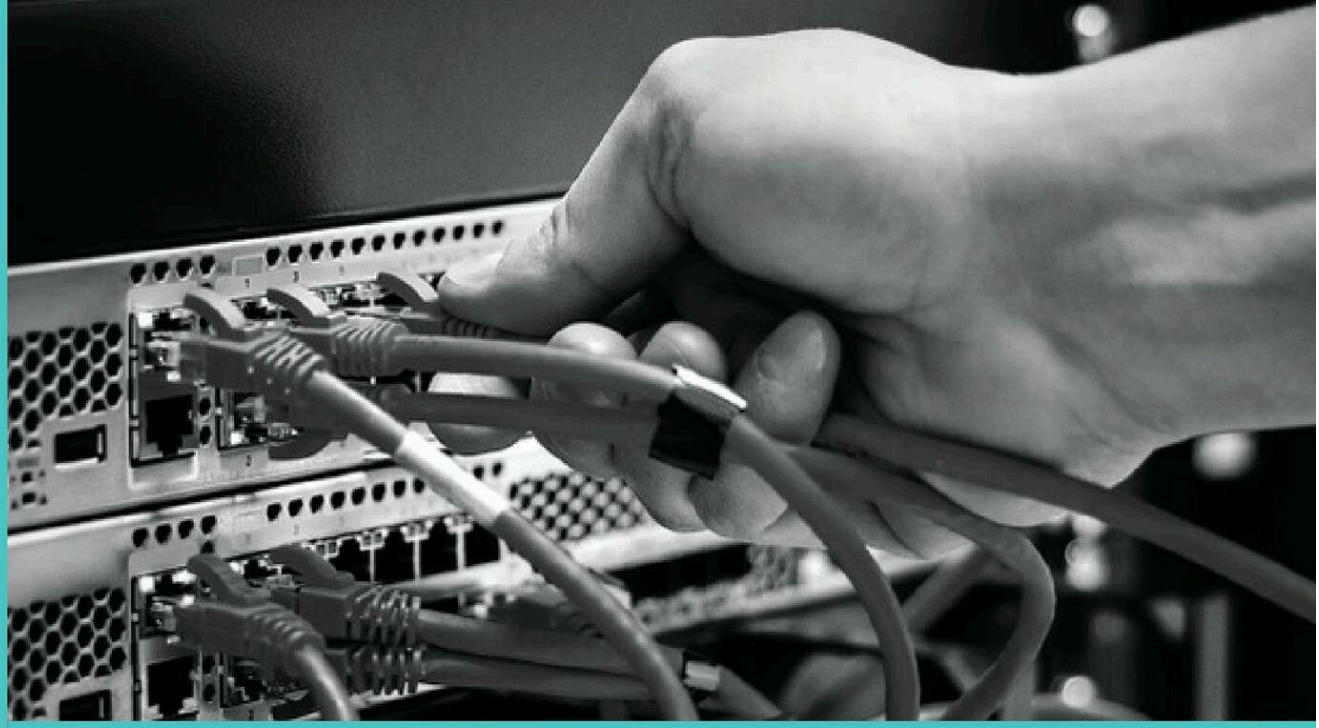
Genèse d'un autoritarisme numérique. Répression et résistance sur Internet en Russie, 2012-2022

Françoise Daucé, Benjamin Loveluck, Francesca Musiani

Sciences sociales



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

Genèse d'un autoritarisme numérique

Répression et résistance sur Internet en Russie, 2012-2022

MINES PARIS | PSL
Presses des Mines

Presses des Mines

Genèse d'un autoritarisme numérique

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

DOI : 10.4000/books.pressesmines.9023
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

https://books.openedition.org

Édition imprimée
EAN (Édition imprimée) : 9782356719720
Nombre de pages : 218

Référence électronique
DAUCÉ, Françoise (dir.) ; LOVELUCK, Benjamin (dir.) ; et MUSIANI, Francesca (dir.). *Genèse d'un autoritarisme numérique*. Nouvelle édition [en ligne]. Paris : Presses des Mines, 2023 (généré le 06 juin 2023). Disponible sur Internet : <http://books.openedition.org/pressesmines/9023>. ISBN : 9782385424244. DOI : https://doi.org/10.4000/books.pressesmines.9023.

Crédits de couverture
© Photo de couverture : iStock.com/kjekol

RÉSUMÉS

Dans le sillage de la fin de l'URSS, l'Internet russe s'est d'abord développé librement, laissant l'initiative à de nombreux acteurs inventant des outils numériques ajustés à leurs usages. Cependant, depuis le début des années 2010, le tournant autoritaire au sommet de l'État russe a entraîné le déploiement d'un maillage d'emprises et de contraintes qui s'est resserré tant sur les acteurs que sur les infrastructures numériques du pays.

Alors que le réseau a longtemps porté les espoirs de démocratisation de la sphère publique russe, son encadrement s'est constitué progressivement, au fil de controverses et d'épreuves. Malgré les critiques et les contournements militants et citoyens, l'oppression numérique a participé de la souverainisation politique et de la dynamique belliciste dont le moment culminant a été l'invasion de l'Ukraine en février 2022.

Le livre, nourri par les enquêtes de terrain réalisées dans le cadre du projet ANR ResisTIC, dessine un panorama de la gouvernance coercitive et des usages numériques émancipateurs en Russie, de la paix à la guerre. Il met l'accent sur les multiples acteurs et objets numériques au cœur des controverses politiques et des tensions d'usage dans l'espace numérique russe dans les années 2010. 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. Au prisme du cas russe, ce sont les reconfigurations numériques contemporaines, de la surveillance à la souveraineté, que ce livre interroge.

FRANÇOISE DAUCÉ (DIR.)

Directrice d'étude à l'EHESS et directrice du Centre d'études russes, caucasiennes, est-européennes et centrasiatiques (CERCEC). Ses travaux en sociologie politique de la Russie contemporaine portent sur les nouvelles formes de censure et d'emprise sur le monde médiatique à l'heure d'Internet. Elle a coordonné le projet ANR ResisTIC de 2018 à 2022.

BENJAMIN LOVELUCK (DIR.)

Maître de conférences en sociologie à Télécom Paris dans le département Sciences Économiques et Sociales, équipe de l'Institut Interdisciplinaire de l'Innovation (i3) et chercheur associé au Centre d'études et de recherches en sciences administratives et politiques (CERSA, CNRS-Paris 2). Ses travaux portent sur les pratiques politiques en ligne, les libertés numériques et la régulation d'Internet.

FRANCESCA MUSIANI (DIR.)

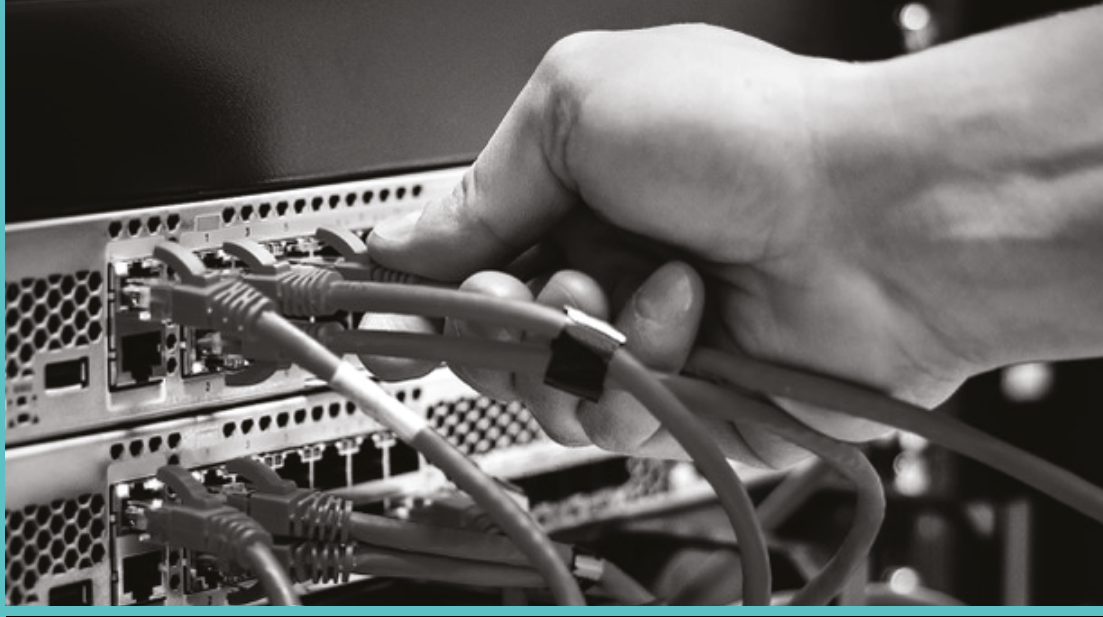
Chargée de recherche HDR au CNRS, co-fondatrice et directrice adjointe du Centre Internet et Société (CIS), chercheuse associée à MINES Paris-PSL et à l'Internet Governance Lab de l'American University. Ses recherches portent sur les infrastructures et les architectures techniques d'Internet comme outils de

gouvernance. En 2022, elle a publié avec Ksenia Ermoshina l'ouvrage Concealing for Freedom (Mattering Press).

NOTE DE L'ÉDITEUR

Cette publication a bénéficié du soutien de l'Institut Carnot M.I.N.E.S. et du projet de recherche
ResisTIC, financé par l'Agence Nationale de la Recherche.

Sciences sociales



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

Genèse d'un autoritarisme numérique

Répression et résistance sur Internet en Russie, 2012-2022

MINES PARIS | PSL
Presses des Mines

Françoise Daucé, Benjamin Loveluck, Francesca Musiani (dir.), *Genèse d'un autoritarisme numérique. Répression et résistance sur Internet en Russie, 2012-2022,* Paris, Presses des Mines, Collection Sciences sociales, 2023.

60, boulevard Saint-Michel - 75272 Paris Cedex 06 - France

presses@mines-paristech.fr

www.pressesdesmines.com

ISBN : 978-2-35671-972-0

Dépôt légal : 2023

Achevé d'imprimer en 2023 (Paris)

Cette publication a bénéficié du soutien de l'Institut Carnot M.I.N.E.S. et du projet de recherche ResisTIC, financé par l'Agence Nationale de la Recherche.

Genèse d'un autoritarisme numérique

MINES PARIS | PSL

Collection Sciences sociales

Responsable de la collection : Cécile Méadel
Centre de sociologie de l'innovation (www.csi.mines-paristech.fr)

Christelle Gramaglia,
Habiter la pollution industrielle.

Catherine Cavalin, Jaércio Da Silva, Pauline Delage, Irène Despontin Lefèvre, Delphine Lacombe, et Bibia Pavard,
Les violences sexistes après #MeToo

Caroline Rizza et Sandrine Bubendorff,
Gérer les crises avec les media sociaux ?

Vincent-Arnaud Chappe et Jean-Philippe Tonneau,
Le droit du travail en sociologue

Frédéric Goulet, Patrick Caron, Bernard Hubert, et Pierre-Benoit Joly,
Sciences, techniques et agricultures.

Quentin Gilliotte,
L'Expérience culturelle en régime numérique

Guillaume Sire,
Dernier refuge. Existe-t-il des livres numériques ?

Josiane Jouët,
Numérique, féminisme et société

Olivier Fournout,
Le nouvel héroïsme

Michèle Dupré et Jean-Christophe Le Coze,
Des usines, des matières et des hommes

Clément Combes et Hervé Glevarec,
Séries

Lise Conté,
Une sociologie pour l'action

Sabine Chalvon-Demersay,
Le Troisième souffle

Alexandre Mathieu-Fritz,
Le praticien, le patient et les artefacts

Gwenaële Rot, François Vatin,
In the flow

Catherine Cavalin, Emmanuel Henry, Jean-Noël Jouzel, Jérôme Pélisse,
Cent ans de sous-reconnaissance des maladies professionnelles

Baptiste Coulmont, Pierre Mercklé,
Pourquoi les top-modèles ne sourient pas

Serge Proulx,
La participation numérique : une injonction paradoxale

Eve Chiapello, Antoine Missemer, Antonin Pottier,
Faire l'économie de l'environnement

Sylvain Brunier, Olivier Pilmis,
La règle et le rapporteur

Vincent-Arnaud Chappe,
L'Égalité au travail

Fabien Foureault,
Le Capital en action

Frédéric Graber, Martin Gireaudeau,
Les Projets

Denis Ruellan,
Reportères de guerre

Brice Laurent, Michael Baker, Valérie Beaudouin, et Nathalie Raulet-Croset,
Innovation et participation

Dominique Pasquier,
L'internet des familles modestes

Jérôme Denis,
Le travail invisible des données

Christine Barats, Julie Bouchard et Arielle Haakenstad,
Faire et dire l'évaluation

Fabien Granjon, Venetia Papa & Gökçe Tuncel,
Mobilisations numériques

Ronan Le Velly,
Sociologie des systèmes alimentaires alternatifs

Collectif CSI,
Capitalization

Nicolas Auray,
L'Alerte ou l'enquête

Patrick Castel, Léonie Hénaut et Emmanuelle Marchal,
Faire la concurrence

Mélanie Dulong de Rosnay,
Les Golems du numérique

Michel Peroni,
Devant la mémoire. Une visite au Musée de la mine « Jean-Marie Somet » de Villars

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

Genèse d'un autoritarisme numérique

Répression et résistance sur Internet en Russie, 2012-2022

Remerciements

Nous devons d'abord remercier tous les militants de l'Internet libre qui, malgré les risques, ont accepté de répondre à nos nombreuses questions et nous ont invité à participer à leurs rencontres, nous ouvrant les portes de leurs *Cryptofest*, *Privacy Days* et autres hackathons organisés en Russie. Les militants des associations *Roskomsvoboda*, *Obchtchestvo Zachtchity Interneta* (OZI) et *Teplitsa sotsial'nykh tekhnologi (La serre des technologies sociales)* ont été des passeurs exceptionnels de leurs savoir-faire techniques dans le déroulement de cette enquête en terrain difficile, en Russie d'abord puis dans les pays étrangers (Lettonie, Lituanie, Géorgie…) où ils ont trouvé refuge.

Nous devons ensuite remercier les professionnels de l'espace public (journalistes, blogueurs, éditeurs, activistes, acteurs politiques) ainsi que les acteurs de l'internet (*ITichniki,* techniciens, développeurs, fournisseurs d'accès, formateurs) qui ont témoigné sur l'évolution de leurs conditions de travail dans un environnement numérique de plus en plus oppressif. Les entretiens avec les journalistes de nombreux médias (*Grani, Lenta, Gazeta, Kommersant, RBK, Novaïa Gazeta, Mediazona, Meduza, Radio Svoboda, Proekt, Takie Dela, The Insider, Arzamas, Dojd*) et les éditeurs de plusieurs maisons d'édition ont nourri cette recherche. Les discussions avec les militants de la *Fondation de lutte contre la corruption* (FBK) ont été particulièrement éclairantes.

Ces remerciements seraient incomplets sans une mention pour tous les citoyens russes qui, en diverses circonstances, nous ont renseigné sur leurs pratiques numériques quotidiennes ou militantes, à Moscou, à Saint-Pétersbourg ou dans le nord de la Russie. Les malheurs du temps veulent que nous ne puissions citer leurs noms pour ne pas ajouter à leurs embarras politiques en Russie ou hors de ses frontières.

Nous devons aussi beaucoup à tous nos collègues qui mènent des recherches sur les reconfigurations numériques contemporaines, dans les contextes autoritaires ou démocratiques. Leurs interventions lors des séminaires bimensuels que nous avons organisés de 2018 à 2021 à l'EHESS ont été particulièrement stimulantes pour nous fournir des repères partagés et faire avancer collectivement nos travaux.

Ce livre est issu d'une recherche menée avec le soutien de l'Agence Nationale de la Recherche (ANR) ainsi que de nos centres de recherche qui ont porté ce projet collectif (Centre d'études russes, caucasiennes, est-européennes et centrasiatiques / CERCEC, Centre Internet et Société, i3-Télécom Paris, ILCEA4, Eur'Orbem) que nous remercions pour leur soutien. Notre reconnaissance chaleureuse va à Fabrice Demarthon, Thomas da Silva, Marianne Rahmé et Timofey Balin qui nous ont aidés aux diverses étapes d'avancement de ce projet.

Tableau de translittération du russe vers le français

	Dans le corps du texte		Dans les notes de bas de page
Г, г	*gu*	avant un **e**, un и ou un ы	g
	g	tous les autres cas	
Е, е	*e*	après une consonne	e
		après un и ou un й	
		au début du mot, si convention admise	
	ïe	après une voyelle autre que и ou й	
	ie	au début du mot	
		après ь ou ъ	
		s'il s'agit d'une convention admise	
Ё, ё	*io*	tous les cas	ë
	e	s'il s'agit d'une convention admise	
Ж, ж	*j*	tous les cas	ž
И, и	ï	après une voyelle autre que и	i
	i	tous les autres cas	
Й, й	non transcrit	mots finissant par ий	j
		mots finissant par ый	
	ï	tous les autres cas	
Н, н	*ne*	en fin de mot après un и ou un ы	n
	n	tous les autres cas	
С, с	*ss*	entre deux voyelles	s
	s	tous les autres cas	
У, у	*ou*	tous les cas	u
	u	si convention admise	
Х, х	*kh*	tous les cas	h

	Dans le corps du texte		Dans les notes de bas de page
Ц, ц	*ts*	tous les cas	c
Ч, ч	*tch*	tous les cas	č
Ш, ш	*ch*	tous les cas	š
Щ, щ	*chtch*	tous les cas	ŝ
Ъ, ъ	non transcrit	ou apostrophe	‘
Ы, ы	*y*	tous les cas	y
Ь, ь	non transcrit	ou apostrophe	‘
Э, э	*e*	tous les cas	è
Ю, ю	*ou*	après un и ou un й	û
	ïou	après une voyelle autre que и ou й	
	iou	tous les autres cas	
	you	si convention admise	
Я, я	*a*	après un и ou un й	â
	ïa	après une voyelle autre que и ou й	
	ia	tous les autres cas	
	ya	si convention admise	

Source : https://fr.wikipedia.org/wiki/Transcription_du_russe_en_français

Glossaire des acronymes

En français

CEDH	Cour européenne des droits de l'homme
FAI	Fournisseur d'accès à Internet
DDH	Défense des droits humains
ONG	Organisation non-gouvernementale

En anglais

BGP	*Border Gateway Protocol* (Protocole d'échange de routes externe)
DNS	*Domain Name System* (Système de noms de domaine)
DPI	*Deep Packet Inspection* (Inspection profonde des paquets)
GAFAM / MAGMA	Google, Apple, Facebook, Amazon, Microsoft puis Meta, Apple, Google, Microsoft, Amazon (à partir de 2022)
IP	*Internet Protocol*
IXP	*Internet Exchange Point* (Point d'échange Internet)
OONI	*Open Observatory of Network Interference*
OSINT	*Open Source Intelligence* (Renseignements en source ouverte)
TOR	*The Onion Router*
VPN	*Virtual Private Network* (Réseau privé virtuel)

En russe

FAS	*Feministskoie antivoennoe soprotivlenie* (Résistance féministe contre la guerre)
FBK	*Fond bor'by s korrupciej* (Fondation de lutte contre la corruption, fondée par A. Navalny)
FSB	*Federal'naâ služba bezopasnosti Rossijskoj Federacii* (Service fédéral pour la sécurité)
FZ	*Federal'nij zakon* (Loi fédérale)
Gosuslugi	*Gosudarstvennye uslugy* (Services publics)
MVD	*Ministerstvo vnutrennih del* (Ministère de l'intérieur)
OZI	*Obŝestvo Zaŝiti Interneta* (Société pour la Défense d'Internet)
RAEK	*Rossijskaâ associâciâ èlektronnyh kommunikacij* (Association russe des communications électroniques)
Revizor	Système de contrôle des blocages de sites en Russie
RKN	Roskomnadzor (Agence fédérale russe de régulation des médias et des télécommunications)
Rosreestr	*Federal'naâ služba gosudarstvennoj registracii, kadastra i kartografii* (Service fédéral pour l'enregistrement des biens, le cadastre et la cartographie)
SORM	*Sistema operativno-razysknyh meropriiatij* (Système pour les activités opérationnelles d'enquête)
TSPU	*Tehničeskie sredstva protivodejsviia ugrozam* (Moyens techniques de lutte contre les menaces)

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: zarožd aûšiesiâ 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.

