

Françoise Daucé, Benjamin Loveluck & Francesca Musiani (éd.), *Genèse d'un autoritarisme numérique : répression et résistance sur Internet en Russie, 2012-2022*, Paris, Presses des Mines, 2023, 218 p. – ISBN numérique 978-2-38542-424-4, ISBN édition imprimée 978-2-35671-972-0

Comment l'emprise des autorités s'est-elle peu à peu refermée sur le réseau Internet en Russie, malgré sa construction historiquement décentralisée et les espoirs qu'il portait pour la démocratisation du pays ? Cette question est au centre de l'ouvrage dirigé par Françoise Daucé, Benjamin Loveluck et Francesca Musiani et constitue le fil conducteur des huit chapitres. Pour y répondre, les A. analysent le durcissement des lois et des politiques de contrôle de l'Internet russe à partir du début des années 2010, en s'intéressant aux acteurs qui les contestent, dont les « citoyens mobilisés », opposants politiques, journalistes indépendants, mais aussi les développeurs de logiciels et les fournisseurs d'accès au réseau (FAI). Cette perspective permet d'ouvrir l'analyse sociologique aux acteurs qui façonnent le réseau depuis sa création en Russie.

Face au constat de la fermeture de l'espace public russe, les coordinateurs du volume soulèvent dès l'introduction la question de la qualification du système politique en Russie et s'appuient sur le concept de « démocratie illibérale » tel que défini par David Lewis¹. Selon D. Lewis, le système politique russe repose sur un principe charnière au nom duquel toutes les normes, y compris juridiques, peuvent être transgressées par ses détenteurs : celui de l'« ordre » (p. 15). On pourrait lui ajouter le principe de sécurité, mis en avant dans le discours

1. Marlène Laruelle trouve une première occurrence du concept dans le principe de « démocratie souveraine », développé par Vladislav Sourkov pour théoriser la nature politique du pouvoir en Russie (« Illiberalism: A Conceptual Introduction », *East European Politics*, vol. 38, n° 2, 2022, p. 303-327). La notion aurait été intéressante à mentionner au vu de l'importance du principe de « souveraineté » dans les politiques russes après 2010.

officiel pour justifier le renforcement des lois sur le numérique depuis les années 2010.

C'est donc pour faire primer l'ordre social et politique que la législation russe s'est vue complétée par les lois visant à « encadrer et à surveiller la circulation » des données numériques, « contrôler l[es] infrastructure[s] » et maîtriser « les activités économiques des acteurs privés » (p. 34) du secteur, comme l'explique Valéry Kossov dans le premier chapitre. L'A. y montre comment les autorités russes se servent de la promulgation des lois pour affermir leur contrôle sur l'écosystème numérique dans une tentative de « souverainisation » (p. 33) du secteur, devenue une trajectoire forcée après le lancement de la guerre de grande ampleur en Ukraine le 24 février 2022, suivi par le départ de nombreuses entreprises étrangères. V. Kossov explique que l'inflation législative russe en matière de numérique n'a pas conduit, toutefois, à une unification du droit qui « recoup[erait] tous les secteurs » (p. 33) juridiques (constitutionnel, pénal, administratif, commercial et bancaire). On aurait pu expliquer ici l'ambiguïté et l'incomplétude volontaires de certaines lois russes en matière de blocage des contenus dès les années 2010, évoquée dans la conclusion du chapitre. L'A. y relève aussi l'important paradoxe d'une législation russe du numérique largement tournée vers un objectif d'autonomie, pourtant voué à se heurter aux « interdépendances technologiques » (p. 49) mondiales dans le cadre d'une guerre qui soumet, en outre, les différents secteurs économiques et industriels du pays à des sanctions occidentales.

À cette présentation du durcissement du cadre normatif et juridique du numérique en Russie succède un chapitre de Ksenia Ermoshina, Benjamin Loveluck et Francesca Musiani, qui aborde les effets concrets de la législation sur les acteurs. Les A. proposent une « web-ethnographie » (p. 55) des FAI russes, en s'appuyant sur une méthodologie riche allant des entretiens à l'étude des forums en ligne perçus comme moyens de socialisation et d'organisation professionnelles. Cette démarche permet de « déconstru[ire] l'image trop simplifiée » (p. 53) d'un contrôle direct et total de l'État sur l'Internet en Russie au moyen des technologies de surveillance. Les A. examinent ainsi non seulement les stratégies de contrôle de l'information mises en place par les autorités russes à l'aide d'appareils et de logiciels de stockage, d'analyse et de filtrage des données, mais aussi celles des FAI, qui se voient contraints d'installer ces appareils et logiciels sur leurs infras-

structures à leurs frais pour se conformer à la législation. Certains FAI déploient des « stratégies de contournement » des lois, telles que la « censure sélective » (p. 62), pour tromper les systèmes de surveillance de l'agence Roskomnadzor, le contrôleur de l'Internet russe.

