoise, & Musiani, Francesca (dir.), « Infrastructure-embedded control, circumvention and sovereignty in the Russian Internet: an introduction », *First Monday* vol. 26, n° 5.

[Deibert, 2019] Deibert, Ronald J., « The road to digital unfreedom: three painful truths about social media », *Journal of Democracy* vol. 30, n° 1, p. 25-39.

[Deibert & Rohozinski, 2010] Deibert, Ronald J., & Rohozinski, Rafal, « Control and subversion in Russian cyberspace », in Deibert, Ronald J., Palfrey, John, Rohozinski, Rafal, & Zittrain, Jonathan (dir.), *Access Controlled. The Shaping of Power, Rights, and Rule in Cyberspace*, Cambridge, MA and London, MIT Press, p. 15-34.

[DeNardis, 2014] DeNardis, Laura, 2014, *The Global War for Internet Governance*, New Haven, CT, Yale University Press.

[DeNardis, 2012] DeNardis, Laura, « Hidden levers of Internet control. An infrastructure-based theory of Internet governance », *Information, Communication & Society* vol. 15, n° 5, p. 720-738.

[Diamond et al, 2016] Diamond, Larry, Plattner, Marc F., & Walker, Christopher (dir.), *Authoritarianism Goes Global. The Challenge to Democracy*, Baltimore, MD, Johns Hopkins University Press.

[Diamond, 2010] Diamond, Larry, « Liberation technology », *Journal of Democracy* vol. 21, n° 3, p. 69-83.

[Ermoshina & Musiani, 2021] Ermoshina, Ksenia, & Musiani, Francesca, « The Telegram ban: How censorship « made in Russia » faces a global Internet », *First Monday* vol. 26, n° 5.

[Etling et al., 2010] Etling, Bruce, Alexanyan, Karina, Kelly, John, Faris, Robert, Palfrey, John, & Gasser, Urs, « Public discourse in the Russian blogosphere: mapping RuNet politics and mobilization », Berkman Center Research Publication n° 2010-11, Harvard (http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Public_Discourse_in_the_Russian_Blogosphere_2010.pdf).

[Feldstein, 2021] Feldstein, Steven, *The Rise of Digital Repression. How Technology Is Reshaping Power, Politics, and Resistance*, New York, Oxford University Press.

[Fialkova & Yelenevskaya, 2005] Fialkova, Larisa, & Yelenevskaya, Maria N., « Incipient soviet diaspora: encounters in cyberspace », *Narodna umjetnost: hrvatski časopis za etnologiju i folkloristiku* vol. 42, n° 1, p. 83-99.

[Gabowitsch, 2017] Gabowitsch, Mischa, *Protest in Putin's Russia*, Cambridge and Malden, MA, Polity Press.

[Gelman, 2010] Gelman, Vladimir, « The dynamics of subnational authoritarianism (Russia in comparative perspective) », *Russian Politics & Law* vol. 48, n° 2, p. 7-26.

[Gillespie, 2018] Gillespie, Tarleton, *Custodians of the Internet. Platforms, Content Moderation, and the Hidden Decisions that Shape Social Media*, New Haven, CT, Yale University Press.

[Glasius & Michaelsen, 2018] Glasius, Marlies & Michaelsen, Marcus, « Illiberal and authoritarian practices in the digital sphere. Prologue », *International Journal of Communication* vol. 12, p. 3795-3813.

[Gunitsky, 2015] Gunitsky, Seva, « Corrupting the cyber-commons: social media as a tool of autocratic stability », *Perspectives on Politics* vol. 13, n° 1, 2015, p. 42-54.

[Guriev & Treisman, 2022] Guriev, Sergei & Treisman, Daniel, *Spin Dictators. The Changing Face of Tyranny in the 21st Century*, Princeton University Press.

[Haggart et al., 2021] Haggart, Blayne, Tusikov, Natasha & Scholte, Jan Aart (dir.), *Power and Authority in Internet Governance. The Return of the State?* , Abingdon and New York, Routledge.

[Han, 2018] Han, Rongbin, *Contesting Cyberspace in China. Online Expression and Authoritarian Resilience*, New York, Columbia University Press.

[Hintz & Milan, 2018] Hintz, Arne & Milan, Stefania, «» Through a glass, darkly»: everyday acts of authoritarianism in the liberal West», *International Journal of Communication* vol. 12, p. 3939-3959.

[Hmed & Laurens, 2011] Hmed, Choukri, & Laurens, Sylvain, «Les résistances à l'institutionnalisation», in Lagroye, Jacques, & Offerlé, Michel (dir.), *Sociologie de l'institution*, Paris, Belin, p. 131-148.

