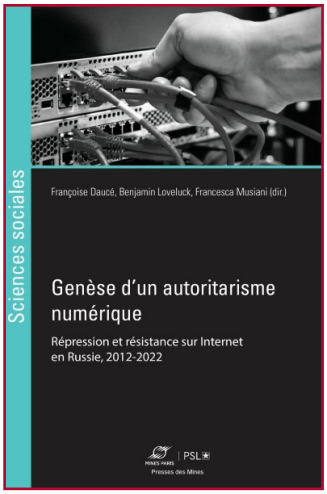
Françoise DAUCÉ, Benjamin LOVELUCK & Francesca MUSIANI (éds), *Genèse d'un autoritarisme numérique. Répression et résistance sur Internet en Russie, 2012-2022*. Paris : Presses des Mines, 2023, 224 p.

Kevin LIMONIER
Professeur de géographie
Institut Français de Géopolitique
Université Paris 8 (FR)
kevin.limonier@protonmail.com

Doi : 10.5077/journals/connexe.2025.e2418



Dans les années 1990 et 2000, le segment russe de l'Internet était réputé pour constituer l'un des espaces de liberté les plus remarquables du cyberespace. Au début des années 2010, la situation a toutefois commencé à évoluer, d'abord de manière subtile, puis de façon spectaculaire avec la généralisation progressive de la censure numérique et de la surveillance électronique. Face à ce tournant autoritaire, divers modes de résistance ont progressivement émergé, notamment par le contournement ou la réappropriation des normes sociotechniques qui structurent cette véritable société de contrôle à l'ère numérique.

C'est l'histoire de cette dynamique que retrace l'ouvrage, organisé en huit chapitres complémentaires, chacun offrant un éclairage sur une facette particulière du phénomène. Les trois premiers chapitres sont consacrés à l'analyse des différentes dimensions de l'autoritarisme numérique russe. Le premier chapitre retrace la genèse juridique des principales lois de censure et de contrôle, au premier rang desquelles figure la fameuse loi sur le « Runet souverain ». Le chapitre met également en lumière les stratégies de résistance à ce que l'auteur, Valéry Kossov, qualifie à juste titre d'« oppression juridique ». Le deuxième chapitre s'avère particulièrement éclairant en proposant une immersion au cœur du dispositif sociotechnique de contrôle numérique. Dans ce chapitre, Ksenia Ermoshina, Benjamin Loveluck et Francesca Musiani procèdent à un véritable « décorticage » des matériels et logiciels mobilisés par l'État russe pour renforcer la surveillance électronique. Que le lectorat ne se laisse pas décourager par la technicité du propos : la démonstration se distingue par une pédagogie remarquable qui permet de comprendre comment ces dispositifs de contrôle tissent leur toile autour du citoyen russe. Le troisième chapitre s'intéresse pour sa part à un mécanisme de contrôle situé au niveau des plateformes d'intermédiation : l'algorithme de l'agrégateur d'actualité de Yandex – le « Google russe » –, qui constitue un puissant levier de contrôle et de contrainte numérique dans la Russie contemporaine tant ce service est massivement utilisé par la population. Si les auteurs (Françoise Daucé et Benjamin Loveluck) décrivent en détail la genèse de ce « *gatekeeping* algorithmique », on notera que le processus de prise de contrôle par l'État est d'abord analysé sous l'angle des controverses qu'il suscite et des textes officiels qui en découlent. Une entrée par les acteurs du pouvoir, par leurs stratégies ou leurs motivations aurait permis d'éclairer le phénomène sous l'angle, complémentaire, des *gatekeepers* et de leurs représentations du monde numérique.

Après avoir analysé certains processus d'oppression numérique, l'ouvrage se penche logiquement sur les modes de résistance qui ont émergé pour y faire face. Les chapitres quatre à sept explorent ainsi différentes modalités de résistance et de contournement du contrôle numérique. Le quatrième chapitre aborde la question de la formation à la sécurité informatique en contexte autoritaire et dresse un panorama de « l'écosystème » qui s'est constitué en Russie pour permettre aux individus d'acquérir un niveau de connaissance suffisant afin d'éviter poursuites, menaces et pressions. Face à la fuite en avant autoritaire provoquée par l'invasion à grande échelle de l'Ukraine, ce chapitre analyse également les défis auxquels doivent faire face les organisations russes en exil, prises entre déstructuration et restructuration hors des frontières du pays.