Chapitre 1

Oppression juridique et recours numériques : droit, lois et jugements

Valéry Kossov

« La Russie a atteint sa souveraineté numérique car, toutes les sociétés étrangères étant parties du marché, nous sommes désormais livrés à nous-mêmes » a récemment déclaré le ministre russe du développement numérique Maksoute Chadaev[1]. Ces propos semblent marquer la fin d'une décennie où les autorités russes se sont progressivement efforcées de resserrer leur contrôle sur l'écosystème numérique en l'inscrivant dans le processus de souverainisation d'Internet. Ce processus, présenté dans un premier temps comme la volonté de s'émanciper de l'ingérence étrangère, se traduit par la production massive de lois, dont les fonctions régulatrices prennent rapidement un tour de plus en plus répressif et politisé. Dans le même temps, la souverainisation se présente sous les auspices de l'isolement et de l'autarcie technologique, qui s'accroît particulièrement après le début de l'invasion de l'Ukraine.

Pourtant, et malgré l'abondante législation régissant le domaine numérique, le droit d'Internet ne s'est pas encore définitivement transformé – ni en Russie, ni dans le reste du monde – en une branche unifiée, recoupant dans le même temps tous les secteurs du droit, depuis le droit constitutionnel jusqu'à la procédure pénale, en passant par le droit administratif, commercial ou bancaire [Huet, 2012, pp. 9-10]. En effet, la diversité des objets de régulation et l'extension des usages du numérique incitent les autorités publiques à repenser les réglementations nationales pour encadrer les différents acteurs, pratiques et activités sur Internet. Dans le contexte russe, la régulation du domaine numérique se met en place à mesure que les objets de cette régulation, que ce soit les informations, contenus et données de nature diverse ou des rapports commerciaux, arrivent et se développent progressivement sur le Web. Son contrôle devient ainsi un enjeu majeur pour le régime autoritaire, celui-ci cherchant à affirmer son emprise sur ce domaine qui semblait lui échapper pendant les années 2000. En effet, depuis la présidence de D. Medvedev (2008-2012) et son projet de modernisation

1 « Mincifry ob"âvilo o dostiženii cifrovogo suvereniteta: inostrannye IT kompanii ušli », *Kommersant*, 25 novembre 2022, https://www.kommersant.ru/doc/5682591 consulté le 27 novembre 2022.

économique, l'État cherche à reprendre l'initiative dans le développement des nouvelles technologies, avec la mise en place de nouvelles structures, chargées de coordonner les activités des acteurs publics et privés, mais aussi de les encadrer et de les surveiller[2].

Le retour à la présidence de V. Poutine et la vague de contestations des élections législatives et présidentielles de 2011-2012 marquent une nouvelle étape dans le rapport de l'État à l'écosystème numérique : le premier commence à privilégier davantage son rôle de régulateur, que celui de coordonnateur des acteurs et de leurs activités. Le discours du pouvoir laisse déjà entrevoir une tendance à la souverainisation d'Internet, qui se traduit par le renforcement des emprises de l'État sur le domaine numérique national, avec l'usage du droit comme outil privilégié. C'est ainsi que depuis 2012, l'Assemblée fédérale, parlement russe dominé par le parti du pouvoir « Russie unie », multiplie les initiatives législatives relatives à la régulation d'Internet. Le nombre de projets de loi portant sur le domaine numérique passe de 5 en 2011, à 114 en 2017, démontrant ainsi une ferme volonté des autorités d'élargir le champ des objets de contrôle[3].

Objets et acteurs du droit d'Internet en Russie

Cette législation hétérogène et tentaculaire, adoptée souvent sous forme d'amendements aux lois déjà en vigueur, peut être divisée, en fonction de son champ d'application, en trois blocs, correspondant aux domaines où l'État cherche à assurer sa souveraineté :

- les lois visant à encadrer et à surveiller la circulation des informations et des données ;
- les lois permettant de contrôler l'infrastructure numérique ;
- la législation qui encadre les activités économiques des acteurs privés.

Ce classement reste imparfait, car la portée de certaines lois peut s'avérer plus vaste et couvrir à la fois plusieurs domaines d'application. Cependant, malgré les particularités d'usage, la prise en compte de l'objet d'une loi comme critère de classement permet d'en déduire une certaine logique interne du législateur, correspondant aux finalités de la souverainisation numérique.

---

2 C'est en 2010 que le gouvernement crée dans la banlieue de Moscou le centre d'innovations Skolkovo, pensé comme une nouvelle « Silicon Valley russe » dont la vocation serait d'élaborer et de commercialiser les nouvelles technologies, afin d'attirer ainsi d'importants investissements étrangers [Limonier, 2012].

3 *Svoboda Interneta 2020 : vtoraâ volna repressij*, rapport de Setevye Svobody, 2020 https://runet.report/static/core/doc/Свобода%20интернета%202020.%20Вторая%20волна%20репрессий.pdf

Le processus législatif, intense, s'accompagne de la mise en place d'un système d'interaction institutionnelle impliquant plusieurs acteurs étatiques. C'est ainsi qu'en 2008 se crée l'agence gouvernementale Roskomnadzor (RKN), chargée de surveiller la sphère de l'information et de la communication, et qui servira d'interface entre divers acteurs publics et privés, usant de son droit de saisir la justice en cas d'infraction. Les activités de RKN prennent de l'ampleur, se diversifient progressivement, et mettent l'agence en interaction avec diverses structures gouvernementales, comme le Ministère des communications, la police, le Comité d'enquête, le FSB (service fédéral de sécurité), la Prokouratoura (Ministère public), et d'autres acteurs et utilisateurs d'Internet. Si en 2008, l'année de sa création, RKN faisait état de 49 avertissements aux médias pour la diffusion de matériaux extrémistes, de propagande des drogues, de la pornographie ou de la violence[4], en 2020, l'agence était à l'origine des blocages de plusieurs centaines de milliers de sites Internet[5].

Usages et cibles du droit d'Internet en Russie

Le contrôle par le droit concerne plusieurs ensembles de cibles ou sujets de la régulation. C'est ainsi que la législation adoptée pour contrôler la circulation des informations sur Internet touche progressivement les médias, journalistes, organisations militantes et simples utilisateurs d'Internet, tout comme elle s'impose aux diverses entreprises du secteur numérique (FAI, opérateurs, propriétaires des points d'échange de trafic, etc.). Les premiers concernés ont été des médias numériques d'opposition comme *Grani.ru* ou Kasparov.ru, interdits après l'adoption de la loi Lougovoï en 2013 (398-FZ). En effet, après l'entrée en vigueur en 2012 de la loi 139-FZ qui a introduit le système de «listes noires» de sites comportant des informations illicites[6], la loi Lougovoï étend la portée de l'interdiction aux médias d'opposition politique bloqués sur ordre de RKN et sans décision de justice. Dans le même temps, l'application de ces lois entraîne l'obligation pour les FAI de bloquer les contenus illicites et d'installer à cet effet un boîtier appelé «Revizor» permettant à RKN de contrôler l'exécution des filtrages (voir chapitre 2). De même, les lois Iarovaïa (374 FZ, 375 FZ) adoptées en 2016, introduisent l'obligation de stocker les données numériques des utilisateurs et

4 Rapport d'activité du RKN pour 2008 https://digital.gov.ru/ru/events/20581/ consulté le 2 décembre 2022.

5 Rapport d'activité du RKN pour 2021 https://rkn.gov.ru/plan-and-reports/reports/p449/ consulté le 2 décembre 2022.

6 Dans un premier temps, l'objectif de la loi 139-FZ consistait à protéger les jeunes des informations comportant la propagande des drogues, des jeux de hasard en ligne, la pédopornographie, des appels au suicide.

produisent ainsi un impact sur l'infrastructure et l'économie des FAI, qui se trouvent contraints d'agrandir leurs capacités de stockage de données.

Enfin la loi dite «sur l'Internet souverain» (90 FZ), entrée en vigueur en 2019, permet à l'État de prendre le contrôle des points de trafic transfrontalier, de modifier le routage et de surveiller les contenus. Si dans un premier temps, les autorités justifient la nécessité d'une telle loi par le souci d'assurer le fonctionnement autonome d'Internet en Russie en cas de coupures provenant de l'extérieur[7], les pratiques se sont avérées très éloignées des usages déclarés au départ par l'État, impactant tant la circulation des informations sur l'Internet russe que son infrastructure. En effet, la loi prévoit l'installation de matériel TSPU[8] chez tous les grands opérateurs aux frais de l'État. Celui-ci peut être utilisé pour bloquer automatiquement les contenus interdits au moyen de la technologie DPI (*deep packet inspection*)[9], mais aussi pour ralentir le trafic de certaines plateformes, comme ce fut le cas de Twitter en été 2021, ou encore pour couper l'Internet mobile dans certaines zones et à des moments précis, comme lors des manifestations à Moscou à l'été 2019[10]. Les implications de cette loi vont encore plus loin, pour constituer un moyen de pression sur les entreprises de Big Tech dont les ressources et les bénéfices peuvent être affectées par le ralentissement du trafic. C'est probablement en partie par une telle menace que les autorités russes ont obtenu le retrait de l'application Smart Vote du mouvement de l'opposant A. Navalny des app stores de Google et Apple pendant les élections législatives de l'automne 2021[11]. Enfin, la guerre en Ukraine et l'instauration de la censure en Russie ont permis de mettre ces menaces à exécution, avec le blocage, pour les utilisateurs russes, de Twitter, mais aussi de Facebook et Instagram, à la suite d'un jugement attribuant à la société Meta le statut d'organisation extrémiste[12].

Ainsi, la prise de contrôle sur l'infrastructure du Web par le biais juridique, que ce soit des installations techniques, des algorithmes ou des logiciels, permet à l'État d'étendre son emprise sur le flux d'informations et le trafic. Dans le même temps,

---

7 Notice explicative publiée sur le site de la Douma d'État. «Prinât zakon o suverennom Internete», 16 avril 2019, http://duma.gov.ru/news/44551/ consulté le 28 novembre 2022.

8 *Texničeskie sredstva protivodejstviâ ugrozam*, «Moyens techniques de lutte contre les menaces»

9 L'inspection profonde des paquets de données.

10 «V poslednie gody vlsati «otrubali» Internet v svoix stranah sotni raz. So vremenem vkus k otklučeniäm rastët», *Cnews*, 1er septembre 2021, https://www.cnews.ru/news/top/2021-09-01_eksperty_opasayutsya_zloupotreblenij consulté le 2 décembre 2022.

11 «Human rights advocates decry Apple, Google decision to pull Navalny app as Russia voting begins», *Washington Post*, 17 septembre 2021, https://www.washingtonpost.com/business/2021/09/17/navalny-google-apple-app-russia/ consulté le 2 décembre 2022.

12 Jugement du tribunal du district Tverskoï de Moscou N° 02-2473/2022, https://mos-gorsud.ru/rs/tverskoj/services/cases/civil/details/de7ea6a0-a3ab-11ec-8a7e-51b31fb55b35?participants=Meta consulté le 2 décembre 2022.

la logique de la souverainisation est poussée plus loin, dans la mesure où l'État cherche à s'immiscer dans les activités économiques des sociétés numériques, pour à la fois être en mesure d'imposer des contraintes légales à leur développement sur le marché russe, et pouvoir les sanctionner en cas d'infraction, tout en s'assurant de la bonne exécution des sanctions. Auprès des géants numériques nationaux, comme Yandex, VK (VKontakte) ou Mail.ru, qui se trouvent déjà dans l'orbite de l'État, l'exécution des décisions de justice ou du gouvernement ne trouve pas de résistance. Par exemple, après l'adoption de la loi 208 FZ sur les sites agrégateurs de nouvelles, Yandex a modifié ses algorithmes de sélection des médias en accordant la priorité aux médias gouvernementaux [Daucé & Loveluck, 2021]. Le groupe VK accepte de livrer aux organes de sécurité les données personnelles des utilisateurs[13]. La situation est plus délicate avec les grandes entreprises internationales, dont la présence physique sur le territoire de la Russie est limitée, et qui sont de ce fait moins exposées aux mesures de coercition.

Plusieurs lois ont été adoptées en 2021, visant à pallier ce problème et à renforcer le contrôle du marché numérique russe. Par la loi dite « sur l'atterrissage » (236-FZ), entrée en vigueur en 2021, l'État contraint les entreprises étrangères à ouvrir en Russie des succursales, afin qu'elles portent la responsabilité pour leurs maisons-mères devant la justice russe. D'autres lois (347-FZ) visent à assurer la mainmise de l'État sur le marché de la publicité en ligne, afin de mieux contrôler le système d'imposition sur les bénéfices des acteurs privés, ou encore à faire préinstaller des logiciels fabriqués en Russie sur les produits des grandes marques étrangères commercialisés sur le territoire national (425-FZ). D'une part, l'État poursuit sa stratégie visant à encadrer davantage les acteurs nationaux, par des mécanismes de coercition légaux ou économiques, dont les médias numériques, qui jouent un rôle de plus en plus important dans la diffusion des informations sur Internet, en concurrence avec la télévision contrôlée par l'État. De l'autre, depuis les sanctions consécutives à l'annexion de la Crimée en 2014, il cherche à imposer des contraintes légales aux divers acteurs occidentaux de l'industrie numérique [Nocetti, 2019].

Outre les opérateurs gérant l'infrastructure d'Internet et les grandes entreprises du numérique, la législation touche un ensemble plus large d'acteurs, comprenant des journalistes, des militants, et de simples utilisateurs de plateformes ou réseaux sociaux. La finalité de cette régulation consiste toujours à limiter la circulation des informations et des échanges sur des thèmes sensibles de nature politique, contestant le régime, comme les élections, ou simplement sur des problèmes sociaux que l'État préfère occulter (les violences conjugales, l'écologie, etc.). Le répertoire d'action comprend des poursuites pénales ou administratives

13 Note analytique de Roskomsvoboda, « Vkontakte rasskažet pol'zovatelâm o zaprosah silovikov », 15 août 2018, https://roskomsvoboda.org/40933/ consulté le 28 novembre 2022.

contre les journalistes, militants ou utilisateurs des réseaux sociaux, dont les propos peuvent être interprétés par la police comme relevant de l'« apologie du terrorisme », de l'« appel à l'extrémisme », de l'« outrage à la mémoire de la Grande Guerre patriotique » ou, plus récemment, du « discrédit » de l'armée et d'autres institutions publiques, ainsi que de la diffusion de « fausses informations » sur des sujets portant atteinte à l'ordre public[14]. De l'avis des avocats spécialisés en droit numérique, les motifs sont parfois interprétés très librement par les enquêteurs, car la définition des délits, dans les lois, manque de précision[15]. Les affaires sont montées à partir de la surveillance des réseaux sociaux russes et du monitoring régulier des réseaux sociaux étrangers. L'éventail des normes répressives s'est alourdi avec la mise en place du mécanisme de l'action administrative préjudicielle, qui permet de condamner un utilisateur au pénal après une première sanction administrative. Les sanctions sont souvent appliquées par la justice au mépris du caractère non rétroactif de la loi, ce qui permet de juger un individu pour des informations répréhensibles aujourd'hui, alors qu'elles ont été diffusées il y a dix ans.

Dans un premier temps, les normes du droit pénal et administratif ont été utilisées de façon sélective. Leur usage relevait de l'agenda politique et de l'importance que le pouvoir accorde à tel ou tel cas. Puis au fur et à mesure du raidissement du régime, et surtout après le début de la guerre en Ukraine, l'usage répressif des lois a pris davantage d'ampleur, touchant un vaste ensemble d'acteurs, dont des médias et des ONG indépendants, mais aussi de simples utilisateurs. Ainsi, deux nouvelles lois ont été adoptées en urgence et sont entrées en vigueur le 4 mars (32-FZ) et le 25 mars 2022 (63-FZ). Ces deux lois fédérales apportent des amendements au Code d'infractions administratives et au Code pénal, et prévoient différentes sanctions pour la diffusion des informations discréditant l'armée russe, ainsi que des « fausses informations » sur l'action de l'armée russe, des troupes de Rosgvardia[16], du Parquet, des ambassades et du ministère des Situations d'urgence, dans ce qui est appelé officiellement « opération spéciale en Ukraine ». En ce qui concerne le discrédit de l'armée, le délit est sanctionné au titre de l'article 23.3.3 du Code des infractions administratives par des amendes atteignant en moyenne 35 000 roubles (500 euros). Il s'agit en pratique de sanctionner principalement les divers propos anti-guerre publiés sur les réseaux sociaux, tout comme l'usage même du vocable *vojna* (la guerre) dans des contextes divers. Des sanctions administratives s'appliquent également pour l'affichage

14 La première version de la loi (39-FZ) sanctionnant la diffusion des fausses informations est entrée en vigueur en 2019. Sa portée est étendue en 2020 aux informations sur la pandémie du Covid-19 (100-FZ) et sur l'armée russe depuis le début de la guerre en 2022 (63-FZ).

15 Entretien avec un avocat de Roskomsvoboda réalisé le 19 juillet 2021.

16 Les formations militaires créées en 2016 sur la base des troupes du Ministère de l'Intérieur russe pour renforcer les forces du maintien de l'ordre traditionnelles.

matériel ou virtuel des symboles considérés comme « anti-guerre », à savoir des rubans verts, ou bleus et jaunes[17]. De mars à novembre 2022, le nombre d'affaires administratives relatives au discrédit de l'armée a progressé de façon saisissante, pour atteindre 3 000 environ, dont seulement 100 cas ont été rejetés par la justice russe[18].

Dans le même temps, le nouvel article 207.3 du Code pénal prévoit des poursuites pour la diffusion des « fausses informations », ou *fake news,* sur les activités de l'armée et d'autres institutions d'État[19]. La loi ne donne pas de définition précise de la notion de « fausses informations ». C'est donc aux juges d'instruction et aux experts de l'enquête qu'incombe l'appréciation de la nature des informations et de la gravité des faits[20]. Selon l'avocat Pavel Tchikov, l'usage de cette norme a été calqué sur les pratiques d'application de l'article 207.1, introduit au Code pénal en 2020, qui pénalise la diffusion de fausses informations sur le Covid-19 : toutes les données ne provenant pas des sources gouvernementales sont considérées comme fausses[21]. Désormais, les informations relatives à la guerre qui contredisent les communiqués du Ministère de la Défense russe, voire tous les faits qui n'ont pas été évoqués par le Ministère, sont ainsi traités comme « délibérément mensongers » par la police, et leur diffusion peut entraîner des poursuites au pénal. Au total, au bout de six mois de guerre, le Parquet russe faisait état de 149 affaires pénales relatives à la diffusion de *fake news* sur l'armée[22].

Le public visé par la nouvelle norme comporte des journalistes, des blogueurs et des utilisateurs d'Internet partageant des articles, des images ou des vidéos qui contredisent les données du Ministère de la Défense, ou révèlent des faits passés sous silence par les sources officielles. Ainsi, la publication de chiffres des pertes de l'armée russe non conformes à ceux des statistiques officielles, l'évocation

17 « Novgorodcu naznačili obâzatel'nye raboty za razdaču zelënyh lentoček » Бездформата, 11 mars 2022, https://velikiynovgorod.bezformata.com/listnews/obyazatelnie-raboti-za-razdachu-zelyonih/103340546/ consulté le 30 mai 2022.

18 Statistiques de l'association Setevye Svobody, https://t.me/NetFreedomsProject/673 consulté le 29 novembre 2022.

19 « Federal'nyj zakon o vnesenii izmenenij v Ugolovnyj kodeks Rossijskoj FederaciiF i stat'i 150 i 151 Ugolovno-processual'nogo kodeksa Rossijskoj Federacii », 63-FZ, 25 mars 2022, http://www.consultant.ru/document/cons_doc_LAW_412674/3d0cac60971a511280cbba229d9b6329c07731f7/#dst100009 consulté le 30 mai 2022.

20 Les trois alinéas de l'article 207.3 détaillent les sanctions encourues, qui commencent par des amendes (alinéa 1), pour aller jusqu'à 15 ans d'emprisonnement (alinéa 3), au cas où les actes imputés entraîneraient des conséquences graves pour le fonctionnement de l'armée ou des institutions publiques.