[Howard & Hussain, 2013] Howard, Philip N., & Hussain, Muzammil M., *Democracy's Fourth Wave? Digital Media and the Arab Spring*, Oxford and New York, Oxford University Press.

[Howells & Henry, 2021] Howells, Laura & Henry, Laura A., «Varieties of digital authoritarianism: analyzing Russia's approach to Internet governance», *Communist and Post-Communist Studies* vol. 54, n° 4, p. 1-27.

[Jamil, 2021] Jamil, Sadia, «The rise of digital authoritarianism: evolving threats to media and Internet freedoms in Pakistan», *World of Media–Russian Journal of Journalism and Media Studies,* vol. 3, p. 5-33.

[Jones, 2022] Jones, Marc Owen, *Digital Authoritarianism in the Middle East. Deception, Disinformation and Social Media*, London, Hurst.

[Kalathil & Boas, 2003] Kalathil, Shanthi & Boas, Taylor C., *Open Networks, Closed Regimes. The Impact of the Internet on Authoritarian Rule*, Washington, DC, Carnegie Endowment for International Peace.

[Keremoğlu & Weidmann, 2020] Keremoğlu, Eda & Weidmann, Nils B., «How dictators control the internet: a review essay», *Comparative Political Studies* vol. 53, n° 10-11, p. 1690-1703.

[Keucheyan & Tessier, 2008] Keucheyan, Razmig, & Tessier, Laurent, «Présentation. De la piraterie au piratage», *Critique,* vol. 64, n° 733-734, p. 451-457.

[Konradova & Schmidt, 2014] Konradova, Natalya, & Schmidt, Henrike, «From the utopia of autonomy to a political battlefield: towards a history of the «Russian Internet»», in Gorham, Michael S., Lunde, Infunn & Paulsen, Martin (dir.), *Digital Russia. The Language, Culture and Politics of New Media Communication*, London, Routledge, p. 34-44.

[Lamensch, 2021] Lamensch, Marie, «Authoritarianism has been reinvented for the digital age», *Center for International Governance Innovation*, 9 juillet 2021 (https://www.cigionline.org/articles/authoritarianism-has-been-reinvented-for-the-digital-age/)

[Laruelle, 2021] Laruelle, Marlène, *Is Russia Fascist? Unraveling Propaganda East and West,* Ithaca, NY and London, Cornell University Press.

[Laruelle, 2022] Laruelle, Marlène, «So, is Russia fascist now? Labels and policy implications», *The Washington Quarterly* vol. 45, n°2, p. 149-168.

[Lewis, 2020] Lewis, David G., *Russia's New Authoritarianism. Putin and the Politics of Order*, Edinburgh, Edinburgh University Press.

[Liang et al., 2018] Liang, Fan, Das, Vishnupriya, Kostyuk, Nadiya & Hussain, Muzammil M., « Constructing a data-driven society: China's social credit system as a state surveillance infrastructure », *Policy & Internet* vol. 10, n° 4, p. 415-453.

[Limonier, 2021] Limonier, Kevin, « Vers un « Runet souverain » ? Perspectives et limites de la stratégie russe de contrôle de l'Internet », *EchoGéo* n° 56.

[Lokot, 2020] Lokot, Tetyana, « Articulating networked citizenship on the Russian Internet: a case for competing affordances », *Social Media + Society* vol. 6, n° 4.

[Loveluck, 2015a] Loveluck, Benjamin, *Réseaux, libertés et contrôle. Une généalogie politique d'internet*, Paris, Armand Colin.

[Loveluck, 2015b] Loveluck, Benjamin, « Internet, une société contre l'État ? Libéralisme informationnel et économies politiques de l'auto-organisation en régime numérique », *Réseaux* n° 192, p. 235-270.

[MacKinnon, 2012] MacKinnon, Rebecca, *Consent of the Networked. The World-Wide Struggle for Internet Freedom*, New York, Basic Books.

[MacKinnon et al., 2014] MacKinnon, Rebecca, Hickok, Elonnai, Bar, Allon & Lim, Hae-in, *Fostering Freedom Online: The Role of Internet Intermediaries*, UNESCO Series on Internet Freedom.

[Marczak et al., 2018] Marczak, Bill, Scott-Railton, John, McKune, Sarah, Razzak, Bahr Abdul, & Deibert, Ron, *HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*, Citizen Lab research report No. 113, University of Toronto (https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/).

[Mare, 2020] Mare, Admire, « State-ordered Internet shutdowns and digital authoritarianism in Zimbabwe », *International Journal of Communication* vol. 14.

[Maréchal, 2018] Maréchal, Nathalie, « From Russia with crypto: a political history of Telegram », *FOCI' 18 – 8th USENIX Workshop on Free and Open Communications on the Internet*, Baltimore, MD (https://www.usenix.org/node/220216).