Le cinquième chapitre s'intéresse à la manière dont le data-journalisme a permis à de nombreux journalistes russes d'enquêter malgré une censure grandissante, dans la lignée de ce qu'Allan Deneuville qualifie de « contre-enquêtes numériques » (2022). Le sixième chapitre explore une facette moins connue, mais particulièrement stimulante, des interstices de liberté qui subsistent dans ce Runet sous contrôle : celle des livres en ligne, de leur circulation et de leur consommation dans un pays où le droit d'auteur s'est imposé tardivement. Ce chapitre ouvre également la voie à l'exploration d'autres espaces liminaux de liberté, tels que les forums et communautés de partage pirate d'œuvres audiovisuelles et vidéoludiques. Enfin, le septième chapitre revient sur l'évolution des pratiques du militantisme en ligne en proposant une chronologie claire, ponctuée de ruptures qui correspondent aussi aux étapes marquantes de l'émergence de l'autoritarisme numérique russe.

Un dernier chapitre conclusif ouvre des perspectives nouvelles. La guerre, qui a conduit à l'exil de centaines de milliers de Russes, a fait émerger une forme de Runet « hors les murs », susceptible de jouer un rôle central dans la structuration d'une opposition politique cohérente en exil. L'enjeu est de tout premier ordre : comme le soulignait en 2023 le journaliste russe Mikhail Zygar (2024), la capacité des exilés à s'unir et à proposer une alternative politique crédible dépend en grande partie de leur aptitude à se doter d'un espace numérique commun.

Dans son ensemble, l'ouvrage offre ainsi un panorama riche des techniques et pratiques de contrôle numérique ainsi que des dynamiques de résistance et de contournement qui sont à l'œuvre – à l'intérieur comme à l'extérieur des frontières de la Fédération de Russie. Cependant, on regrettera la quasi-absence d'un objet fondamental : l'État russe, ainsi que les acteurs publics ou privés qui lui sont liés et qui sont les principaux artisans de l'oppression numérique telle que décrite dans l'ouvrage. Des services de renseignement aux entreprises numériques de surveillance en passant par l'administration présidentielle ou Roskomnadzor, un grand nombre d'acteurs et d'administrations participent à la construction des dispositifs sociotechniques de contrôle de l'autoritarisme numérique. Or, excepté dans le deuxième chapitre, ces acteurs ainsi que les stratégies qu'ils mettent en place sont souvent traités de manière relativement marginale. C'est là l'une des principales limites de l'ouvrage, dans lequel l'État russe apparait parfois comme une sorte de Léviathan, extérieur au périmètre du texte.

Or, comme l'écrivait Juan Linz (2007), l'une des principales caractéristiques de l'autoritarisme est justement d'entretenir le flou sur la manière dont s'exerce effectivement le pouvoir et le contrôle. Une myriade d'acteurs prospère dans cette confusion artificielle, qui a pour but de cacher ce que Claude Raffestin appelait « la séquence totalitaire du pouvoir » (1980) – c'est-à-dire la capacité d'un ordre à contrôler un espace et à le surveiller sans être vu. En laissant dans l'ombre ces acteurs qui ne veulent pas être vus, l'ouvrage traite ainsi d'abord des modes de résistances à l'autoritarisme, plutôt que de l'autoritarisme en lui-même. Il constitue en cela un travail important pour comprendre les mobilisations en contexte autoritaire, à l'heure où les technologies numériques démultiplient l'efficacité des régimes répressifs.

Références citées

Deneuville Allan, Hernández López Gala, Rasmi Jacopo, 2022. « Un âge de nouvelles enquêtes ? », *Multitudes* 89 (4) : 58-66.

Linz Juan, 2007. *Régimes totalitaires et autoritaires*, Paris : Armand Colin.

Raffestin Claude, 1980. *Pour une géographie du pouvoir*, Québec : Département de géographie de l'Université Laval.

Zygar Mikhail, 2024. *War and punishment: Putin, Zelensky, and the path to Russia's invasion of Ukraine*, New York: Scribner.