21 « Dezertiroval iz mirnoj žizni v SIZO », *Meduza*, 17 mai 2022, https://meduza.io/feature/2022/05/17/dezertiroval-iz-mirnoy-zhizni-v-sizo consulté le 30 mai 2022.

22 Statistiques de l'association Setevye Svobody, https://t.me/NetFreedomsProject/679 consulté le 29 novembre 2022.

des cas de désertion de soldats ou de policiers contractuels, ou la mention des victimes dans la population civile ukrainienne – toutes ces informations, quelle que soit la forme de publication en ligne (sites Internet, réseaux sociaux, chaînes Telegram) peuvent constituer un prétexte pour engager la responsabilité pénale des individus qui les font circuler.

Dans ces stratégies déployées par l'État pour contrôler les espaces d'information, le recours aux poursuites administratives ou pénales se combine avec des contraintes légales complémentaires, visant à intimider les acteurs évoqués précédemment. Il s'agit de l'obligation d'ajouter la mention « provenant d'un agent de l'étranger » sur les publications des ONG, médias, et plus récemment des personnes physiques reconnues « agents de l'étranger » par le Ministère de la Justice russe (272-FZ, 2012 ; 327-FZ, 2017 ; 481-FZ, 2020)[23]. Le Kremlin réfute régulièrement le caractère répressif de ces lois[24]. Cependant, outre les contraintes d'ordre financier qu'elles entraînent pour les acteurs concernés, ces lois les désignent à la vindicte, dans l'espace public russe, sous une étiquette porteuse de connotations négatives [Baunov, 2021]. Les registres des « agents de l'étranger » du ministère de la Justice se sont remplis assez vite, en particulier ces deux dernières années[25] où l'application de la loi s'est élargie à des domaines autres que politique. La notion d'engagement dans des activités politiques, principal motif permettant d'attribuer le statut d'agent de l'étranger, est définie de manière très vague (art. 2.1 de la Loi 272-FZ), ce qui laisse à la discrétion des autorités toute latitude pour l'appliquer. Par conséquent, le Ministère de la Justice inclut dans ses registres non seulement des médias non-gouvernementaux ou des ONG impliquées en politique, mais également des organisations politiquement neutres qui ne bénéficient pas des financements d'État[26]. Par ailleurs, les sanctions administratives, sous forme d'amendes, se multiplient en 2021 pour défaut de

23 La loi prévoit entre autres un système complexe de comptes rendus justificatifs des revenus et des dépenses que les sujets reconnus « agents de l'étranger » doivent rendre aux autorités, ainsi que d'autres restrictions des droits des personnes physiques.

24 Lors des conférences de presse en ligne, le représentant du Kremlin Dmitri Peskov rappelle régulièrement que le statut d'agent de l'étranger ne représente pas un obstacle au travail des médias et des journalistes en Russie. « V Kremle isključili ograničenie raboty Meduzy iz-za statusa inoagenta », *RBC*, 28 avril 2021, https://www.rbc.ru/rbcfreenews/60893eb09a79475e858c563e consulté le 23 juin 2022.

25 Les listes de médias, ONG ou personnes physiques frappées du statut d'agent de l'étranger peuvent être consultées sur le site du Ministère de la justice. Le suivi de l'usage de la loi se complique toutefois par la tenue de plusieurs registres où sont inclus séparément les médias étrangers exerçant la fonction d'agent de l'étranger, les ONG, etc. Malgré cette difficulté, le registre des médias étrangers reconnus comme « exerçant la fonction d'agents de l'étranger » nous permet d'évaluer la dynamique de l'application de la loi en 2021. Site du Ministère de la Justice de la Fédération de Russie, https://minjust.gov.ru/ru/documents/7755/ consulté le 15 avril 2022.

26 Il s'agit par exemple des associations féministes, des organisations de lutte contre les violences conjugales ou pour la protection des droits des enfants.

signalement comme « agent de l'étranger » des sources ou références dans les publications en ligne[27]. Ces affaires se comptent par centaines, rien qu'à Moscou, et concernent tant les sites des médias, réseaux sociaux et ONG, que ceux des associations professionnelles.

L'existence de quatre registres séparés des « agents de l'étranger » (ONG, médias, personnes physiques et associations non-enregistrées) pose le véritable problème de leur contrôle par des instances étatiques et crée de la confusion lors de l'attribution de ce statut, avec différents types de contraintes. Afin de rationaliser l'usage de cette norme, mais aussi pour durcir davantage son effet sur ce groupe d'acteurs hétérogènes, le législateur a décidé d'adopter une nouvelle loi, intitulée « sur le contrôle des activités des personnes se trouvant sous influence étrangère » (loi 255-FZ) qui est entrée en vigueur le 1er décembre 2022. Elle réunit les dispositions juridiques relatives au statut d'agent de l'étranger éparpillées entre plusieurs lois, et introduit des critères homogènes pour l'attribution de ce statut aux personnes physiques ou morales. La loi prévoit un registre unique ainsi qu'une procédure standardisée de radiation de ce registre. D'une manière générale, cette loi accorde davantage de marge de manœuvre aux autorités pour attribuer ce statut, car le financement étranger n'en sera pas le critère déterminant. En effet, un individu peut être déclaré « agent de l'étranger » au motif d'avoir obtenu un « soutien étranger », quelle qu'en soit la forme, matérielle ou immatérielle, ou s'il se trouve « sous une influence étrangère ». Le caractère vague de ces critères laisse le champ libre à l'interprétation des cas par les organes de maintien de l'ordre, et permet d'étendre, si nécessaire, la portée de la loi à l'ensemble de la population russe à l'exception des agents de la fonction publique, personnels des entreprises d'État, membres des partis politiques ou fonctionnaires des organisations internationales. Dans le même temps, la loi introduit des contraintes supplémentaires pour les « agents de l'étranger », limitant sensiblement leurs droits civiques, notamment dans le domaine électoral, et elle prévoit une procédure unique, bien encadrée, de sortie de ce statut[28]. La stratégie de l'État consisterait ainsi à garder dans le viseur toute personne susceptible d'exprimer en ligne ses désaccords avec le point de vue officiel, et pouvoir l'écarter légalement de la vie publique pendant les périodes électorales, ou dans des situations de tensions, tout en ménageant une « voie de secours » pour ceux qui seraient prêts à manifester leur allégeance au régime.

---

27 Le défaut de signalement récurrent peut conduire au retrait de la licence et au blocage du média. C'est la raison pour laquelle le 28 mars 2022, le quotidien *Novaïa Gazeta* a décidé de suspendre ses activités après avoir reçu le deuxième avertissement du RKN relatif au non-signalement d'une ONG « agent de l'étranger » dans un article du journal. Voir le communiqué de la rédaction : https://novayagazeta.ru/articles/2022/03/28/roskomnadzor-soobshchil-chto-vynes-vtoroe-preduprezhdenie-novoi-gazete-news, consulté le 15 avril 2022.

28 Rapport Inoteka, 28 avril 2022, https://inoteka.io/ino/2022/04/28/novyy-zakon-ob-inoagentah-chto-pomenyaetsya consulté le 30 mai 2022.

D'autre part, l'intimidation se renforce avec la loi 272-FZ, datant de 2012, mais complétée en 2015 et 2021, qui introduit la notion d'« organisations indésirables représentant une menace pour la sécurité de l'État ». Il s'agit de médias et d'ONG dont les activités sont simplement interdites sur le territoire de la Russie. Cela se traduit par l'impossibilité d'avoir des succursales pour des entreprises, médias ou ONG étrangers et russes, ou d'effectuer des opérations financières, mais aussi de diffuser des informations sur Internet puisque les sites de ces organisations se trouvent inscrits sur la « liste noire » de RKN. Comme dans le cas des « agents de l'étranger », un signalement pour le lecteur est obligatoire à chaque fois que le nom de l'organisation apparaît dans des publications en ligne, qu'il s'agisse d'articles de presse, de blogs ou de réseaux sociaux. Depuis 2021, la législation s'est alourdie, prévoyant des peines de prison importantes pour sanctionner la participation aux activités des « organisations indésirables », ce qui a conduit à l'auto-dissolution ou à l'exil des ONG, médias ou autres acteurs (voir chapitre 8)[29]. Le registre du Ministère de la Justice inclut tant des ONG politiques, comme Otkrytaïa Rossiïa ou des observateurs étrangers des élections russes, que des médias faisant du journalisme d'enquête, comme *Proekt Media, Bellingcat, The Insider*, des organisations religieuses, ou encore *Bard College*, l'université privée américaine de sciences humaines qui avait ouvert une faculté des arts auprès de l'Université de Saint Pétersbourg[30].

Enfin, la situation s'aggrave encore sur le plan répressif dans le cas des organisations reconnues comme « extrémistes ». Selon la loi 114-FZ, c'est sur décision de justice que le statut d'organisation extrémiste peut être attribué, impliquant la liquidation, mais surtout des sanctions pénales pour ceux qui ont participé aux activités de l'organisation ou lui ont alloué des financements. Des sanctions s'appliquent également pour la diffusion et l'affichage public de matériaux divers de l'organisation (publications, vidéos, images, logos, etc.). Si dans le cas de l'ONG de Navalny, la Fondation anti-corruption (FBK) reconnue comme « organisation extrémiste » en 2021, les questions d'application ne se posent pas[31], il n'en est pas de même avec la société Meta Platforms (maison mère de Facebook) qui s'est vu attribuer ce statut le 22 mars 2022. En effet, cette

29 Plusieurs membres de l'ONG de M. Khodorkovski Otkrytaïa Rossiïa ont été ainsi condamnés post factum au pénal pour participation à une « organisation indésirable » après sa dissolution en 2021. Souvent la police utilise comme prétexte des *repost* sur Facebook des informations sur l'ONG datant d'avant 2021, et donc antérieurs à l'adoption des amendements pénaux augmentant les peines. C'était notamment le cas d'Andreï Pivovarov, ancien directeur d'Otkrytaïa Rossiïa, condamné en 2022 à quatre ans de prison.

30 Registre du Ministère de la Justice, https://minjust.gov.ru/ru/documents/7756/ consulté le 15 avril 2022.

31 Les collaborateurs de Navalny ont été contraints pour la plupart de quitter la Russie. Toutes les publications de FBK sont bannies du Web et leur reproduction est sanctionnée, tout comme l'abonnement à la chaîne Telegram de Navalny et à d'autres réseaux sociaux de la FBK.

loi n'a encore jamais été utilisée contre une grande entreprise internationale, d'où les nombreuses interrogations des juristes sur ce qui est susceptible d'entraîner des sanctions pénales, et surtout l'inquiétude des utilisateurs des réseaux sociaux et des autres produits de Meta, ou encore des investisseurs russes[32].

L'arsenal des outils juridiques prend ainsi de plus en plus de poids, dans la vie politique et sociale russe, affectant aussi bien les infrastructures numériques que les différents acteurs sociaux. L'ampleur de la législation semble désormais couvrir la plupart des domaines où s'exerce la régulation étatique, traduisant la volonté d'encadrer la circulation des informations à l'intérieur du pays. Ainsi, dès avant la guerre, l'État avait drastiquement renforcé son contrôle sur l'Internet et sur une grande partie des activités non-gouvernementales. Dans la situation actuelle, quelles sont les implications de cette législation pour les différents acteurs de l'écosystème numérique russe, et comment peuvent-ils faire face à cet arsenal juridique de régulation, dévoyé à des fins répressives ?

Les stratégies de résistance et de contournement de l'oppression juridique

La multiplication des contraintes juridiques, en particulier dans le contexte de la guerre en Ukraine, a pour conséquence la réduction du champ d'action des médias, des milieux militants et de la liberté d'expression de manière générale, mais surtout sur Internet, qui est devenu un espace privilégié pour la censure. Bien que l'État semble avoir une emprise totale sur l'espace juridique, avec la mise au service de l'exécutif des pouvoirs législatif et judiciaire, il reste un certain nombre d'outils légaux permettant aux entreprises, médias, militants et utilisateurs de se défendre, avec le concours de quelques ONG proposant les services d'avocats. Il existe actuellement plusieurs organisations assurant la défense des droits numériques : Setevye Svobody (« Libertés des réseaux ») prenant le relais de l'association

32 En effet, le RKN a bloqué Facebook et Instagram tout en laissant libre d'accès l'application WhatsApp. Les utilisateurs des réseaux sociaux de Meta ne sont pas pénalisés *a priori*, mais il est interdit d'afficher le logo de Meta ou d'acheter ses actions à la bourse. La situation ne cesse d'évoluer et le Parquet de Moscou a fait en octobre 2022 un avertissement à une blogueuse de mode russe sur Instagram, pour l'usage de la plateforme, alors que ses publications n'ont aucun rapport avec la politique ou la guerre. Voir « Pervoe blogerskoe predupreždenie » *Advokatskaâ ulica*, 6 octobre 2022, https://advstreet.ru/columns/pervoe-blogerskoe-preduprezhdenie/ consulté le 30 novembre 2022.

Agora[33], ainsi que le cabinet d'avocats Digital Rights Center créé par les juristes de l'ONG Roskomsvoboda. D'autres, comme le Centre de défense des droits des médias, OVD-info, ou Pervyï otdel, se chargent d'une manière plus large de la protection des droits des journalistes, des militants ou de simples citoyens poursuivis par divers organes de répression.

Dans ce contexte politique sensible, et *a fortiori* dans celui de la guerre, l'action en justice contre l'État et ses institutions est plutôt rare, et la défense des accusés s'avère peu fructueuse. Selon une militante interviewée, il s'agit essentiellement de « soins palliatifs » accordés aux personnes prises dans les rouages de la machine répressive de l'État[34]. Des plaintes contre RKN et d'autres structures de l'exécutif ont pourtant été déposées régulièrement avant la guerre, sans toujours aboutir à des décisions satisfaisantes. Toutefois, ce recours à l'action en justice contre l'État, ou par une plainte contre X, reste un outil que les avocats engagés considèrent comme assez efficace, car il peut provoquer le débat public autour des problèmes de limitation des droits numériques, ou constituer un précédent de justice[35]. La saisine de la justice attire l'attention des médias et sensibilise l'opinion publique aux conséquences de telle ou telle initiative de l'État, notamment concernant l'usage des données biométriques, ou la reconnaissance faciale lors de la surveillance vidéo. Au-delà de la simple victoire dans l'affaire en cours, cette stratégie du litige stratégique vise à laisser une trace durable dans la société et à produire un effet sur le public en général, et sur les autorités en particulier.

Avant la guerre, les avocats de Setevye Svobody cherchaient eux-mêmes des jugements discutables ou des condamnations abusives d'utilisateurs d'Internet, pour pouvoir les contester auprès de la Cour européenne des droits de l'homme (CEDH), après avoir épuisé les possibilités de recours devant les juridictions russes. Il s'agissait d'une procédure compliquée avec des délais souvent très longs, l'examen des plaintes nécessitant des échanges fastidieux avec la justice russe. Cependant, c'était un moyen non négligeable pour obtenir gain de cause, et pour établir un canal de communication entre les juridictions européenne et russe aboutissant tant à la constitution de précédents et à des ajustements des pratiques judiciaires en Russie, qu'au versement de réparations financières aux justiciables russes. Notamment, dans les jugements condamnant les internautes

33 Fondée en 2005, l'association Agora a été déclarée « ONG agent de l'étranger » en 2014, puis liquidée par une décision de justice en 2016. Agora International qui a succédé à l'ONG dissoute depuis 2016 n'a pas de personnalité morale et constitue, selon les propos du fondateur d'Agora, Pavel Tchikov, davantage « un club d'intérêt » pour la défense des droits humains qu'une organisation à but lucratif. Voir Smirnov Sergueï « Osoznannoe dopusênie ugolovnogo dela i tur'my », interview avec Pavel Tchikov, *Mediazona*, 28 novembre 2015, https://zona.media/article/2015/26/11/agora-international consulté le 15 avril 2022.

34 Entretien du 19 novembre 2022.

35 Entretiens du 19 et 23 juillet 2021.

pour irrespect du pouvoir (loi 30-FZ), les recours devant la justice russe et la CEDH ont permis de réduire l'usage de cette loi par les organes d'instruction en 2020-2021[36].

Ce précieux outil est devenu caduque après le début de la guerre en Ukraine. Le 16 mars 2022, le Comité des Ministres du Conseil de l'Europe a décidé d'exclure la Russie de cette organisation, ce qui a entraîné la dénonciation par la Russie de la Convention européenne des droits de l'homme et sa sortie du système de protection des droits et libertés et de la Cour européenne des droits de l'homme[37]. Cette exclusion se répercute directement sur les justiciables russes, car les citoyens russes ne peuvent plus saisir la CEDH afin de faire condamner l'État pour violation de leurs droits. Formellement, la Russie a gardé son statut de membre du CE jusqu'au 1er janvier 2023, et les requêtes des plaignants russes déposées avant le 16 septembre 2022 pouvaient être examinées par la CEDH[38]. Cependant, après avoir dénoncé la Convention européenne des droits de l'homme, la Russie n'accepte plus de suivre les arrêts rendus par la CEDH pendant cette période, et le Parquet russe a mis fin à ses échanges avec la juridiction européenne. Pendant le printemps 2022, certains avocats russes restaient persuadés que, pendant cette période, le dépôt des plaintes devant la CEDH avait tout son sens et constituait toujours un ultime moyen de protéger les droits humains[39]. Cependant, un nouveau projet de loi, déposé à la Douma le 16 mai 2022 et définitivement adopté le 11 juin 2022 (loi 183-FZ), prévoit la non-exécution par la Russie des décisions de la CEDH prises après le 16 mars 2022[40]. Malgré son caractère contradictoire, le loi permet à l'État russe de mettre fin brusquement aux versements des compensations aux plaignants, dont le nombre pourrait augmenter sensiblement depuis le 24 février 2022, compte tenu des pratiques judiciaires controversées

36 «Sto nedrugov vlasti : kogo i kak nakazyvaût v Seti», Roskomsvoboda, https://roskomsvoboda.org/post/sto-nedrugov-vlasti-kogo-i-kak-nakazyiv/ consulté le 30 novembre 2022.

37 «La Fédération de Russie est exclue du Conseil de l'Europe», salle de presse du Comité des Ministres du CE, 16 mars 2022, https://www.coe.int/fr/web/portal/-/the-russian-federation-is-excluded-from-the-council-of-europe consulté le 15 avril 2022.

38 Selon l'article 58, paragraphe 1 de la Convention, les parties ne peuvent dénoncer la Convention qu'après un préavis de six mois. En attendant, toutes les obligations des parties prévues par la Convention demeurent effectives et inchangées. C'est dans ce sens que les dispositions de l'article 58 ont été interprétées par la CEDH. «Resolution of the European Court of Human Rights on the consequences of the cessation of membership of the Russian Federation to the Council of Europe in light of Article 58 of the European Convention on Human Rights», https://echr.coe.int/Documents/Resolution_ECHR_cessation_membership_Russia_CoE_ENG.pdf consulté le 14 avril 2022.

39 «Napomnit' rossijskim vlastäm odnu važnuû veŝ», interview d'Ekaterina Gorbunova avec l'avocat Dmitri Gurin, *Advokatskaïa Oulitsa*, 24 mars 2022, https://advstreet.ru/interview/napomnit-rossiyskim-vlastyam-odnu-vazhnuyu-veshch/ consulté le 15 avril 2022.

40 «Rešeniâ ESPČ ne budut ispolnâtsâ v RF: zakonoproekt», site de l'avocat Oleg Anišikov, 17 mai 2022, https://europeancourt.ru/2022/05/17/36465/ consulté le 30 mai 2022.

dans les affaires liées à la censure militaire[41]. Cela marque également une rupture unilatérale et rapide des rapports entre la justice russe et la CEDH.

Enfin, d'un point de vue juridique, la Russie peut un jour réintégrer le Conseil de l'Europe et le système de la Convention européenne des droits de l'homme, ce qui rétablira son statut auprès de la CEDH, même si le caractère autarcique des aspirations à la souverainisation de la justice et du système normatif russes observé ces dernières années, tout comme le discours actuel des dirigeants politiques en rupture avec le droit international, semblent renvoyer cette possibilité à une perspective éloignée[42].