[Morgunova, 2012] Morgunova, Oksana, « National living on-line? Some aspects of the Russophone e-diaspora map. » *E-diasporas Atlas* working paper, avril 2014 (http://www.e-diasporas.fr/working-papers/Morgunova-Russophones-EN.pdf).

[Morgus, 2018] Morgus, Robert, « The spread of Russia's digital authoritarianism », in Wright, Nicholas D. (dir.), *AI, China, Russia, and the Global Order. Technological, Political, Global, and Creative Perspectives*, Washington, DC, United States Department of Defense.

[Morozov, 2011] Morozov, Evgeny, *The Net Delusion. The Dark Side of Internet Freedom*, New York, Public Affairs.

[Motyl, 2016] Motyl, Alexander J., « Putin's Russia as a fascist political system », *Communist and Post-Communist Studies* vol. 49, n° 1, p. 25-36.

[Musiani et al., 2019] Musiani, Francesca, Loveluck, Benjamin, Daucé, Françoise, & Ermoshina, Ksenia, « Souveraineté numérique : l'Internet russe peut-il se couper du reste du monde ? », *The Conversation*, 18 mars 2019 (https://theconversation.com/souverainete-numerique-lInternet-russe-peut-il-se-couper-du-reste-du-monde-113516).

[Nocetti, 2015] Nocetti, Julien, « Russia's 'dictatorship-of-the-law' approach to Internet policy », *Internet Policy Review* vol. 4, n° 4.

[Oates, 2013] Oates, Sarah, *Revolution Stalled. The Political Limits of the Internet in the Post-Soviet Sphere*, Oxford, Oxford University Press.

[Polyakova & Meserole, 2019] Polyakova, Alina, & Meserole, Chris, « Exporting digital authoritarianism: the Russian and Chinese models », *Brookings Policy Brief, Democracy and Disorder Series*, Washington, DC, Brookings Foundation, p. 1-22 (https://www.brookings.edu/research/exporting-digital-authoritarianism/).

[Poupin, 2022] Poupin, Perrine, « Conflit contre un projet de méga-décharge à Shies. Enjeux de souveraineté dans le nord-ouest russe à l'ère d'Internet », *Terminal,* n° 134-135.

[Roberts, 2018] Roberts, Margaret E., *Censored. Distraction and Diversion Inside China's Great Firewall*, Princeton, NJ, Princeton University Press.

[Scott, 2009] Scott, James C., *La domination et les arts de la résistance. Fragments du discours subalterne*, Paris, Éd. Amsterdam.

[Sinkkonen & Lassila, 2022] Sinkkonen, Elina, & Lassila, Jussi, « Digital authoritarianism and technological cooperation in Sino-Russian relations: common goals and diverging standpoints », in Kirchberger, Sarah, Sinjen, Svenja & Wörmer, Nils (dir.), *Russia-China Relations. Emerging Alliance or Eternal Rivals?* , Cham, Springer, p. 165-184.

[Snyder, 2022] Snyder, Timothy, « We Should Say It. Russia is Fascist », *The New York Times*, 19 mai 2022. (https://www.nytimes.com/2022/05/19/opinion/russia-fascism-ukraine-putin.html).

[Soldatov & Borogan, 2015] Soldatov, Andreï, & Borogan, Irina, *The Red Web. The Kremlin's Wars on the Internet*, New York, Public Affairs.

[Stadnik, 2021] Stadnik, Ilona, « Control by infrastructure: political ambitions meet technical implementations in RuNet », *First Monday*, vol. 26, n° 5.

[Tesquet, 2020] Tesquet, Olivier, À la trace. Enquête sur les nouveaux territoires de la surveillance, Paris, Premier Parallèle.

[Tréguer, 2019] Tréguer, Félix, *L'Utopie déchue. Une contre-histoire d'Internet XV^e-XXI^e siècle*, Paris, Fayard.

[Uffelmann, 2014] Uffelmann, Dirk, « Is there a Russian cyber empire? », in Gorham, Michael S., Lunde, Ingunn & Paulsen, Martin (dir.), *Digital Russia. The Language, Culture and Politics of New Media Communication*, London and New York, Routledge, p. 266-284.

[Van der Vet, 2020] Van der Vet, Freek, « Imprisoned for a 'like': the criminal prosecution of social media users under authoritarianism », in Wijermars, Mariëlle & Lehtisaari, Katja (dir.), *Freedom of Expression in Russia's New Mediasphere*, Abingdon and New York, Routledge, p. 209-224.

[Waldner & Lust, 2018] Waldner, David & Lust, Ellen, « Unwelcome change: coming to terms with democratic backsliding », *Annual Review of Political Science* vol. 21, p. 93-113.