Dans le chapitre suivant, Françoise Daucé et Benjamin Loveluck analysent la mise au pas de l'« espace public numérique » (p. 73) par les autorités russes à travers le cas de l'agrégateur d'actualités Yandex.Novosti. Pour ce faire, les A. fondent leur analyse sur le fonctionnement même de l'agrégateur, qui leur permet de passer de ses caractéristiques sociotechniques aux enjeux politiques qu'il recouvre. Cette démarche démontre un « écart entre la diversité des ressources médiatiques russes en ligne et l'étrécissement de l'échantillon de médias [dans ses] classements » (p. 75), généralement financés par l'État russe ou favorables aux politiques du gouvernement. Les A. analysent la façon dont les autorités russes ont « disciplin[é] l'algorithme pour contrôler l'actualité » (p. 78) et expliquent que l'abandon de Yandex.Novosti, évoqué à plusieurs reprises par les entreprises Yandex puis VKontakte, est de nouveau envisagé depuis 2022 au vu de la valeur hautement (géo)politique et stratégique de son système de sélection des informations en Russie.

Le quatrième chapitre de l'ouvrage, rédigé par Olga Bronnikova, Ksenia Ermoshina et Anna Zaytseva, présente un paradoxe entre la défense d'une « sécurité de l'information » (p. 99) par les autorités, qui se traduit par une répression des contenus critiques envers l'État, et la défense de leur « sécurité numérique » (p. 98) par les militants et opposants politiques, qui doivent protéger leurs ordinateurs contre l'intrusion des services de sécurité intérieure. Les A. s'appuient sur des enquêtes de terrain menées notamment à Moscou, Saint-Petersbourg, Minsk et en ligne entre 2018 et 2022, auprès de formateurs en sécurité numérique militant pour un Internet libre. Elles ont aussi interrogé leurs étudiants, souvent des journalistes, défenseurs des droits humains ou militants écologistes et anti-corruption. Leurs recherches établissent que les « pratiques d'auto-défense numérique » de ces acteurs impliquent largement l'usage d'outils et infrastructures de grandes multinationales étrangères, dont les GAFAM (Google, Apple, Facebook, Amazon et Microsoft). Selon les A., ce souci de sécurité s'est élargi à la « société civile [en] générale » (p. 116) en une dizaine d'années, dépassant les communautés de spécialistes et utilisateurs avertis.

Le chapitre suivant, rédigé par Françoise Daucé, s'intéresse au journalisme d'investigation numérique, ou « data-journalisme » (p. 124), dans un contexte de censure de l'information en Russie. F. Daucé pose d'abord la question de sa définition, soulignant l'aspect polysémique du terme, qui suppose le recours à des méthodes comprenant « l'usage statistique de données numériques » et le « renseignement de sources ouvertes (OSINT) » (p. 119). Inscrivant ce chapitre dans la suite des travaux de Cyril Lemieux, elle relève que cette forme de journalisme se veut « factuel[le], fondé[e] sur l'exhaustivité et l'exactitude » (p. 120), marquant ainsi sa différence avec un « journalisme politique » (p. 120) qui, au-delà de la présentation des faits, prend position. Elle montre aussi que le data-journalisme fait du journalisme d'enquête une méthode pluridisciplinaire intégrant des parties techniques, telles que l'apprentissage du code informatique, et la maîtrise de l'infographie pour mettre « en équivalence des données et des faits » (p. 120). Analysant sa réception par les internautes, Françoise Daucé relève que « l'engouement » pour le data-journalisme est « proportionnel » en Russie « à la fermeture de l'espace public russe » (p. 123). Ce journalisme qui aide la société civile à « “regarder d'en bas” les pouvoirs étatiques et commerciaux » (p. 120), se trouve ainsi au cœur d'une « lutt[e] pour l'interprétation et l'appropriation des données » (p. 130), entre opposants politiques et journalistes d'investigation d'une part et autorités étatiques de l'autre. Il acquiert une importance particulière en contexte de guerre, avec l'usage des données numériques à des fins militaires.

Le sixième chapitre, signé par Bella Ostromoukhova, étudie l'intrication des enjeux économiques et politiques que recouvre la volonté de contrôle des ouvrages numériques par l'État russe et les éditeurs au moyen du droit d'auteur. L'A. analyse aussi l'opposition entre cette volonté de contrôle et celle de transgression des limitations d'accès à ces contenus par les « *hackers* », qui militent pour un accès libre à la connaissance. Elle inscrit son étude dans le temps long, en revenant d'abord sur les restrictions de publication à l'époque soviétique et les stratégies d'acteurs pour les contourner, telles que le « marché noir des biens culturels » (p. 143) auquel était liée la pratique du *samizdat*. B. Ostromoukhova présente ensuite l'émergence du nouveau cadre législatif des droits d'auteur dans la Russie des années 1990 et d'un « marché légal des textes au format numérique » dans ce contexte de « libéralisation et d'ouverture du marché des biens culturels »