Pour défendre leurs clients, les avocats mobilisent d'autres astuces juridiques. Par exemple, ils parviennent à trouver des vices de forme et à invalider les preuves numériques réunies par l'instruction. Ainsi, si le procès-verbal d'instruction invoque une capture d'écran d'un document répréhensible faite depuis un ordinateur fixe, alors que le visuel du document provient du smartphone de l'enquêteur, le tribunal sera amené à ne pas reconnaître la validité de la preuve[43]. Les failles de ce type et bien d'autres permettent parfois de gagner les affaires en justice. Les avocats interrogés reconnaissent toutefois que ces stratégies ne sont plus efficaces dans les affaires sensibles et politisées, lorsque l'instruction, l'accusation et la justice font front commun contre la défense et les prévenus. Les marges de la résistance par la voie légale sont, dans ce cas, très limitées.

Étant donné que les avocats encourent eux-mêmes le risque de poursuites, certaines stratégies d'anticipation déployées relèvent davantage du contournement et de l'adaptation que de la résistance. Notamment, certaines organisations militantes, comme Setevye Svobody ou Agora International, mènent leurs activités sous forme de «projet» sans être officiellement enregistrées en tant qu'ONG, et en évitant de se localiser dans un lieu précis. Ainsi, elles n'ont pas de bureaux pouvant être perquisitionnés par la police et s'expatrient entièrement dans l'espace virtuel, avec notamment des chaînes sur la plateforme de messagerie Telegram leur permettant de communiquer sur les particularités de nouvelles lois, leur application, la jurisprudence, et d'informer leurs collègues et d'autres publics intéressés sur les droits et les moyens juridiques de résistance à l'arbitraire des autorités policières. Cela se fait toutefois dans le strict respect de la législation, avec ses contraintes, afin de pouvoir exercer leurs fonctions d'avocats en *off-line* auprès de la justice. D'autres organisations s'expatrient à l'étranger, comme

41 Certains plaignants peuvent obtenir des réparations jusqu'au 1er janvier 2023 sur décision du Parquet russe.

42 Interview de Dmitri Medvedev à l'agence RIA et la chaîne de télévision RT du 26 mars 2022, https://ria.ru/20220326/medvedev-1780208448.html consulté le 15 avril 2022.

43 Entretien du 17 juin 2022.

l'ancienne équipe de Komanda 29 (« Team 29 »), une association de journalistes et de juristes spécialisés dans les affaires d'atteinte au secret d'État), devenue Pervyï otdel en Géorgie, et son créateur l'avocat Ivan Pavlov, accusé d'avoir divulgué des éléments d'enquête, son statut ayant été suspendu par la Chambre des avocats de Saint Pétersbourg[44]. S'il s'agit avant tout d'échapper aux poursuites individuelles, cette stratégie de dernier ressort permet également de garder la possibilité de poursuivre des activités depuis l'exil, tout en s'appuyant sur un réseau de collègues restés en Russie pour comparaître aux procès.

Les stratégies d'adaptation individuelles ou collectives comprennent l'utilisation des moyens de sécurité informatique, avec l'usage quasi-banalisé d'un VPN, le chiffrement de données, l'utilisation de messageries jugées fiables comme Signal, Telegram ou Wire, l'élaboration de solutions individuelles de protection des données ou de contournement des blocages. Ces stratégies sont partagées à travers des groupes d'échange, des formations collectives sous forme de *webinar* ou *hackathons*. Les juristes de Roskomsvoboda ont organisé à Moscou une école qui forme aux spécificités du droit dans le domaine numérique. Ces savoirs et compétences circulent à l'international, à travers les collaborations avec des associations de défense de droits numériques dans les pays de l'espace postsoviétique comme le Kazakhstan, le Kirghizstan ou la Biélorussie, et avec les associations internationales de défense des droits humains, comme International Network of Civil Liberty Organization (INCLO), et des droits numériques Access Now. Ces collaborations, même si elles ne prévoient pas nécessairement un financement étranger, demeurent toujours une prise de risque pour les associations russes, car le statut d'agent de l'étranger pourrait leur être attribué pour leur participation à des formations dispensées par une ONG étrangère, assimilée par les autorités à une « assistance étrangère non-matérielle », ou désormais à « l'influence étrangère ».

Ainsi, le répertoire d'actions des milieux militants a beaucoup évolué durant la dernière décennie en s'adaptant au durcissement de la législation, de la répression en ligne et aux restrictions des droits numériques. Quelques perspectives émergent concernant leur avenir, dans un champ juridique de plus en plus contraignant, et qui théoriquement semble désormais suffisant pour exclure toute liberté d'expression de l'espace numérique « souverainisé », et plus largement de l'espace social russe.

44 Pavlova, Zinaida, « Stalo izvestno, čem Sovet AP Sankt Peterburga motiviroval priostanovlenie statusa advokata Ivana Pavlova », *Advokatskaïa Gazeta*, 5 avril 2022, https://www.advgazeta.ru/novosti/stalo-izvestno-chem-sovet-ap-sankt-peterburga-motiviroval-priostanovlenie-statusa-advokata-ivana-pavlova/ consulté le 2 décembre 2022.

Conclusion

La souverainisation d'Internet en Russie, accompagnée d'une régulation juridique aussi opaque qu'omniprésente, et de plus en plus répressive, a amené le système juridique vers un modèle mono-normatif, avec la méfiance grandissante des institutions d'État envers les acteurs internationaux et la défiance vis-à-vis de leurs sources de droit. Ces dernières années, il tend davantage à la mono-normativité [Barraud, 2018], c'est-à-dire un modèle où les normes régissant le cyberespace ont une origine exclusivement étatique. Un tel système normatif éloigne sensiblement la perspective d'une co-régulation d'Internet et touche à la fois aux infrastructures, aux entreprises du numérique et aux utilisateurs. Il réprime ainsi le développement concurrentiel des technologies numériques, mais surtout la circulation des informations et les activités en ligne des médias et militants indépendants, tout autant que l'expression libre des utilisateurs. Ainsi, les récents jugements administratifs sanctionnent *de facto* l'expression même d'une opinion sur la guerre, qui, pour la justice, devient un délit de discrédit, de manque de respect, ou encore d'appel à la haine vis-à-vis de l'armée et des institutions d'État. Quant au Code pénal, c'est lui qui est mobilisé dans les cas de *fake news,* pour sanctionner la confrontation et le partage en ligne de faits et d'événements relatifs à la guerre, interprétés par la justice comme une manipulation de l'opinion publique. L'usage répressif du droit s'inscrit donc pleinement dans la logique de la souverainisation de l'espace numérique, que le Kremlin poursuit depuis le début des années 2010, cherchant à uniformiser les canaux d'information et à les aligner sur les sources officielles.

D'autre part, ce processus de souverainisation révèle le peu d'intérêt que l'État manifeste pour une auto-organisation horizontale de la population et pour toute forme de *feedback* ou d'information alternative provenant des médias, des ONG et des militants. Les perspectives sont donc peu réjouissantes pour ces acteurs, car, outre l'acharnement judiciaire, l'État ne leur accorde évidemment aucun financement et ne favorise pas non plus les dons privés des entreprises russes. Ils sont donc contraints de trouver des fonds à l'étranger, ce qui les conduit inévitablement au statut d'agent de l'étranger. La loi « sur les agents de l'étranger » restera donc à l'avenir une épée de Damoclès suspendue en permanence au-dessus des acteurs concernés, quel que soit leur domaine d'activité : journalisme d'investigation, observation des élections, écologie, violence familiale ou droits des femmes.

D'une part, cette abondance de lois aux formulations parfois obscures et peu précises laisse la place à l'interprétation abusive des normes. De l'autre, le manque de clarté dans la législation engendre des difficultés pour son application. En effet, en Russie l'approche positiviste dans l'usage du droit donne lieu à une régulation

excessive des moindres questions par des lois, limitant ainsi l'autonomie de la justice. Or les rythmes élevés de production de textes de lois, sur commande, provenant essentiellement du gouvernement ou de l'Administration présidentielle, traduisent uniquement la volonté de l'exécutif. Celui-ci est amené par la suite à préciser les modalités de l'exécution des lois, par le biais de divers règlements et circulaires, alourdissant encore davantage la régulation [Šul'man, 2020]. Par ailleurs, les lois sont souvent votées sans véritables consultations des professionnels du web ou du droit numérique, par des députés démunis de compétences techniques ou juridiques. Cela crée en conséquence des difficultés de compréhension et d'interprétation de ces textes par la police et les juridictions. La régulation par le droit de l'espace de l'information produit ainsi une fausse impression de contrôle, alors qu'elle introduit de la confusion, mais aussi de l'arbitraire, au sein même des institutions étatiques. Ainsi, les lois récentes dites « sur la censure militaire » laissent à la discrétion de la police l'interprétation et l'appréciation des faits, sans lui fournir de définitions précises du « discrédit » ou de la « fausse information ». Par conséquent, cela donne lieu à des sanctions qui peuvent varier, dans un espace juridique *a priori* homogène, depuis les amendes administratives jusqu'à des peines de prison ferme, pour des faits parfois identiques.

Enfin, les ambitions du législateur surestiment parfois le développement des technologies et des investissements dans le domaine numérique. Malgré les progrès récents des boîtiers DPI et des autres techniques de blocage et de surveillance, un certain nombre de lois, dont la loi Iarovaïa, attendent toujours d'être suivies d'effet, faute de moyens humains et techniques. D'autres dispositions légales coercitives sont laissées à l'abandon, ou du moins dépénalisées à cause des problèmes soulevés par leur exécution. La souveraineté numérique et technologique, telle qu'elle se présente dans le discours, la doctrine et les normes, semble encore loin d'être réalisée. Elle semble même sensiblement compromise par la rupture des échanges, conséquence de la guerre avec les pays occidentaux. De son côté, le droit d'Internet, tourné vers les objectifs de la souverainisation, s'inscrit dans un modèle coercitif, qui semble peu viable en dehors du système des interdépendances technologiques, et qui se heurte à ses contradictions internes, évoluant, dans le contexte de la guerre et des sanctions économiques, vers davantage d'autarcie et d'isolement.

Références bibliographiques

[Barraud, 2018] Barraud, Boris, « La corégulation d'Internet (ou comment répondre à la plurinormativité par l'internormativité) – Une contribution française », *Les Cahiers de droit*, vol. 59, n°1.

[Baunov, 2021] Baunov, Alexandre, « Inostrannyj agent. Politiko-semantičeskij analiz », *Centre Analytique Carnegie*, Moscou, https://carnegie.ru/commentary/85578.

[Daucé & Loveluck, 2021] Daucé, Françoise & Loveluck, Benjamin, « Codes of conduct for algorithmic news recommendation: The Yandex.News controversy in Russia », *First Monday* vol. 26, n° 5.

[Huet, 2012] Huet, Jérôme, « Le juriste et la communication numérique : une brève introduction », in Teyssié, Bernard (dir.), *La Communication numérique, un droit, des droits*, Paris, Editions Panthéon-Assas.

[Limonier, 2012] Limonier, Kevin, « Analyse géopolitique des enjeux d'une politique de puissance : le cas de la science et de l'innovation en Russie », *Hérodote*, n° 146-147, p. 193-216.

[Morozov, 2011] Morozov, Evgeny, *The Net Delusion. How Not To Liberate the World*, Penguin UK.

[Nocetti, 2019] Nocetti, Julien, « La Russie en quête de son « Internet souverain », *Revue des médias*, https://larevuedesmedias.ina.fr/la-russie-en-quete-de-son-Internet-souverain.

[Šul'man, 2020] Šul'man, Ekaterina, *Praktičeskaâ politologiâ. Posobie po kontaktu s real'nost'û.*, Moskva, ACT.

Chapitre 2

Surveillance et censure des infrastructures Internet en Russie : marchés, régulation et boîtes noires

Ksenia Ermoshina, Benjamin Loveluck et Francesca Musiani

Dès le début des années 2010, le développement de l'Internet russe a été marqué par un fort interventionnisme de l'État, tant en termes d'instruments juridiques que d'infrastructures techniques. Dans le contexte de la doctrine du « Runet souverain », un volet important de la stratégie des autorités a consisté à encourager le développement de solutions techniques de fabrication russe destinées à la censure et l'interception du trafic Internet. Un marché florissant s'est donc ouvert aux fournisseurs russes de solutions logicielles et matérielles pour la surveillance et le filtrage du réseau.

Ce chapitre propose une analyse de cette industrie et de ses effets sur les fournisseurs d'accès à Internet (FAI), ancrée à la fois dans la sociologie des techniques et de l'innovation et dans l'économie politique, et qui s'appuie sur une méthodologie plurielle. Le chapitre retrace les controverses suscitées par les différents assemblages technologiques que les acteurs de l'Internet russe doivent adopter pour être en conformité avec la réglementation en vigueur, mais qui sont coûteuses et complexes à mettre en œuvre et qui soulèvent de nombreuses préoccupations éthiques et politiques.

Dans un premier temps, nous distinguons deux stratégies distinctes de contrôle de l'information : la surveillance en ligne (ou « interception légale ») d'un côté et la censure (ou « filtrage du trafic ») de l'autre. Nous présentons ainsi deux types de dispositifs qui ont été au centre de la loi Iarovaïa de 2016, et nous discutons leur influence sur le marché des FAI : d'un côté, les systèmes de surveillance appelés SORM (« système pour les activités opérationnelles d'enquête ») qui établissent un lien direct avec les agences de renseignement, et de l'autre les solutions de filtrage du trafic utilisées pour bloquer l'accès aux sites Web placés sur liste noire par Roskomnadzor (RKN), l'agence fédérale russe de régulation des médias et des télécommunications.

Dans un deuxième temps, nous montrons le pas supplémentaire qui a été franchi avec la loi « pour un Internet souverain » de 2019. En effet, tous les opérateurs doivent depuis installer sur leurs réseaux un nouveau type de dispositifs appelés « TSPU » (« moyens techniques de lutte contre les menaces »). Ceux-ci comportent un filtre DPI (*deep packet inspection*) capable d'analyser les paquets de données, de ralentir ou de bloquer l'accès à certaines ressources et, comme la loi de 2019 le prescrit, de limiter la circulation du trafic à l'intérieur de la Russie. Par exemple, en 2021, le dispositif a été utilisé pour ralentir Twitter ou encore pour bloquer l'application d'aide au vote proposée par l'opposition lors des élections. Ce filtrage peut être activé à distance, ne requiert pas la collaboration des opérateurs et échappe à toute surveillance citoyenne. Cette nouvelle contrainte imposée aux FAI marque un tournant dans le contrôle exercé par les autorités sur les infrastructures numériques.

Ce chapitre analyse les effets de ces mesures sur les équilibres du marché russe de l'Internet et sur ses relations avec les réseaux et services étrangers, et évalue la capacité des acteurs à contourner ce système à travers un ensemble de ruses juridiques et techniques. Enfin, il analyse l'impact de l'invasion de l'Ukraine par la Russie sur ces technologies de contrôle d'information, en montrant comment les sanctions internationales ont dévoilé le rôle des grands fabricants internationaux dans le projet techno-juridique du « Runet souverain ». Avec le départ de la Russie de Nokia, IBM, Intel ou Cisco du marché des télécoms russe, que reste-t-il des boîtiers de surveillance et de censure ?

Une étude socio-économique des « boîtes noires » de l'Internet russe

Avec plus de 6 326 licences délivrées en 2020 (et entre 3 461 et 3 940 d'entre elles actives[1]), l'industrie russe des fournisseurs de services Internet se caractérisait jusqu'à la fin des années 2010 par une forte concurrence, des prix bas, une bonne qualité de connectivité, ainsi qu'une topographie relativement décentralisée et un nombre important d'accords de *peering* transnational. De nombreux FAI russes ont commencé comme « réseaux locaux » (*domovaya set'*), et ont formé des communautés professionnelles actives, d'où le nombre important d'associations, conférences et forums professionnels. À partir du milieu des années 2010, cependant, le marché des FAI a été progressivement affecté par une centralisation

1 Les fournisseurs d'accès eux-mêmes proposent des façons différentes d'analyser le marché. Notamment, une étude a été conduite par plusieurs employés des FAI en décembre 2017 selon laquelle il existait 3 940 FAI actifs (https://habr.com/en/post/345258/) alors que selon RKN, seulement 3 461 FAI se sont déclarés au régulateur en 2018 (https://rkn.gov.ru/news/rsoc/news70316.htm).

juridique et infrastructurelle grandissante. Entre 2017 et 2020[2], le nombre de licences délivrées pour les « Services télématiques » et les « Services de transfert de données » a diminué (respectivement de 9 395 à 8 000 et de 7 035 à 6 326[3]). En outre, parmi les initiatives gouvernementales visant à créer un « Internet russe autonome », figure l'introduction d'un « point central de contrôle ». Cela implique, entre autres, un registre obligatoire de tous les points d'échange de trafic et des câbles transnationaux. Jusqu'à présent, ceux-ci n'avaient pas été correctement documentés auprès des différentes instances gouvernementales.

Le chapitre aborde la surveillance et la censure à l'œuvre dans l'Internet russe sous l'angle de leur économie politique, ce qui permet d'éclairer leurs logiques et leur fonctionnement inhérents. Dans le cas de la Russie, ces aspects du pouvoir de l'État ont été graduellement réaffirmés, et ce de manière très explicite, dans la période récente. Nous montrons comment les « boîtes noires » imposées aux acteurs privés au niveau de l'infrastructure Internet par le biais de mesures réglementaires sont intégrées dans (et contribuent à) un ensemble de relations sociales, économiques et politiques. Nous déconstruisons ainsi l'image trop simplifiée d'un contrôle direct par l'État via la technologie. Ce faisant, nous cherchons à comprendre un aspect essentiel de la « lutte mondiale pour la gouvernance de l'Internet » [DeNardis, 2014], et comment les infrastructures d'Internet elles-mêmes peuvent être mises à profit pour affirmer des relations de pouvoir.

Ce « tournant vers l'infrastructure » dans la gouvernance de l'Internet [Musiani, Cogburn, DeNardis & Levinson, 2016] présente également une image plus complexe de l'articulation entre la « loi » et le « code » [Lessig, 2006], et entre les régimes politiques et leur traduction en pratiques socio-techniques et économiques. En effet, la relation entre les procédures juridiques et leur mise en œuvre technique constitue une dimension centrale de la gouvernance de l'Internet : le comportement des internautes est régulé par l'inscription de normes, d'*affordances* et de contraintes à la fois dans les infrastructures techniques et dans la loi, et les décideurs les exploitent de plus en plus pour atteindre des objectifs (géo-)politiques (Winseck, 2017). C'est particulièrement vrai en Russie, où la loi et le code interagissent de manière très spécifique : les solutions techniques sont souvent à la traîne par rapport à la réglementation, car la loi cherche à obtenir le contrôle de l'infrastructure (voir par exemple [Ermoshina & Musiani, 2017]). Par ailleurs, cette surenchère régulatrice a donné lieu à des critiques de la part de la communauté des FAI la décrivant comme un « théâtre de la sécurité » [Schneier, 2003], où la rhétorique politique sert avant tout des opportunités commerciales

2 Cet index n'est désormais plus mis à jour par la Société de défense d'Internet (Obŝestvo Zaŝiti Interneta – OZI, ONG russe de défense des libertés numériques).

3 Selon les données d'OZI.

sous-jacentes. Étant donné la règle imposée de « substitution des importations » (le fait de privilégier les entreprises nationales, mis en place bien avant la guerre contre l'Ukraine), les solutions de contrôle de l'information doivent être « fabriquées en Russie ». Dans ce contexte, la réglementation de l'Internet russe produit un marché à part entière de la censure et de la surveillance, façonnant la concurrence entre les différents fournisseurs domestiques de composants d'infrastructure et affectant les opérations et les stratégies des FAI.

L'étude de ces marchés permet d'analyser de près la relation entre normalisation et concurrence : même si la gouvernance de l'Internet russe est de plus en plus présentée comme une question de souveraineté nationale, l'État russe reste lent à produire et à certifier des solutions techniques pour la surveillance et la censure. De plus, le contexte de l'invasion de l'Ukraine par la Russie en 2022, et les sanctions internationales prises en rétorsion, rendent visibles les dépendances de l'industrie russe de surveillance et de censure par rapport aux composants, infrastructures et savoir-faire étrangers. Il en résulte des failles techno-juridiques et des zones grises qui créent à la fois des incertitudes et des opportunités. L'étude du marché des « boîtiers » intermédiaires (ou « *middleboxes* ») permet également de mettre en lumière des pratiques de résistance qui se développent souvent en réponse à des techniques de filtrage et de surveillance spécifiques, et de suivre et comprendre la politisation des professionnels du web.

Nos méthodes ethnographiques examinent en détail les « normes, fils et réglages » [Star, 1999, p. 379] des trois solutions techniques abordées dans ce chapitre. Ces technologies peuvent être considérées comme des « boîtes noires » [Callon, 2013], à plusieurs niveaux : d'abord en raison de leur opacité technique supposée, mais aussi en raison de leurs fonctions de filtrage et de surveillance, qui les placent dans le champ du secret d'État et du secret commercial. Elles ne ressemblent pas toujours à des « boîtiers » physiques clairement identifiables (bien que parfois, ce soit effectivement le cas), mais consistent plutôt en une multitude de solutions logicielles, d'objets techniques distribués et d'ajustements techno-juridiques qui complètent les infrastructures matérielles existantes. En outre, elles sont un lieu clé des controverses liées à la surveillance et à la censure en Russie, générant des ambiguïtés, des interprétations, des litiges, des résistances et des négociations.

Notre étude sur ces activités, qui sont à la fois spécialisées et parfois entourées de secret, a posé plusieurs problèmes. Ceux-ci ont été en partie minimisés en adoptant une approche de « méthodes mixtes », et la collecte de trois principaux types de matériaux au cours de la période 2017-2019, puis en 2022. Tout d'abord, nous avons réalisé quinze entretiens avec des fournisseurs d'accès à Internet (principalement des petites et moyennes entreprises entre 5 000 et 100 000 clients), des experts en informatique, des avocats spécialisés dans l'Internet, des

vendeurs d'équipements de filtrage et de DPI, des militants anti-censure et anti-surveillance, et des ingénieurs travaillant au point d'échange Internet (IXP) de Saint-Pétersbourg. Nous avons ensuite effectué cinq entretiens en été-automne 2022, pour une mise à jour de l'enquête. Les personnes interrogées ont demandé à rester anonymes.

L'étude a été complétée par une web-ethnographie et une analyse des forums et tchats dédiés aux FAI, qui ont été sélectionnés et observés pendant toute la période (voir l'annexe pour plus de détails). Nous avons également effectué une analyse de documentation technique et du matériel de communication produit par les vendeurs de solutions de surveillance et de censure : sites web, présentations commerciales et matériel tiré de conférences professionnelles spécialisées. Enfin, des mesures de l'ampleur de la censure ont été conduites par nos soins en 2018 (en partenariat avec Citizen Lab; [Valentinovich & Ermoshina, 2019]), pour analyser l'application technique de la censure sur le Runet. Une analyse à l'aide de l'outil OONI Explorer[4], ainsi que l'analyse des données de routage BGP et d'autres métriques de trafic ont été conduites plus récemment en 2022, afin d'évaluer les impacts de l'invasion de l'Ukraine par la Russie sur la connectivité du Runet et l'accessibilité des ressources numériques.

SORM et le marché de la surveillance : contraintes et bricolages

SORM est un système d'interception légale des télécommunications. Il s'agit d'un objet distribué composé de commutateurs, de serveurs, de volumes de stockage de données, d'extracteurs, de terminaux de contrôle à distance et de logiciels installés aux frais des opérateurs, mais directement contrôlé par le FSB (Service fédéral de sécurité) et auquel peuvent accéder à la demande d'autres agences et services de police (impôts, douanes, police des frontières, etc.). SORM-1 a été mis en place en 1995 pour les écoutes et la surveillance téléphonique. Depuis, il a évolué vers SORM-2, adapté à l'Internet en 1998, et vers SORM-3 en 2014, qui comprenait des spécifications pour la collecte de métadonnées (telles que l'heure et la date, la localisation, l'expéditeur et les destinataires des messages) et de fichiers multimédias.

La dernière itération a été définie par les lois « Iarovaïa » 374-FZ 4 et 375-FZ adoptées en 2016, soulevant une vague de critiques de la part des organisations de défense des droits et libertés numériques[5]. Après presque deux ans de discussions

4 Open Observatory of Network Interference, projet open source de surveillance de la censure d'Internet à l'échelle mondiale, appuyé sur un réseau de bénévoles (https://explorer.ooni.org/).

5 Voir par exemple la réaction de Electronic Frontier Foundation à la loi Iarovaïa : https://www.eff.org/deeplinks/2016/07/russia-asks-impossible-its-new-surveillance-laws

en raison de la complexité technique de la loi, et en raison d'abondantes critiques venant de la communauté des FAI, la réglementation a été quelque peu assouplie. Selon l'amendement du 12 avril 2018, les fournisseurs de télécommunications doivent désormais stocker les métadonnées pendant trois ans et le contenu de tous les appels vocaux, données, images et messages texte pendant 30 jours (au lieu des 90 jours initiaux), en augmentant la durée de stockage de 15% chaque année. Mais cette obligation d'augmentation de 15% a déjà été reportée deux fois. D'abord en 2020 dans le contexte de la pandémie, ensuite en mars 2022, suite aux sanctions internationales, révélant à la fois la difficulté de mettre en œuvre cette mesure ainsi que l'incapacité du marché russe à proposer des solutions technologiques permettant de répondre, par ses propres moyens, aux demandes des régulateurs[6].

Les données stockées dans le contexte de la loi Iarovaïa doivent être mises à la disposition des autorités sur demande et peuvent être obtenues sans mandat ni ordonnance judiciaire ; en outre, les services en ligne utilisant des données cryptées pour la messagerie, le courrier électronique ou les médias sociaux doivent permettre au FSB d'accéder à ces communications en clair. Le nouveau règlement a suscité de vives critiques, non seulement en raison de l'extension du champ de la surveillance, mais aussi en raison des coûts élevés du stockage des données[7].

Pendant longtemps, pour se conformer à la réglementation les FAI ont opté pour des bricolages à partir de l'équipement existant, comme confirmé lors de la conférence des fournisseurs KROS 8 en mai 2017 par un représentant de NORSI-TRANS, l'un des leaders du marché des solutions SORM :

> « Le stockage de tout le trafic Internet pendant six mois n'est pas compatible avec les réalités économiques de notre pays. La seule solution pratique pour SORM est d'utiliser les équipements existants, avec des extensions minimales et une solution technique claire, sans magouilles[8]. »

De plus, le processus de certification de SORM est long et complexe, impliquant une multitude d'acteurs institutionnels responsables chacun de la certification

6 Le 28 mars 2022, les régulateurs ont apporté encore une modification à la loi, qui autorise à ne pas stocker le trafic des services de streaming et des chaînes de radio et télévision en ligne.

7 Selon les chiffres officiels du gouvernement publiés le 8 décembre 2022, « le coût de l'équipement SORM dépend de la bande passante et de la vitesse de connexion. Par exemple, pour une vitesse de 0-3 Gbit/seconde le coût de l'équipement varie entre 2 et 4,5 millions de roubles, pour 3-6 Gbit/seconde – entre 3 et 6 millions de roubles, pour 6-10 Gbit/seconde – entre 4 et 7.5 millions de roubles. De plus, ces prix incluent les travaux d'implémentation et configuration, stockage de données pendant 3 ans et garantie pour 1 an » (voir https://sozd.duma.gov.ru/bill/254008-8).

8 Chaîne Telegram ZaTelekom, message publié le 25 mai 2017 à 10:04 (https://t.me/zatelecom/192)

d'un ou plusieurs composants du système. Ceux-ci doivent être testés selon une méthodologie qui doit d'abord être validée par le FSB et le ministère des communications. Ensuite, le FSB teste l'installation à l'aide d'un simulateur, et c'est seulement après cela que le processus de certification de trois mois peut commencer. En l'absence de solutions standardisées et certifiées par l'État, les FAI se limitaient à adapter les infrastructures existantes, dans l'anticipation de devoir à nouveau investir de façon substantielle lors de leur publication[9]. Par ailleurs, les responsabilités juridiques pour fuite de données ou mauvaises configurations ne sont pas clairement définies, alors que les erreurs de configuration des boîtiers SORM sont fréquentes, ce qui met en danger les données personnelles des utilisateurs. La situation est particulièrement problématique en raison de la nature sensible des données, des différentes parties impliquées et de l'absence de transparence du processus.

Les exigences sont adaptées à la taille et au budget des FAI. Les grands FAI doivent s'équiper, mais les petits n'installent pas toujours des boîtiers SORM et répondent plutôt aux demandes du FSB de manière ponctuelle : « Quand c'est nécessaire, le FSB nous appelle ou nous contacte par e-mail et nous demande de faire un tcpdump du trafic pour une adresse IP et le partager via ftp[10] ». Une autre stratégie longtemps utilisée s'appelle « outSORMing » et consiste à passer par des opérateurs plus grands qui louent une partie de leurs installations SORM. Cette stratégie a été normalisée en 2022, et est désormais préconisée par les régulateurs de façon officielle[11].

Cependant, la période de flexibilité relative permettant aux FAI d'éviter les installations de SORM s'est terminée en janvier 2022, lorsqu'un nouveau projet de loi 333-34 du Code Fiscal de la Fédération de Russie[12] a été proposé qui introduit des peines plus strictes pour le non-respect des obligations SORM et augmente considérablement le coût d'une licence (en le multipliant par 183 !). L'ensemble des documents qui accompagnent ce projet de loi inclut une étude dévoilant non seulement les chiffres quant au non-respect des obligations SORM, mais qui montre aussi que le régulateur est désormais très informé quant aux ruses et contournements utilisés par les FAI auparavant, et documentés dans notre étude précédente (notamment la fermeture de l'entreprise et sa réouverture avec une nouvelle licence – voir [Ermoshina et al., 2021]).

9 Intervention d'un FAI sur le forum Nag.ru, 4 novembre 2015.

10 Entretien avec Aleks Lomakin, Directeur de l'Association des FAIs Alternatifs, 28 août 2018.

11 Voir sur le site de la Douma : https://sozd.duma.gov.ru/bill/254008-8

12 http://www.consultant.ru/document/cons_doc_LAW_28165/a3cd0bcff028f127a00fa0aa61842f4ff13ffafb/

Année	Nombre de violations	Amende
2020	954	243 amendes (entre 3 et 40 000 roubles, somme totale 4 000 000 roubles)
2021	1096	400 amendes (entre 3 et 100 000 roubles, somme totale de 15 000 000 roubles)
2022 (1re moitié)	404	95 amendes (entre 3 et 100 000 roubles, somme totale 3 000 000 roubles)

Tableau 1. Nombre de violations et d'amendes par année dans la période 2020-2022. Source https://sozd.duma.gov.ru/bill/254008-8

Pratiques et technologies de censure

S'agissant de la censure, les lois introduisant le blocage des contenus web existent depuis 2012, date à laquelle une liste noire des pages web prohibées par RKN a été introduite, ainsi que la cooptation des FAI sous juridiction russe pour mettre en œuvre le blocage [Sivetc, 2020]. La réglementation a été mise en place dans le sillage des manifestations de 2011-2012 contre les irrégularités électorales, qui ont entraîné un remaniement du paysage médiatique numérique [Denisova, 2017], mais ses pleines implications sont apparues lors de la guerre en Ukraine de 2014, qui est devenue un banc d'essai pour le renforcement du contrôle de l'information par les autorités russes, y compris sur les territoires annexés.

Cependant, nos entretiens montrent que dès 2008-2009, les FAI ont reçu des demandes de blocage d'accès ad hoc à des sites web spécifiques (jeux d'argent, pornographie, vente de drogue). L'introduction d'une liste noire centralisée a rendu plus difficile pour les FAI d'ignorer les demandes et de se défendre devant les tribunaux. Cependant, les exigences précises quant aux méthodes de blocage n'ont été publiées qu'en mars 2018 avec la loi 149-FZ, article 10, qui définit les paramètres techniques des «pages de blocage» standardisées et un ensemble détaillé de recommandations techniques pour le filtrage des contenus.

Le principe de «liste noire» a été sévèrement critiqué par les défenseurs de la liberté d'expression, car les catégories de contenu «illégal» ont été vaguement définies, ce qui a conduit à des décisions arbitraires. En outre, l'absence de contrôle judiciaire facilite la mise sur liste noire de sites web d'opposition pour des motifs politiques. Ces mesures ont initialement déclenché une série d'initiatives qui ont exploité le

mécanisme du système de noms de domaine en tant qu'outil de contestation, comme en témoigne la controverse autour de la bibliothèque en ligne de Maksim Moshkow, bloquée en 2012. Moshkow, un pionnier de l'Internet russe, avait été le fer de lance de grands projets Internet médiatiques (par exemple Gazeta.ru) ; Lib.ru, également connu sous le nom de Bibliothèque de Maksim Moshkow, a commencé à fonctionner en novembre 1994 et est devenu la plus grande et la plus complète bibliothèque électronique en langue russe.

La réponse de Moshkow au blocage de sa bibliothèque a été d'exploiter une vulnérabilité du mécanisme de censure du web pour bloquer le site principal du ministère de la Justice lui-même. Étant donné que de nombreux FAI bloquaient automatiquement toutes les adresses IP du « A-Record »[13] d'un DNS sur liste noire, Moshkow a simplement modifié le A-record de son site web en ajoutant l'adresse IP du ministère de la Justice[14]. Suivant le même principe, en 2017, un certain nombre de « guérillas » basées sur les DNS ont eu lieu, conduisant aux blocages des sites de banques et services du gouvernement et de plusieurs serveurs racine DNS. Les activistes ont utilisé la liste noire de RKN comme point de départ : ils ont acheté quelques noms de domaine « orphelins » dont l'abonnement avait expiré mais qui figuraient toujours dans la liste, et ont procédé à la modification de leurs A-Records respectifs. En exploitant la même vulnérabilité, le 6 mai 2018, le développeur et hacker Leonid Evdokimov a écrit « Digital Resistance » en morse sur les graphiques des FAI bloqués (figure 1).

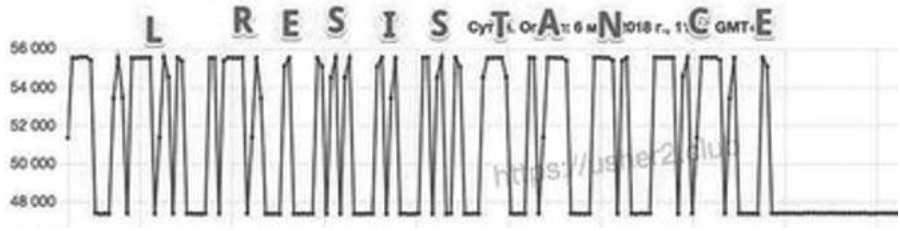


Figure 1. Le message en code Morse de L. Evdokimov.
Source : site de Phil Kouline, hébergeur indépendant, expert et militant pour le RuNet libre (https://usher2.club/articles/msg-digitalresistance/)[15].

13 Le A-Record permet d'associer une ou des adresse(s) IP à un nom de domaine.

14 https://tjournal.ru/46700-moshkov-minjust.

15 Ce site a longtemps maintenu le registre des adresses IP bloquées, sous forme de graphique. Devenu source privilégiée de données pour les médias et les régulateurs, il a été consulté fréquemment, y compris par les agents de Roskomnadzor. D'où le choix de Leonid Evdokimov de visualiser son message sur ce graphique.

Ces actions ont eu des conséquences sur la réglementation et la mise en œuvre de la censure, ainsi que sur la manière dont les listes de blocage sont maintenues. Avant l'action de Evdokimov, en avril 2018, la liste noire comptait 5 136 noms de domaine orphelins qui auraient pu être utilisés pour reproduire une attaque DNS, alors que le 13 mai 2018, elle ne comptait déjà plus que 204 noms de domaine de ce type. Cet effet secondaire a été critiqué par certains de nos répondants, selon qui les activistes ont finalement aidé RKN à améliorer sa gestion de la censure sur Internet.

Malgré la critique de la censure par les acteurs de la société civile et par certains FAI eux-mêmes, les opérateurs russes doivent cependant mettre en œuvre ces mesures réglementaires, qui affectent leur activité et, dans une certaine mesure, remettent en question les valeurs d'ouverture qu'ils pourraient défendre. À l'instar de SORM, les solutions pour le blocage des sites sont des objets hybrides et peuvent prendre différentes formes : des scripts « faits maison » par les FAI, des solutions hardware, des solutions basées sur le cloud ou des logiciels de type DPI. Pendant longtemps, les FAI avaient le choix entre différentes options et méthodes de blocage. Le directeur de SkyDNS, un fournisseur proposant des solutions de filtrage du trafic, souligne :

> « Il y avait une sorte de vide technologique – bloquez comme vous voulez. RKN ne pouvait pas conseiller les FAI en terme de solutions, de peur de tomber sous le coup des lois antitrust. Mais très vite, il y a eu plusieurs plaintes d'administrateurs de sites Web bloqués par erreur… Ils ont donc commencé à imposer le blocage par URL. Les FAI avaient l'habitude d'écrire leurs scripts par eux-mêmes, mais ce n'est plus très fréquent, car ils risquent d'être pénalisés »[16].

Le blocage manuel est devenu trop difficile à mesure que la liste noire s'allongeait. De plus, cette liste de blocage a souvent été critiquée par les FAI en raison de ses multiples inexactitudes et de sa structure désordonnée qui entraîne des erreurs. Une enquête informelle sur un forum de FAI[17] montre que les méthodes les plus utilisées sont le blocage d'IP et le DPI.

Certains FAI ont cherché à éviter des investissements importants dans les solutions de filtrage, avec pour conséquence un blocage qui n'était pas appliqué de façon homogène entre les différents réseaux. En décembre 2016, afin de mieux contrôler l'application uniforme de la liste noire, RKN a introduit une autre solution

16 Entretien du 22 novembre 2018.

17 https://forum.nag.ru/index.php? /topic/79886-blokirovka-saytov-provayderami/.

technique : le système automatique Revizor (*AS Revizor*)[18]. Avec l'ajout de Revizor et en raison de ses nombreux dysfonctionnements, l'attribution des responsabilités pour les erreurs de blocage est souvent controversée et génératrice de problèmes. Mikhail Klimarev, président de la Société pour la défense d'Internet (OZI), explique :

> « Supposons que je sois un petit fournisseur d'accès à Internet et que j'achète le trafic pré-filtré de Rostelecom. J'installe Revizor, mais quelque chose n'est pas bloqué. Qui paie l'amende ? Rostelecom ou moi ? Rostelecom dira que j'ai mal configuré l'équipement au niveau local… »[19]

Dans ce contexte d'incertitude juridique et d'absence de spécifications, un marché de solutions de blocage de sites web s'est développé. Contrairement aux fabricants de SORM, la majorité des fabricants d'équipements de filtrage (par exemple SkyDNS, Ruspromsoft ou CarbonSoft) proposaient auparavant des solutions de facturation ou de contrôle parental. Mais certaines entreprises (par exemple, CyberFilter) ont été créées spécifiquement pour répondre aux exigences de RKN.

Les entretiens avec les FAI et l'analyse des forums ont permis d'identifier au moins quatorze solutions de filtrage différentes. Pendant longtemps, une confusion a persisté parmi les FAI au moment de choisir un fournisseur particulier, les leaders du marché étant Carbon Reductor et SKAT. Cependant, dans le but de stabiliser et de standardiser les procédures de blocage, et soi-disant en raison des demandes des FAI, RKN a procédé à un essai massif de treize solutions (août 2017-mars 2018), en les comparant en fonction d'un certain nombre de paramètres, dont par exemple la proportion de contenus « extrémistes » et « autres contenus » non bloqués. RKN a ensuite établi un classement dont les résultats ont été publiés sur son site web[20].

Dans l'ensemble, différentes tendances et stratégies peuvent être identifiées sur le marché russe de la censure pour faire face aux exigences des régulateurs. Les fournisseurs de solutions de filtrage se livrent une concurrence féroce pour en proposer de moins chères ou de plus efficaces, tandis que les grands FAI évitent parfois de tout bloquer pour attirer davantage de clients. La non-conformité se présente ainsi comme un argument commercial : les fabricants intègrent des fonctionnalités permettant d'éviter à la fois les amendes pour non-blocage et

18 Selon une enquête menée par ValdikSS, un hacker et militant associé à Roskomsvoboda qui a conduit une analysé détaillée du boîtier AS Revizor, l'appel d'offres pour son développement aurait été remporté par MFI-Soft, une société également impliquée dans la production de systèmes SORM. Les coûts de production de Revizor ont été estimés à 84 millions de roubles (près de 1,14 million d'euros), mais l'État fournit les appareils aux FAI (voir https://habr.com/ru/post/282087/).