(p. 141). Elle montre comment ce cadre s'est modifié pour devenir un outil politique des autorités russes à travers l'instrumentalisation, voire le détournement, du *copyright* (droit de reproduction et de republication) et de la « lutte contre le piratage » (p. 160) pour bloquer les sites web qui enfreignent les lois de censure des contenus en vigueur. L'A. explique que, face à ces usages restrictifs et répressifs du droit d'auteur, divers acteurs ont mis en place de nouvelles « stratégies de contournement » (p. 141) en créant des « bibliothèques de l'ombre » (p. 142) pour diffuser des livres malgré les restrictions ou en publiant sur leurs sites des « astuces » comme l'usage du *torrent* (téléchargement partagé de ressources) ou de réseaux virtuels privés (VPN). B. Ostro-moukhova conclut que la lutte « pour un Internet libre de toute censure » et celle « pour un accès libre et équitable » aux biens culturels « se chevauchent » (p. 160) dans leurs modes de contestation et de contournement des restrictions.

Le chapitre suivant, rédigé par Perrine Poupin, étudie les phénomènes de contestation politique et de militantisme par des moyens numériques en Russie. Elle explique que l'émergence des réseaux sociaux a fait passer la communication militante et protestataire des mails, listes de diffusion et blogs aux sites de réseaux et médias sociaux tels que YouTube. Ce chapitre met en regard l'usage de l'Internet à des fins politiques par les autorités russes, notamment dans le cadre de la propagande de guerre de l'État, et son utilisation par les militants et opposants politiques pour échanger des informations ou organiser des protestations. Perrine Poupin se penche aussi sur la désinformation en ligne, menée en Russie par de multiples acteurs sur différents sujets incluant la pandémie de COVID-19 et la guerre. Elle remarque que cette désinformation constante provoque des conflits et sape la cohésion de la société civile russe. Ces effets dessinent un avenir « incertain » pour la Russie.

Le dernier chapitre, signé Olga Bronnikova, Françoise Daucé, Ksenia Ermoshina et Benjamin Loveluck, étudie le passage de la répression numérique à la répression physique, à travers les perquisitions, peines de prison et l'exil imposés aux opposants politiques et citoyens contestataires en Russie. Le chapitre vient ainsi clôturer l'ouvrage par un rappel de la gravité des risques encourus par ces acteurs, malgré leur usage de techniques de « sécurité numérique » (p. 194) contre les moyens de surveillance et de désanonymisation des internautes employés par les autorités. Les A. montrent que les modes

de répression pour « étouffer toute contestation » passent des « atteintes aux biens informatiques » et aux « données numériques » (p. 194) des militants à leur arrestation physique, accompagnée de pressions psychologiques, voire de tortures. Face à ces risques, ils se voient souvent contraints à l'exil et sont confrontés à « une expérience de précarisation à la fois personnelle et professionnelle [...], morale et administrative » (p. 202), qui se prolonge sur le plan numérique, puisqu'ils rencontrent des difficultés pour accéder aux ressources en ligne de leur pays d'origine.

Malgré cette lutte personnelle pour leur survie, les acteurs contestataires russes restent souvent engagés dans leur combat pour l'Internet libre et contre « l'autoritarisme croissant du régime politique russe » (p. 207), qui rejoint de ce fait celui des exilés de guerre ukrainiens. Cette jonction des luttes est néanmoins confrontée à des divergences au sujet d'un « colonialisme russe » (*ibid.*), divergences permettant toutefois d'imaginer ce que serait un espace informationnel rusophone « libéré des contraintes autoritaires » (p. 209). Les A. parlent eux-mêmes d'une « domination coloniale » de la Russie (p. 207). Ce concept aurait mérité d'être explicité et replacé dans son contexte historique, celui des empires coloniaux européens du XVI^e au XX^e siècle, que le régime russe instrumentalise pour étendre son influence aux États issus de la décolonisation. Sa reprise par les A., après les autorités et les militants ukrainiens, peut ainsi être vue comme une réponse au discours « anticolonial » promu par la Russie sur la scène internationale².

Les A. montrent enfin que la guerre a fait tomber les « derniers tabous autoritaires » en Russie, en permettant aux autorités de justifier les mesures de censure et de surveillance numériques par la « défense de l'intérêt national » (p. 209). Cela fait du système politique russe un régime toujours plus autoritaire, qui tend vers le totalitarisme sur le plan numérique. Le cas russe offre ainsi un « exemple d'autoritarisme augmenté » (*ibid.*) par le numérique, qui doit permettre de penser et de contrer les dérives autocratiques dans nos sociétés.

Marie-Gabrielle Bertran

IFG/GEODE – Université Paris 8

2. On aurait autrement pu parler d'un « impérialisme » ou « néo-impérialisme » russe, largement étudié dans la littérature.