19 Entretien avec Mikhail Klimarev, directeur de OZI, 14 septembre 2018.

20 https://rkn.gov.ru/communication/p922/

de minimiser les impacts de la censure sur la qualité du service. Par exemple, lors du blocage de Telegram en 2018, un des effets secondaires a été de bloquer également les serveurs d'Amazon, de Google et d'autres sites web populaires. Carbon Reductor a ensuite proposé aux FAI un pack qui garantissait la capacité de fournir à leurs clients un accès aux plateformes telles que YouTube ou Gmail sans être détectés par Revizor et condamnés à une amende par RKN.

De manière générale, entre 2012 et fin 2018, la censure en Russie n'était pas homogène, et les FAI ont développé des moyens pour éviter de s'y conformer, à la fois pour des raisons économiques, mais aussi techniques. En effet, les entretiens et l'analyse des forums montrent que les FAIs partagent une forme d'attention à leurs réseaux et méprisent les interventions extérieures dans leurs installations, notamment imposées par les régulateurs, qu'ils considèrent par ailleurs comme incompétents. Ils ont ainsi développé de nombreuses stratégies de contournement et de « ruses sur les réseaux », qui ont été explorées plus en détail ailleurs (Ermoshina et Musiani, 2021). Parmi celles-ci, on peut évoquer la pratique de censure sélective, appliquée pour essayer de tromper Revizor. Selon le directeur de SkyDNS :

> « Certains opérateurs n'appliquent la censure que sur un sous-réseau distinct qu'ils appellent "bac à sable", où ils installent Revizor. Et pour leurs utilisateurs finaux, ils façonnent un autre réseau où il n'y a pas ou peu de censure. De leur côté, les administrateurs de réseau ou les services d'hébergement se livrent à des ruses techniques ; par exemple, lorsque des adresses IP de Revizor sont identifiées, une page de blocage est envoyée en réponse ».

D'autres stratégies impliquent une résistance juridique. L'organisation OrderCom apporte son soutien aux FAI qui s'opposent aux décisions et amendes mandatées par RKN, avec un certain succès : en 2016, 15 % des décisions ont été annulées. Les FAI contestent également ce qu'ils considèrent comme des erreurs dérivées de l'utilisation de Revizor, en fournissant des copies conformes certifiées des pages bloquées. Cependant, sur les 33 533 décisions de justice entre 2012 et 2017, seuls 46 cas ont été contestés avec succès[21].

Les « TSPU » et la centralisation du contrôle

Après une période de « semi-liberté » pour les FAI et les utilisateurs du Runet, un nouveau dispositif juridique et technique a été introduit en 2019, avec la loi sur la « Stabilité du Runet » (connue du grand public comme la loi sur la « Souveraineté du Runet »). Cette loi a initialement été reçue avec beaucoup de scepticisme par les

21 Voir l'étude menée par Serguey Hovyadinov, spécialiste du droit et des politiques numériques : https://rankingdigitalrights.org/2018/07/19/russia-telcos-fail-to-respect-users-rights/

FAI et les acteurs de la société civile, qui doutaient de la capacité technologique du gouvernement de pouvoir la mettre en place de façon efficace. Son caractère opaque et complexe a également rendu les interprétations délicates. En effet, cette « loi » contient elle-même autour de 30 actes réglementaires qui définissent les « menaces à la stabilité de l'Internet » ou attribuent de nouvelles responsabilités à Roskomnadzor. Par exemple, le contrôle des points d'échange de trafic (IXP), ou l'établissement d'une liste exhaustive des câbles transfrontaliers (qui n'était toujours pas réalisée à la fin de l'année 2022).

L'analyse de la presse et des chaînes Telegram spécialisées montre que les experts engagés dans la lutte « pour le Runet libre » percevaient cette loi comme un « rêve des régulateurs », et voyaient un décalage entre la réalité technologique et l'imaginaire législatif : « Le régulateur voit la régulation du Net comme une sorte de point central de contrôle, un grand écran dans un bunker et beaucoup de gens avec des casques audio. Il croit vraiment que ça ressemble à ça. On dirait un démiurge qui dessine ses rêves d'enfant »[22]. D'autres experts ont fait le lien entre la loi « Sur la souveraineté » et les tentatives inefficaces de bloquer Telegram, ou la loi Iarovaïa de 2016, qui a été modifiée et largement allégée par manque de moyens techniques nécessaires pour sa réalisation. En effet, le principe de souveraineté « par les infrastructures » qui préconisait que tout instrument de contrôle d'information devait être « *made in Russia* » a joué un mauvais tour à son promoteur, car la Russie n'avait pas de solutions technologiques capables de respecter ses propres injonctions.

Cependant, malgré une réception critique et sceptique de la loi de 2019, celle-ci a véritablement bouleversé les façons de contrôler le Runet, à plusieurs niveaux. Tout d'abord, la zone de contrôle des infrastructures de communication par RKN a été élargie de façon radicale. Notamment, l'obligation de fournir des informations sur les clients (comprenant le volume de trafic, les numéros de systèmes autonomes, les coordonnées des propriétaires, etc.) a été élargie jusqu'aux IXP, alors qu'en novembre 2019 (lors de notre entretien avec un représentant de Piter IX, l'IXP de Saint-Pétersbourg) les points d'échange étaient encore exclus de ces dispositions. Depuis 2020, RKN a commencé à répertorier les opérateurs qui possèdent une infrastructure transfrontalière.

Comme nous l'avons montré plus tôt dans ce chapitre, une quinzaine de fabricants proposaient des solutions pour la censure et le filtrage du trafic (dont 7 ont été testées et certifiées par RKN). Les FAI avaient la possibilité de contourner les obligations car ils étaient chargés de choisir, implémenter et maintenir les solutions techniques de filtrage et de surveillance. De nombreuses ruses et bricolages

22 Entretien avec Phil Kouline sur le site *Fontanka*, 30 mai 2019 (https://www.fontanka.ru/2019/05/30/058/).

techno-juridiques leur permettaient de minimiser le contrôle sur les réseaux et ainsi de défendre une certaine vision du Runet « libre ». Les mesures de trafic réalisées entre février et avril 2018 à l'aide du logiciel OONI Probe (développé par le *Open Observatory of Network Interference*) confirmaient cette liberté relative des FAIs. Avec plus de 200 000 mesures menées à l'aide de testeurs locaux, nous avons pu constater une incohérence dans les blocages des sites web de la « liste noire » officielle de RKN [Valentinovich et Ermoshina, 2019].

Or, la loi de 2019 préconise d'installer une solution unique appelée « TSPU » (« moyens techniques de lutte contre les menaces ») qui combine une partie logicielle de type DPI et une partie hardware. Alors que les solutions DPI sont fabriquées en Russie (surtout par RDP.ru, propriété de Rostelecom, ou par Carbon Soft), la partie hardware du TSPU n'est pas entièrement russe. Les solutions couramment utilisées sont produites par Intel, Huawei ou Supermicro, les cartes réseau fabriquées par Mellanox ou Intel. Le « TSPU » n'est pas un boîtier unique. C'est un assemblage d'appareils et de solutions logicielles, préconisés par RKN. Un exemple d'assemblage TSPU peut ainsi comporter : un filtre EcoDPI fabriqué par RDP, un serveur Huawei, un commutateur Eltex, un interrupteur Silicom, un module optique Fiber Trade, un logiciel de chiffrement « Kontinent ». L'assemblage n'est à ce jour pas certifié.

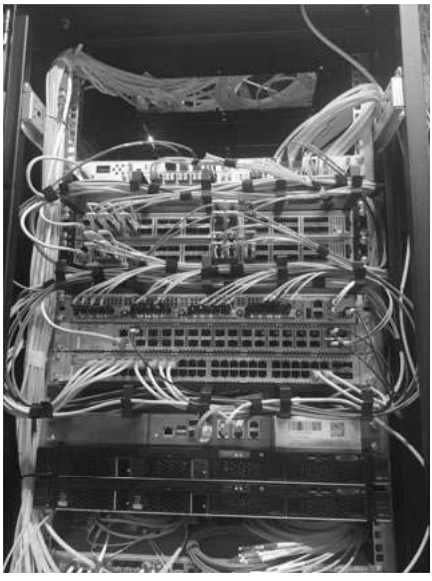


Figure 2. Installation TSPU pour 40Gb/sec.
Source : OrderCom

Les TSPU sont installés par des agents habilités par le FSB et par RKN et se trouvent normalement dans des cages fermées à clé, les FAI ont donc un accès limité à ces installations. Leur achat et mise en place sont pris en charge par l'État, mais la maintenance reste aux frais du FAI. Notamment, la loi prévoit une amende pour les infractions aux règles d'installation, d'exploitation et de modernisation des TSPU qui peut monter jusqu'à 500 000 roubles (à peu près 6 400 euros). En cas de panne, c'est le FAI qui est sanctionné – même si la panne est due à une intervention de RKN. La marge de manœuvre des FAI est alors limitée, et la possibilité de ne pas filtrer le trafic est réduite.

Les TSPU permettent de ralentir certains services, comme Twitter en 2021, ainsi que de bloquer certains VPNs (ExpressVPN, RedShield, NordVPN, etc). En automne 2021, TSPU a été utilisé pour des blocages massifs extra-judiciaires, notamment le site du service de vente en ligne Avito.ru, les serveurs du jeu World of Tanks, GoogleDocs, Apple Music, Recaptcha, Telegra.ph, etc. Ces services ont été bloqués par TSPU lors des élections législatives afin d'arrêter la distribution de l'application SmartVote d'Alekseï Navalny qui appelait à voter pour les candidats d'opposition. Ces services n'ont pas été inscrits au registre des sites bloqués, et ont donc été bloqués sans décision de justice. De plus, l'introduction du TSPU a affecté la transparence de la censure. Alors que la liste noire permet une traçabilité et une certaine veille citoyenne de l'application de la censure (notamment par l'ONG Roskomsvoboda), il n'existe pas à ce jour de liste des sites bloqués par TSPU[23].

Pour les petits fournisseurs dont la vitesse ne dépasse pas 10 Gbit/seconde, l'installation des TSPU n'est pas obligatoire, selon le directeur du Centre Principal des Fréquences Radio Serguey Tyomniy[24]. Or, le marché russe des FAI est caractérisé par un grand nombre de petits fournisseurs avec une bande passante relativement faible, mais dont le trafic cumulé ne constitue que 5% de tout le trafic du pays[25]. Le filtrage doit alors se faire à un niveau au-dessus, par les opérateurs «*upstream*». Cependant, même certains grands opérateurs comme MTS considèrent que le TSPU est une «menace pour la connectivité, la stabilité et le bon fonctionnement du Runet»[26].

23 https://roskomsvoboda.org/cards/card/tspu-blokrovki-Runet/

24 Voir la vidéo de la présentation de Sergej Tëmnij lors de la conférence des opérateurs MUSE le 22 septembre 2022 https://t.me/ordercomru/3588

25 Selon l'agence de presse Interfax, le 15 juin 2021 (https://www.interfax.ru/russia/772325)

26 *Kommersant*, 29 juillet 2021 https://www.kommersant.ru/doc/4919761? query=%D0%B4%D0%BC%D0%B8%D1%82%D1%80%D0%B8%D0%B9%20%D0%B3%D0%B0%D0%BB%D1%83%D1%88%D0%BA%D0%BE

De nouvelles ruses se développent ainsi chez les FAI, notamment au niveau juridique. Lors de la campagne de recensement forcé des FAI conduite par RKN en décembre 2021, l'avocat spécialisé en défense des FAI Dmitriy Galoushko avait conseillé sur sa chaîne Telegram de déclarer la bande passante à moins de 10 Gbit/seconde[27]. Quant à la résistance technologique, elle se déplace dernièrement au niveau du développement des protocoles d'obfuscation de trafic (Shadowsocks, OBFS4, Cloak) et de nouvelles générations de VPN « multi-protocoles » qui masquent le trafic (AmnesiaVPN ou CensorTracker par Roskomsvoboda).

Une autre solution de contournement proposée par les FAI consiste à créer des « coopératives de consommateurs de l'Internet » pour éviter la nécessité d'installer TSPU et SORM[28]. Cela confirme les intentions des FAI, déjà mises au jour lors des entretiens conduits en 2019 avec des représentants de plusieurs petits FAI de Saint-Pétersbourg, qui avaient fait part de leurs stratégies en cas d'activation réelle du « Tcheburnet » (mot utilisé par les défenseurs du RuNet libre pour décrire le projet du RuNet souverain, de « *tcheburashka* », personnage d'un dessin animé soviétique, animal mythique qui n'existait nulle part ailleurs, et « net » pour « Internet ») :

> « On va revenir aux réseaux locaux, mais aussi peut-être expérimenter avec des bricolages administratifs comme les coopératives, associations ou clubs des amateurs de l'Internet, pour partager la connectivité avec des cercles très réduits de proches, amis ou clients fidèles. Mais j'imagine que, en général, si leur plan du Runet souverain marche vraiment, seulement une minorité pourra se permettre d'avoir accès à l'Internet global, une minorité qui a des compétences techniques et l'équipement nécessaire. »[29]

Les effets de l'invasion de l'Ukraine par la Russie sur les infrastructures de contrôle de l'information

L'invasion de l'Ukraine par la Russie en février 2022 a conduit à une intensification des mesures dites de « lutte contre les menaces » extérieures (selon la loi de 2019 : menace à la stabilité, menace à la connectivité, menace à la sécurité). L'analyse de la presse et des chaînes Telegram spécialisées révèle la montée des discours alarmistes quant à la possible déconnexion du Runet, mais aussi le durcissement des contrôles sur celui-ci et l'accélération du projet de Runet « autonome ». Ainsi, des inspections ont été menées dans les bureaux des FAI entre février et août 2022. Le 8 juin 2022, un projet de modification de la loi 333 part 2 du

27 https://t.me/ordercomru/2794

28 Voir les discussions sur le forum Nag.ru : https://forum.nag.ru/index.php? /topic/146324-uslugi-svyazi-bez-sorm-revizor-i-tp/page/3/#comment-1599314

29 Entretien avec D., réalisé le 14 novembre 2019.

Code Fiscal a été proposé, introduisant des amendes pour l'absence d'installation SORM ; le montant de l'amende dépend du profit annuel du FAI mais dans tous les cas doit être égal ou supérieur à 1 million de roubles (à peu près 12 800 euros).

Des essais ont été conduits en août 2022 afin de vérifier la capacité des FAI russes à répondre aux attaques sur le routage effectué via le BGP (Border Gateway Protocol). D'autres essais ont eu lieu en 2022 pour tester les serveurs DNS localisés à l'intérieur du pays. Plusieurs satellites de type nouveau (Gonets M et Skif D) ont été récemment lancés pour assurer une possibilité de connectivité satellitaire et de défense des fréquences hertziennes. Une autre mesure pour la réalisation du plan de l'autonomie technologique et de souveraineté numérique du Runet consiste à développer des autorités de certification[30] propres à la Russie. Cela a été annoncé en septembre 2022, mais le 22 novembre 2022, Sberbank, la caisse d'épargne russe, a acheté un certificat chez l'autorité de certification grecque Harica[31], ce qui montre que, malgré le discours sur la souveraineté et malgré les sanctions, la banque centrale russe continue à utiliser les certificats européens. Cependant, la transition vers les certificats « *made in Russia* » n'est pas synchronisée entre les services administratifs. Ainsi, fin octobre 2022, les services comme Nalog.ru[32] (impôts), Gosuslugi[33] ou Revizor utilisaient encore des certificats délivrés par Let's Encrypt, une autorité de certification californienne.

Le projet du Runet souverain s'avère ainsi être lui-même dépendant de solutions étrangères (notamment américaines ou chinoises, même pour les outils comme Revizor). Alors que ses points de jonction et de dépendance infrastructurelle deviennent de moins en moins nombreux, ils restent fondamentaux. Paradoxalement, le contexte de sanctions internationales met en question la réalisation du projet du Runet souverain. Nos analyses de la documentation technique pour les solutions de communications dites « spéciales » (à destination de l'armée russe) développées par Protei ST (fabricant russe de DPI, SORM et autres solutions logicielles et d'appareils de filtrage, surveillance, facturation ou téléconférence), montrent une dépendance aux processeurs Intel (qui ne peuvent désormais plus être exportés vers la Russie).

30 Un certificat SSL est un certificat numérique que l'on associe à un nom de domaine ou une URL. Il permet d'établir avec certitude le lien entre le site Internet et son propriétaire et permet ainsi de sécuriser les échanges électroniques. Les certificats sont délivrés par des Autorités de Certification qui ont leur système de réputation et notoriété, en fonction de leur ancienneté et les accords avec les OS et navigateurs les plus populaires. Dans le cadre du passage vers le Runet souverain, le développement des Autorités de Certification russes constituerait une décision infrastructurelle importante.

31 Source : https://crt.sh/? id=8043006484

32 https://t.me/zatelecom/24122

33 *Ibid.*

Les sanctions ont même affecté des collaborations de long terme et qui semblaient durables, notamment avec les fabricants taiwanais, qui ont été impliqués dans la production des processeurs « Baikal » – par ailleurs présentés comme « *made in Russia* ». Cependant, malgré les sanctions internationales sur les composants électroniques de « *dual-use* » (qui peuvent être utilisés à des fins militaires), des schémas d'importation dits « parallèles » ont été mis en place à plusieurs niveaux. Individuellement, à l'initiative des FAI qui continuent à se procurer des solutions Cisco, Juniper ou Mikrotik, notamment sur eBay et via le Kazakhstan ; mais aussi, plus systématiquement et sans discrétion, par les fabricants SORM, comme annoncé publiquement lors de la conférence KROS 2022. L'importation parallèle impacte à son tour les coûts des solutions SORM qui ont grimpé de 20%, et les délais de fabrication qui sont montés à 3-4 semaines[34].

L'obligation d'implémenter SORM et des solutions de filtrage a été élargie jusqu'aux territoires occupés d'Ukraine (notamment, Zaporizhe, les régions occupées de Lougansk et Donetsk) mais avec une mise en œuvre réelle à partir de 2026 (selon les lois 5, 6, 7, 8 FZ, qui prescrivent une « période de transition »). Cependant, malgré l'absence d'un cadre légal et d'une procédure technologique standardisée, en novembre 2022, les FAI des régions occupées de l'Ukraine ont reçu un ordre des « Ministères de la communication » locaux, qui demandent aux FAI de bloquer, ralentir ou « partiellement dégrader » les services suivants : Google, YouTube, Zoom, Facebook, Twitter, Viber, Instagram, et d'envoyer des rapports avec des preuves à RKN. Une instruction a été transmise qui explique comment mettre en place ces blocages, et comment vérifier leur efficacité. En cas de refus de bloquer ou ralentir les services, la licence peut être retirée.

Les fabricants russes de boîtiers SORM et DPI explorent de nouveaux marchés notamment orientés vers les régions de l'Asie Centrale et de l'Afrique : Ouzbekistan, Tadjikistan, Kazakhstan, Kyrgyzstan, Iran, Afghanistan (où les solutions de Vas Expert et Protei sont vendues et installées). La Russie exporte donc sa vision de la souveraineté par les infrastructures, alors même que les militants anti-guerre, les journalistes et les développeurs s'exilent dans ces mêmes régions. Mais la fuite des experts techniques est également un facteur qui impacte les marchés SORM et DPI.

Le marché des FAI vit une centralisation rapide, comme nous l'avons montré précédemment. Cette centralisation s'opère en premier lieu au niveau des infrastructures, avec des schémas de « *outsorming* » ou « *upstream filtering* » qui conduisent à une dépendance des petits FAI par rapport aux plus grands, chez qui ils louent une partie des infrastructures ou achètent le trafic en transit. Elle

34 Source : intervention des fabricants SORM à la conférence KROS 2022. https://youtu.be/nZmbsYTfCNM

s'opère également au niveau juridique, comme le montre la chute du nombre de licences distribuées. Les coûts d'entrée sur le marché s'élèvent désormais à 1,5 millions de roubles, pour des licences qui incluent SORM.

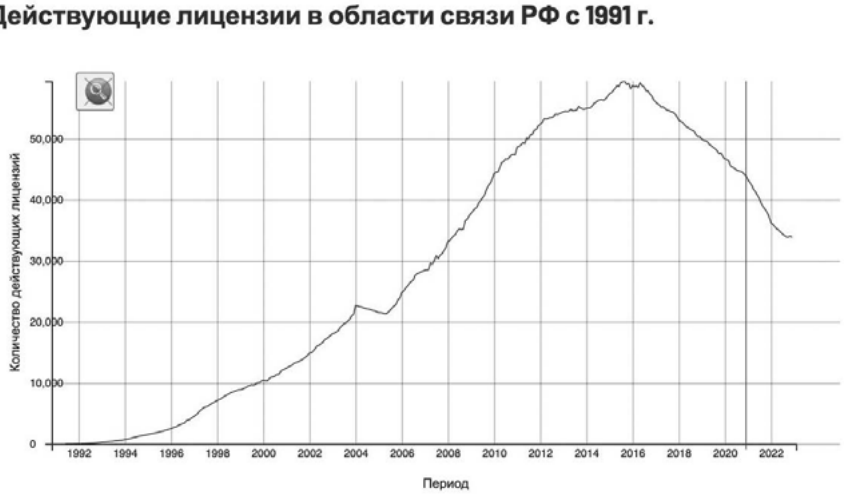


Figure 3. Licences actives délivrées dans le domaine des télécommunications.
Source: https://ifreedomlab.net/connectivity-rating/licenses-russia/

Conclusion

Un florissant marché de la censure et de la surveillance s'est ouvert ces dernières années aux fournisseurs russes de solutions matérielles et logicielles pour le blocage et le filtrage du trafic. Ce chapitre décrit plusieurs technologies controversées qui sont au cœur de ce marché, en montrant l'écosystème d'acteurs et de processus socio-techniques qui les entourent. Il montre également à quel point le développement de ce marché est central dans la mise en place de la stratégie coercitive, autoritaire et centralisatrice qui est à la base de la conception de la souveraineté numérique de l'État russe.

Une étude précédente de ce marché des technologies de surveillance et de censure, qui a porté sur la période 2012-2019 [Ermoshina et al., 2022], a pu démontrer le caractère distribué, voire parfois incohérent, du modèle russe de contrôle de l'information, qui préservait la possibilité d'une certaine liberté de manœuvre pour les FAI. Les évolutions récentes, concernant notamment les TSPU, invitent à en nuancer les conclusions.

Cependant, malgré le réajustement juridique et technique important qui a suivi l'introduction des TSPU, le contrôle des réseaux russes reste relatif. Comme l'a annoncé le directeur de RKN Andrei Lipov, alors que 100 % des opérateurs mobiles ont installé les TSPU, seulement 60 % de fournisseurs d'accès pour Internet fixe en sont équipés. Le directeur du Centre d'Observation des Réseaux de Communication Serguey Khutortsev a évoqué 860 « nœuds TSPU » en 2022 et en a promis 1360 en 2023[35]. Cependant un sondage des FAI, le 22 décembre 2021, montrait que parmi les répondants, seulement 19 % avaient installé TSPU, 3 % avaient signé le plan d'implémentation, 48 % pas encore, 14 % n'allaient pas le faire et 21 % manifestaient leur intention d'« opter pour une stratégie "grise" »[36].

Comme l'ont montré cet exemple et de nombreux autres tout au long du chapitre, l'étude de ce marché continue donc d'être une illustration valable de la diversité des contraintes exercées sur l'Internet russe, elle-même essentielle pour comprendre les multiples formes de résistance, d'évasion et de contournement qui se sont développées en réaction à celles-ci. Dans cet écosystème, la rationalité économique est strictement liée à l'interprétation des normes techno-juridiques, et à la capacité des acteurs à négocier ou à s'opposer à ces normes. Ce chapitre montre de nombreux exemples de stratégies et de compromis qui jettent un nouvel éclairage sur la fabrique de l'autoritarisme et de la résistance numérique en Russie aujourd'hui.

Références bibliographiques

[Callon, 2013] Callon, Michel, « Qu'est-ce qu'un agencement marchand ? », in Callon, Michel et al. (dir.), *Sociologie des agencements marchands. Textes choisis,* Paris, Presses des Mines, p. 325-440.

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

[Ermoshina et al., 2021] Ermoshina, Ksenia, Loveluck, Benjamin & Musiani, Francesca, « A market of black boxes: The political economy of Internet surveillance and censorship in Russia », *Journal of Information Technology & Politics*, vol. 19, n° 1, p. 18-33.

[Ermoshina & Musiani, 2021] Ermoshina, Ksenia & Musiani, Francesca, « Ruser sur les réseaux : résistances 'par l'infrastructure' des fournisseurs d'accès Internet en Russie », *Quaderni*, n° 103, p. 53-70.

35 Voir la vidéo de la présentation de Serguey Khutortsev lors de la conférence spécialisée en cybersécurité « Spektr-Forum 2022 » (https://t.me/ordercomru/3811).

36 Chaîne Telegram de OrderCom, entreprise juridique spécialisée en défense des intérêts des FAI face aux poursuites administratives par le RKN https://t.me/ordercomru/2822

[Ermoshina & Musiani, 2017] Ermoshina, Ksenia & Musiani, Francesca, « Migrating servers, elusive users: reconfigurations of the Russian Internet in the post-Snowden era », *Media and Communication*, vol. 5, n° 1, p. 42-53.

[Lessig, 2006] Lessig, Lawrence, *Code. Version 2.0*, New York, NY, Basic Books.

[Musiani et al., 2016] Musiani, Francesca, Cogburn, Derrick L., DeNardis, Laura & Levinson, Nanette S. (dir.), *The Turn to Infrastructure in Internet Governance*, Basingstoke, Palgrave Macmillan.

[Schneier, 2003] Schneier, Bruce, *Beyond Fear. Thinking Sensibly About Security in an Uncertain World*, New York, Copernicus Books.

[Sivetc, 2020] Sivetc, Liudmila, « The blacklisting mechanism: new-school regulation of online expression and its technological challenges », in Wijermars, Mariëlle & Lehtisaari, Katja (dir.), *Freedom of Expression in Russia's New Mediasphere,* Abingdon, Routledge, p. 39-56.

[Star, 1999] Star, Susan Leigh, « The ethnography of infrastructure », *American Behavioral Scientist*, vol. 43, n° 3, p. 377-391.

[Valentinovich & Ermoshina, 2019] Valentinovich, Igor & Ermoshina, Ksenia, « Measuring Internet censorship in disputed areas: an examination of online media filtering in Russia and Crimea during the 2018 presidential elections », report, Open Technology Foundation, https://www.opentech.fund/news/exploring-online-media-filtering-during-2018-russian-presidential-elections/

[Winseck, 2017] Winseck, Dwayne, « The geopolitical economy of the Internet infrastructure », *Journal of Information Policy* vol. 7, p. 228-267.

Chapitre 3

Discipliner l'espace public numérique : l'agrégateur de nouvelles Yandex.News

Françoise Daucé et Benjamin Loveluck

Depuis l'agression militaire de la Russie contre l'Ukraine en février 2022, surveillance et propagande sont au cœur d'une guerre qui touche aussi le contrôle de l'opinion publique. Dans ce contexte, les flux d'information, déjà étroitement contrôlés par une législation, des institutions et des dispositifs techniques répressifs avant le déclenchement de la guerre (voir chapitres 1 et 2) se resserrent. Les grandes entreprises du numérique, qui participent à la diffusion des contenus en ligne (médias, réseaux sociaux, plateformes de blogs mais aussi agrégateurs de nouvelles) sont particulièrement surveillées. C'est le cas de la société Yandex, fleuron de l'industrie numérique russe, dont le moteur de recherche et l'agrégateur de nouvelles suscitent, depuis le début des années 2010, l'attention croissante des dirigeants russes. Yandex.Novosti – « Yandex.News », l'équivalent russe de Google News, lancé en 2004[1] – fait l'objet d'un encadrement de son service d'information au fil de controverses, de contraintes juridiques mais aussi de limitations techniques qui, progressivement, le privent de toute autonomie. Suite au déclenchement de la guerre, ce processus d'emprise politique s'achève par le transfert de Yandex.News à la plateforme VKontakte (l'équivalent russe de Facebook), elle-même propriété du groupe Gazprom-Media, placé sous la tutelle directe de l'administration présidentielle de V. Poutine. La vente du service à VK vient conclure la dynamique d'encadrement de l'agrégateur engagée au début des années 2010.

La Russie fait partie des rares pays au monde où Google n'a jamais véritablement dominé le secteur de la recherche en ligne. Yandex (contraction de Yet Another iNDEX) est le nom donné par Arkady Voloj et Ilya Segalovitch aux technologies de recherche plein texte en langue russe qu'ils ont développées chez Comptek International. Le moteur de recherche Yandex.ru a été lancé en 1997 – à peu près en même temps que Google, mais dans un contexte économique très différent – et la publicité contextuelle a été ajoutée l'année suivante. En 2000,

1 K. Bharat, « And now, News », *Google Official Blog*, 23 janvier 2006, https://googleblog.blogspot.com/2006/01/and-now-news.html, consulté le 17 février 2023.

Yandex est devenu une société privée mondialisée constituée aux Pays-Bas, cotée au NASDAQ depuis 2011. Jusqu'en 2022, c'était la plus grande entreprise technologique de Russie ; ses activités étaient diversifiées (VTC, livraison de nourriture, jeux vidéo, streaming musical, etc.) et ses revenus avaient plus que triplé en cinq ans, passant de 60 milliards de roubles en 2015 à 218 milliards de roubles en 2020[2]. Yandex a longtemps bénéficié d'un certain degré d'autonomie, et ses fondateurs ont même, à différents moments, exprimé un désaccord politique avec le Kremlin. Cependant, en tant que champion de l'économie nationale et acteur clé de l'organisation de l'information, l'entreprise a fait l'objet d'une surveillance étroite. C'est notamment le cas après les manifestations de 2011-2012 contre la fraude électorale puis lors de l'annexion de la Crimée en 2014, qui ont constitué un tournant plus général pour la Russie en raison du contrôle croissant exercé sur les médias, Internet et la société civile [Oates, 2013 ; Soldatov & Borogan, 2015 ; Wijermars & Lehtisaari, 2020]. Dans ce contexte, l'agrégateur Yandex.News a été tout particulièrement ciblé.

Dans un premier temps, nous présentons dans ce chapitre le principe de fonctionnement d'un agrégateur de nouvelles ainsi que les vulnérabilités déjà identifiées de ces systèmes. Lorsqu'ils sont apparus, les moteurs de recherche et les systèmes de recommandation ont été conçus comme des outils permettant de mieux gérer la diversité des contenus sur le Web. Mais ces plateformes occupent également une place stratégique et sont devenues des intermédiaires clés pour canaliser l'information vers les citoyens. Elles exercent ainsi une forme de pouvoir en façonnant la perception de la réalité sociale. Ce rôle et ces responsabilités ont été mis en lumière à partir du modèle familier de Google News. Les problèmes soulevés par la recommandation automatisée de nouvelles s'inscrivent dans un ensemble plus large de questions concernant le rôle joué par les moteurs de recherche et les plateformes de médias sociaux pour assurer la diversité de l'information [Helberger, 2019] et les possibilités de façonner la sphère publique par le biais du «*gatekeeping* algorithmique» [Napoli, 2014 ; Nechushtai & Lewis, 2019]. Les algorithmes sont souvent critiqués pour leur opacité et le manque d'explicabilité [Pasquale, 2015 ; Saurwein et al, 2015] et bien que ces acteurs aient longtemps défendu une certaine neutralité, il s'avère que les questions liées à la hiérarchisation des nouvelles ne sont pas seulement techniques ou commerciales mais aussi politiques.

Le cas de Yandex.News relève pour partie de ce type de critiques. Les spécificités du dispositif et les débats qu'il a soulevés au cours des années 2010 sont abordés dans la deuxième partie du chapitre. Les controverses associées aux systèmes sociotechniques constituent en effet une voie d'investigation privilégiée pour

2 Yandex 2020 Financial Results (https://ir.yandex/financial-releases? year=2020&report=q4, consulté le 17 février 2023).

accéder aux enjeux politiques [Latour, 2005 ; Marres, 2007]. En Russie, l'attention suscitée par l'agrégateur et les controverses qui l'entourent permettent d'éclairer le rôle de cette « boîte noire » algorithmique en tant que producteur de sens contesté [Bucher, 2016] en complément des autres sources d'information comme la télévision [Alyukov, 2021]. Dans le cas de Yandex.News (et à la différence de Google News), jusqu'en 2022, cinq nouvelles sélectionnées par l'agrégateur étaient affichées en permanence sur la page d'accueil de Yandex, leur assurant une audience considérable. En 2016, les lois visant les agrégateurs de nouvelles contraignent Yandex à restreindre les résultats affichés sur sa page d'actualités [Daucé, 2017]. Trois interprétations rivales de ce qui constitue les « bons » résultats d'agrégation ont été identifiées : celle avancée par l'entreprise Yandex elle-même comme étant le résultat « objectif » de ses algorithmes ; celle des autorités accusant Yandex.News de promouvoir des nouvelles « antipatriotiques », « fausses » ou problématiques ; et enfin celle avancée par les journalistes, les rédacteurs et les professionnels du référencement qui critiquent la plateforme en s'appuyant sur leur sens de ce qui est considéré comme des nouvelles « dignes d'intérêt ».

Cette approche par les controverses est complétée, dans la troisième partie du chapitre, par un audit de l'algorithme lui-même[3], réalisé à partir de méthodes de rétro-ingénierie [Kitchin, 2016 ; Seaver, 2019]. Celles-ci permettent de montrer l'écart entre la diversité des ressources médiatiques russes en ligne et l'étroitesse de l'échantillon de médias représenté par les classements de Yandex.News, exclusivement dominés par un petit ensemble de 14 médias (agences de presse, médias financés par l'État et publications privées « loyales » au gouvernement) [Daucé & Loveluck, 2021]. Avec le déclenchement de la guerre de grande ampleur contre l'Ukraine en février 2022, les usages bellicistes de l'algorithme deviennent plus manifestes encore, conduisant à son transfert sous contrôle direct du pouvoir.

L'histoire de Yandex fournit une étude de cas exceptionnelle de la « gouvernance par les algorithmes » [Musiani, 2013 ; Just & Latzer, 2017 ; voir également Gillespie, 2018], et contribue à comprendre comment les systèmes de recommandation de nouvelles peuvent être sujets à des biais [Kulshrestha et al., 2019 ; Trielli & Diakopoulos, 2019] ou à des formes plus ou moins subtiles de filtrage politique [Jiang, 2014 ; Dovbysh et al. 2022]. Le cas de Yandex permet également de comprendre les spécificités de la politique numérique russe en tant qu'affirmation de la « souveraineté numérique » [Nocetti, 2015 ; Musiani et al., 2019]. Il met au jour les nouveaux « codes de conduite » – impliquant à la fois le code informatique et le code juridique [Lessig, 1999] – qui peuvent être mis en place dans la sphère publique en réseau dans les sociétés contemporaines. Il est révélateur à la fois de la nature stratégique des moteurs de recherche et des algorithmes aujourd'hui

3 Nous remercions Fabrice Demarthon (CNRS/CERCEC) pour son aide dans l'extraction des bases de données et le scrapping des résultats de la page principale de Yandex.News.

[Pasquale, 2015] et des moyens par lesquels le gouvernement russe a cherché à affirmer sa domination sur la gouvernance de l'Internet comprise comme une dimension de la « sécurité de l'information » [Maréchal, 2017]. Il illustre enfin comment les infrastructures numériques peuvent être bridées afin de réguler indirectement la parole en ligne [Sivetc, 2019].

Le *gatekeeping* algorithmique dans les écosystèmes des médias numériques : contexte et enjeux

L'agrégateur Yandex.News est un système automatisé de recommandation d'actualités, le pendant russe de l'agrégateur Google News. Au départ, le service visait à fournir une vue d'ensemble des tendances de l'actualité, en présentant à l'utilisateur des « *clusters* » d'articles connexes. Dans le cas de Google News, des langues et des éditions par pays ont été développées, et des fonctionnalités telles que les alertes par courriel, la personnalisation et la recommandation d'articles d'actualité ont été ajoutées. En 2022, son service indexe des dizaines de milliers de sites d'actualités à travers le monde et est imbriqué avec le moteur de recherche web de Google.

De manière générale, les systèmes de recommandation couvrent un large éventail d'applications, allant du commerce électronique à la musique, aux films et aux actualités [Jannach et al, 2011 ; Ricci et al, 2015]. Ils impliquent un filtrage automatisé, qui repose sur divers paramètres mais qui s'appuie généralement sur les actions des utilisateurs (*backlinks*, clics, recherches, choix, préférences, etc.) afin d'identifier une sélection d'informations qui intéresseront probablement un même utilisateur ou d'autres utilisateurs. S'agissant plus spécifiquement des systèmes de recommandation d'actualités, ils peuvent être fondés principalement sur une analyse du contenu lui-même (la nature des publications, y compris par exemple leur « fraîcheur ») ou bien sur l'activité générée par ces contenus (taux de clics, mesures d'engagement sur les médias sociaux telles que les *likes* et les partages, etc.), sur des formes de « filtrage collaboratif » et la détection des thèmes d'intérêt dans une communauté donnée, ou encore sur les préférences des utilisateurs – ce dernier cas impliquant une personnalisation des actualités agrégées sur la base des données comportementales collectées [Karimi, Jannach & Jugovac, 2018]. En général, les systèmes de recommandation de nouvelles combinent ces approches à différents degrés, selon également que l'utilisateur peut être facilement suivi (par exemple, s'il est connecté ou autrement identifié comme un utilisateur unique).

Au-delà d'une mesure de pertinence combinée à la sélection de contenus pour lesquels d'autres personnes ont manifesté un intérêt, la recommandation d'articles d'actualité nécessite également une sélection *qualitative*. Cette dimension est

plus difficile à définir, car elle implique la recherche d'éléments qui ne font pas nécessairement partie du champ d'action ou de l'attention directe de l'utilisateur. Une mesure clé de la qualité est basée sur la diversité des actualités qu'un agrégateur est capable de fournir. Ce critère peut être évalué en partie en termes de satisfaction de l'utilisateur, mais renvoie également à un enjeu beaucoup plus large concernant le rôle et la responsabilité des médias en tant qu'institution centrale de la démocratie, censée informer correctement les citoyens et fournir un forum public diversifié pour débattre des idées et des opinions [Helberger, 2019].

En outre, les paramètres clés de cette diversité comprennent des dimensions telles que la pluralité des sujets couverts, ainsi que la variété des politiques éditoriales, des perspectives idéologiques, des genres narratifs, etc. [Helberger, Karppinen & D'Acunto, 2018]. Une préoccupation connexe est de savoir si les systèmes de recommandation automatisés peuvent être biaisés à l'encontre de certains types de contenus, qui seraient sous-représentés dans les résultats [Kulshrestha et al., 2019]. En effet, le tableau général peut sembler diversifié, mais des sujets majeurs peuvent être laissés de côté (par exemple, un scandale de corruption), certains sujets peuvent avoir comparativement moins de poids (par exemple, la politique par rapport au sport), ou leur traitement éditorial peut minimiser leur importance (par exemple, en se concentrant sur des aspects moins cruciaux mais plus divertissants).

Très tôt, la « politique des moteurs de recherche » a été présentée comme ayant des implications décisives pour le façonnement de la sphère publique [Introna & Nissenbaum, 2000]. De même, les agrégateurs de nouvelles, qui offrent une visibilité à des informations sélectionnées « automatiquement », ont fait l'objet d'un examen minutieux en raison de leur rôle de plus en plus central et du pouvoir croissant qu'ils ont acquis au sein des écosystèmes médiatiques. Les éditeurs sont devenus de plus en plus dépendants des plateformes numériques [Nielsen & Ganter, 2018], à mesure que ces intermédiaires sont eux-mêmes devenus des *gatekeepers* aux côtés des journalistes [Napoli, 2014], tirant parti du comportement des utilisateurs pour façonner une image globale des « flux hiérarchisés » d'informations [Thorson & Wells, 2015, 2016].

Google, mais aussi Yandex, présentent leurs services comme « neutres », mais ces prétentions à l'objectivité sont critiquées. Les moteurs de recherche de Google sont soupçonnés de piéger les utilisateurs dans des « bulles de filtres » et des « chambres d'écho » [Pariser, 2011 ; Bozdag, 2013]. En rendant les utilisateurs aveugles à certains types d'informations ou à des perspectives alternatives, et en renforçant parfois les préjugés ou les partis pris existants, ces services œuvreraient à saper la sphère publique. Les algorithmes de recherche et les systèmes de recommandation automatisés ont également été accusés de promouvoir l'indignation et les théories

du complot, celui de YouTube étant par exemple présenté comme « le grand radicalisateur[4] ». Cependant, la réalité de ces phénomènes est difficile à évaluer précisément [Flaxman, Goel & Rao, 2016 ; Bruns, 2019], notamment s'agissant des moteurs de recherche (il a ainsi été démontré qu'à l'inverse, ils augmenteraient la diversité de l'information ; voir [Fletcher & Nielsen, 2018]). Dans le cas de Google News, même les fonctions de personnalisation ne semblent pas réduire la diversité des informations [Haim, Graefe & Brosius, 2018]. Bien que les bulles de filtrage individuelles puissent être difficiles à évaluer empiriquement, « la hiérarchisation algorithmique des nouvelles constitue malgré tout une préoccupation pour la diversité des sources, car elle peut concentrer l'attention sur un ensemble restreint de médias avantagés » [Trielli & Diakopoulos, 2019, p. 3].

Discipliner l'algorithme pour contrôler l'actualité ?

Avant d'examiner le cas de Yandex.News, soulignons que pour Google News également la relation avec les organes de presse se présente sous un jour complexe et a généré des controverses. En effet, les agrégateurs offrent une visibilité aux contenus d'actualités en échange d'un accès aux publications, et bien que Google News soit un fournisseur de trafic [Calzada & Gil, 2020], il peut également être perçu comme un média à part entière bénéficiant du contenu (titres et extraits de textes) fourni par les médias d'actualités[5]. Au-delà des questions de droits d'auteur et de modèle économique, les agrégateurs d'actualités affectent la publication de l'actualité elle-même : les contenus doivent respecter des critères valorisés par leurs algorithmes en termes de pertinence, de « fraîcheur », de fréquence des mises à jour, de métadonnées, de *backlinks*, de compatibilité avec les mobiles, etc. Les rédacteurs déploient des stratégies d'optimisation pour les moteurs de recherche (SEO) afin de s'assurer que leur contenu est référencé et promu de manière efficace, en surveillant constamment les analyses d'audience pour comprendre ce qui « fonctionne » et ce qui ne fonctionne pas, quelles histoires gagnent en popularité ou non. En fonction de l'importance du trafic (et donc des recettes publicitaires) d'un site d'information, celui-ci devra adapter son contenu et ses stratégies de publication afin d'être « repris » par les plateformes – ce qui a une incidence directe sur le travail des journalistes et sur les conceptions conventionnelles de la « valeur de l'information » (*newsworthiness*) ou de son « caractère notable » [Boyer, 2013 ; Belair-Gagnon & Holton, 2018 ; Diakopoulos, 2019a].

4 Z. Tufekci, « YouTube, the great radicalizer », *The New York Times*, 10 mars 2018, https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html, consulté le 17 février 2023 ; voir également [O'Callaghan et al., 2015].

5 Cela a donné lieu à des discussions animées dans la plupart des pays, qui ont généralement trouvé un accord, sauf en Espagne, où le service est fermé en raison de l'introduction d'une « taxe sur les liens » qui oblige Google à payer une redevance pour afficher les extraits de texte.

Les algorithmes déployés par ces plateformes peuvent donc être perçus comme une « main invisible » décidant quels sujets seront désignés comme pertinents et quels organes d'information seront poussés sur le devant de la scène selon des critères parfois insondables – affectant profondément la nature même du journalisme, dans la mesure où les professionnels ajustent la forme et la nature des contenus qu'ils publient afin de satisfaire ces contraintes [Brake 2017 ; Christin, 2020]. Le rôle joué par les algorithmes dans le tri des informations, l'orientation de la visibilité et de l'attention, le cadrage des enjeux et la mise à l'agenda, est de plus en plus remis en question, dans la mesure notamment où :

> « La détection algorithmique de tendances peut refléter la popularité d'un enjeu tout en le portant à la connaissance d'un public élargi, aidant ainsi à rassembler les personnes intéressées par cet enjeu. D'un autre côté, on peut raisonnablement se poser des questions lorsqu'un fil d'actualité manque d'informer ses utilisateurs de mouvements sociaux importants tout en continuant à les amuser et à détourner l'attention vers des événements populaires. » [Diakopoulos, 2019a, p. 183]

Par ailleurs, l'impact des moteurs de recherche sur les choix et les préférences des utilisateurs peut avoir une grande portée, et dans une série d'expériences contrôlées, il a même été démontré qu'il pouvait faire basculer les électeurs indécis [Epstein & Robertson, 2015].

Compte tenu de son rôle central dans la diffusion des informations aujourd'hui, Google est régulièrement soupçonné de donner de la visibilité à des sources illégitimes (par exemple, le forum d'images controversé 4chan après la fusillade de Las Vegas en 2017[6]) ou d'être politiquement biaisé en faveur de certains types de sources d'informations (« de gauche ») [Diakopoulos, 2019b]. Il a également été affirmé que le trafic référencé par les moteurs de recherche semble profiter principalement à un petit nombre d'organes de presse déjà très visibles – ce qui consacre les hiérarchies médiatiques existantes et sape les prétentions à un plus grand pluralisme [Hindman, 2008, 2018 ; Hong & Kim, 2018]. Cela peut également être le cas avec l'agrégation de nouvelles : il a été démontré que pour Google News, seuls cinq organismes de presse représentent près de la moitié de toutes les nouvelles recommandées et que les médias traditionnels dominent les recommandations ([Nechushtai & Lewis, 2019] ; voir également [Bui, 2010]).

Dans le contexte politique russe, les questions soulevées par l'agrégateur Yandex. News sont de même nature mais se posent de manière plus aiguë encore : comment identifier les biais d'agrégation dans un contexte politique oppressif ?

6 A. Robertson, « After its 4chan slip-up, is it time for Google to drop Top stories? », *The Verge*, 3 octobre 2017, https://www.theverge.com/2017/10/3/16413082/google-4chan-las-vegas-shooting-top-stories-algorithm-mistake, consulté le 17 février 2023.

Les résultats peuvent-ils être manipulés pour des motifs politiques, soit en interférant directement avec les résultats, soit en trompant l'algorithme ? Comment s'est élaborée progressivement l'emprise politique pesant sur la hiérarchisation des nouvelles ? Comment critiquer ou contourner un outil manipulé dans un contexte où les libertés politiques ont disparu ? Pour répondre à ces questions, l'étude des controverses qui surgissent autour de l'agrégateur permet de saisir les enjeux politiques qui pèsent sur ce service.

Yandex.News dans les controverses politiques en Russie

Depuis 2004, Yandex.News présente une sélection de sujets et d'articles censés refléter les thèmes les plus largement couverts par les médias en Russie à un moment donné. Ce service a été mis au point par une équipe d'informaticiens et de linguistes, pour développer la reconnaissance et l'extraction des actualités. Lors de son lancement, Yandex.News affirmait que l'algorithme fonctionne « sans intervention humaine ». Les actualités publiées par les médias partenaires sont regroupées en « sujets » en vertu du *clustering* réalisé par l'algorithme. Le robot analyse les mots-clés et les faits et les regroupe par thèmes, en utilisant trois critères principaux : le taux de citation, la nouveauté et le degré d'information[7].

Lev Gershenzon[8] a dirigé l'équipe de développement de Yandex.News à partir de 2004, alors que Yandex n'employait qu'environ 200 personnes au total. À cette époque, Google News existait déjà, mais, selon L. Gershenzon, « Chez Yandex, nous étions plus forts et plus attrayants pour les utilisateurs. C'est pourquoi nous avons placé le Top 5 sur la page principale, ce que Google n'a jamais essayé de faire[9] ». En effet, jusqu'en septembre 2022, un encart de 5 actualités est constamment présenté sur la page d'accueil du moteur de recherche de Yandex – assurant à cette petite sélection de nouvelles une audience quotidienne massive, et entraînant un trafic considérable vers les publications présentées.

7 Ces principes sont présentés ici : https://yandex.ru/promo/news/index (consulté le 17 février 2023).

8 Diplômé de la chaire de linguistique théorique et informatique de l'université des sciences sociales de Moscou (RGGU).

9 L. Gershenzon, entretien avec les auteurs, janvier 2020.

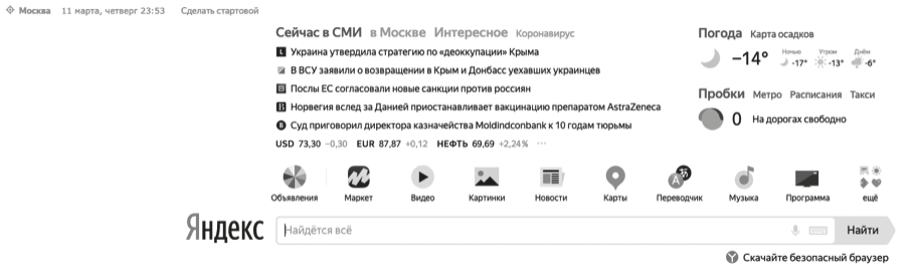


Figure 4. La page d'accueil de Yandex, capture d'écran, 11 mars 2021

Bien que Google propose également une sélection de « Top Stories » dans son moteur de recherche, celles-ci sont liées à des recherches spécifiques et n'apparaissent avec le reste des résultats qu'après coup, lorsqu'une requête a été formulée. Le Top 5 est donc essentiel pour comprendre comment Yandex, en tant que plateforme, fonctionne comme système de recommandation d'actualités. En 2017, selon Grigori Bakounov, directeur technique de Yandex : « L'audience quotidienne des cinq actualités qui apparaissent sur la page d'accueil de Yandex est la même que celle de la page d'accueil – c'est-à-dire environ 20 millions de personnes, selon les jours. 6 millions de personnes visitent quotidiennement la page Yandex.News[10] ».

Yandex.News au cœur du contrôle politique

Jusqu'au début des années 2010, selon les journalistes russes, « Yandex et le Kremlin représentent deux Russies différentes qui se recoupent peu[11] ». Le cofondateur de Yandex, Ilya Segalovitch, et certains de ses collègues ont activement participé aux protestations contre les fraudes électorales en 2011 et 2012. Depuis lors cependant, le gouvernement russe a augmenté sa pression sur l'entreprise [Oates, 2013 ; Soldatov & Borogan, 2015]. Yandex est considéré comme un actif national clé, assurant un certain degré d'indépendance vis-à-vis des entreprises étrangères (notamment américaines) du Web. Ses activités sont contraintes par des moyens politiques, juridiques, techniques et économiques [Vendil Pallin, 2017]. En 2009, les propriétaires de Yandex ont vendu une « action dorée » (action prioritaire) à

10 « Protesty ne v tope », *Radio Svoboda* - Krym Realii, 29 mars 2017, https://ru.krymr.com/a/28397904.html

11 E. Osetinskaia, « Yandex, a Russian Success Story and Putin's High-Tech Tiger », editorial pour *The Moscow Times*, 27 septembre 2017, https://themoscowtimes.com/articles/yandex-a-russian-success-story-and-putins-high-tech-tiger-59029.

Sberbank, la caisse d'épargne russe contrôlée par l'État – ce qui donne de facto à cette dernière un droit de veto sur les questions stratégiques[12]. Bien que critiquée, une loyauté relative envers l'État a également apporté à l'entreprise certains avantages. Yandex a ainsi gagné un conflit antitrust contre Google et bénéficié de la pré-installation obligatoire de logiciels russes sur les smartphones en 2021[13].

Cependant, de multiples controverses autour de l'agrégateur sont apparues après 2012, qui ont graduellement mis fin à la croyance en son objectivité. Suite aux manifestations, cette année a été décisive pour la liberté d'expression et pour la régulation d'Internet en Russie [Lonkila, Shpakovskaya & Torchinsky, 2020]. La vague de protestations contre les fraudes électorales – qui a suivi les Printemps arabes – a déclenché une réponse sévère des autorités, qui ont lancé un durcissement progressif des règles régissant l'expression publique [Denisova, 2017]. Depuis cette date, Yandex.News a été spécifiquement visé par différentes mises en cause politiques, par de nouvelles régulations juridiques ainsi que par les contraintes éditoriales pesant sur les médias indépendants. L'une des mesures les plus significatives a été l'établissement par la loi, en 2012, d'une liste noire de sites web censurés, dont les FAI ont depuis été tenus d'empêcher l'accès. Elle visait à l'origine les jeux d'argent illicites, la pédopornographie, les informations liées à la production et à la distribution de drogues, et les informations encourageant le suicide. Cependant, la notion d'« informations interdites » a ensuite été étendue aux « incitations à des actions illégales » ou à la « promotion de l'extrémisme », et a été utilisée en 2014 pour bloquer des sites d'opposition tels que *Grani.ru*, Kasparov.ru ou le blog LiveJournal du leader de l'opposition Alekseï Navalny. La liste est gérée et régulièrement mise à jour par Roskomnadzor, l'agence de surveillance de la communication et des médias, qui accorde également des licences aux médias de masse en Russie. Les sites web bloqués ont ainsi disparu des classements de Yandex.News.

Le contrôle de la sphère publique s'est à nouveau intensifié en 2014, lors du conflit avec l'Ukraine et l'occupation de la Crimée. Des campagnes médiatiques ont été lancées par les autorités, impliquant à la fois les médias d'État et la désormais tristement célèbre « usine à trolls » d'E. Prigojine, afin d'alimenter le soutien aux opinions pro-russes et de saper la crédibilité de toute voix pro-ukrainienne [Fedor, 2015 ; Mejias & Vokuev, 2017]. C'est à cette époque (marquée notamment par les révélations de Snowden sur la surveillance d'Internet par les agences de renseignement américaines) que Poutine déclare que Yandex a été créé

12 M. Seddon, « Yandex agrees restructuring with Kremlin », *Financial Times*, 18 novembre 2019, https://www.ft.com/content/999e3ca6-09db-11ea-bb52-34c8d9dc6d84.

13 Le 16 mars 2021, la Douma adopte une loi fixant des amendes pour la vente de téléphones, tablettes et ordinateurs sans applications russes préinstallées Amendement à l'article 14.8 du Code des infractions administratives (https://sozd.duma.gov.ru/bill/757430-7).

sous influence occidentale, et qu'Internet en général est un « projet spécial de la CIA ». Yandex.News, en particulier, est accusé de partialité par les autorités pour avoir donné de la visibilité à des informations s'écartant du discours officiel. Le site (pro-Kremlin) *Pravda.ru* s'est interrogé : « Yandex est-il en train d'attiser un 'Maïdan' en Russie ? » (en référence aux manifestations de Kiev qui ont conduit au changement de régime en Ukraine)[14]. Le journal s'est indigné des titres choisis par l'agrégateur et a affirmé qu'il était nécessaire de réglementer son activité. En mai 2014, le porte-parole du Kremlin, Dmitri Peskov, a déclaré que Yandex. News devrait être enregistré comme un média de masse, ce qui le placerait sous le contrôle de Roskomnadzor.

En 2016, une loi sur les agrégateurs de nouvelles étend le contrôle à ces intermédiaires et vise spécifiquement Yandex.News. Les agrégateurs de nouvelles recevant plus d'un million de visiteurs quotidiens deviennent légalement responsables des résultats qu'ils publient (et risquent de lourdes amendes en cas de violation), à moins que les médias sélectionnés ne soient officiellement enregistrés auprès de Roskomnadzor. Des accords formels sont mis en place entre Yandex.News et les médias, avec 6 700 « partenariats » établis en 2016. La loi entre en vigueur le 1er janvier 2017. Tous les médias non enregistrés (y compris les voix dissidentes comme *Mediazona*) ainsi que tous les médias étrangers (comme la BBC en russe, ainsi que les médias en exil comme *Meduza*) disparaissent du Top 5 de Yandex.News. Après l'adoption de la loi, Tatiana Isaeva, directrice de Yandex. News depuis 2012, annonce qu'elle quitte l'entreprise. Elle fait valoir dans une interview accordée à *Meduza* que son travail est rendu caduque par la loi et que les objectifs mêmes de l'agrégateur – mettre en évidence les nouvelles importantes et mettre différents points de vue à la disposition de l'utilisateur – sont mis à mal : « L'agrégateur est vraiment destiné à couvrir l'image [de l'actualité] d'un seul coup d'œil. Si cette image se réduit à un seul point de vue, on ne voit absolument pas en quoi un agrégateur est nécessaire[15] ».

Malgré l'adoption de la loi, l'agrégateur Yandex a continué d'être critiqué par les autorités. En août 2019, Yandex est accusé par les députés de la Douma russe de diffuser des « *fake news* » après qu'un article inexact du quotidien *Kommersant* est arrivé en tête de la sélection de Yandex.News. L'article affirme que la Douma envisage l'interdiction des véhicules anciens, ce qui suscite une large indignation dans la société et conduit les députés à apporter des précisions, selon lesquelles il s'agit d'une recommandation qui ne concerne que les véhicules professionnels et non les véhicules personnels. Cependant, l'information reste en tête de la sélection

14 « Yandex « ražigaet » Majdan v Rossii? », Pravda, http://www.pravda.ru/topic/yandex-617/, consulté le 25 août 2016.

15 Entretien avec Tatâna Isaeva publié dans Meduza, 24 octobre 2016, https://meduza.io/feature/2016/10/24/oschuscheniya-chto-ot-mediasredy-otstali-net, consulté le 17 février 2023.

même après avoir été démentie, ce qui conduit certains députés à s'en prendre à l'agrégateur d'informations. Le député Andreï Isaev accuse Yandex d'« exacerber délibérément la situation sociale et politique » et d'« ingérence étrangère », tandis qu'Adalbi Chkhangochev déclare avoir appelé la PDG de Yandex, Elena Bounina, pour lui demander de réviser l'algorithme de l'agrégateur d'informations – ce à quoi Yandex répond en menaçant de fermer son service d'agrégation[16]. Ce nouveau scandale intervient dans un contexte politique difficile pour le gouvernement, les mouvements d'opposition ayant manifesté durant l'été pour dénoncer le refus de les laisser s'inscrire aux élections de la Douma de Moscou.

Yandex.News face au discrédit médiatique

Depuis 2012, des journalistes indépendants et des militants politiques dénoncent l'emprise progressive sur l'agrégateur des tenants de la position « patriotique » (législateurs, administrations régionales, médias officiels…). Les principaux défenseurs des libertés en ligne qui soutenaient initialement l'agrégateur Yandex. News sont devenus sceptiques quant à sa capacité à rester à l'abri des interventions politiques. Ils recueillent des preuves de ses partis pris pour dénoncer sa partialité. Ils affirment que les classements de Yandex.News sont biaisés en faveur du pouvoir. Selon eux, les biais peuvent provenir de l'agrégateur lui-même, qui sape les informations sur l'opposition, ou d'acteurs officiels qui ont appris à tromper l'algorithme. Cette suspicion est nourrie par les observateurs, qui, lors d'événements spécifiques, constatent un décalage entre leur sens commun de ce qui compte et la sélection automatisée fournie par Yandex.

Selon un journaliste de *Kommersant*, « l'algorithme est utilisé par des journaux dépendants du pouvoir, qui publient des informations qui sont poussées vers le haut par l'algorithme[17] ». Ces techniques consistent à repousser les limites de l'optimisation des moteurs de recherche (SEO) et à jouer avec les algorithmes de Yandex.News en créant artificiellement de multiples sources d'information. Elles peuvent être comprises comme l'exploitation des vulnérabilités de la plateforme afin d'obtenir une visibilité accrue. Une logique similaire préside aux stratégies des sites web de *junk news* qui augmentent leur « découvrabilité » dans le moteur de recherche Google (par l'optimisation de mots-clés cette fois) à des fins de désinformation [Bradshaw, 2019]. Ces tentatives de façonner les résultats de recherche sont en fait aussi anciennes que la recherche sur le web elle-même, et les algorithmes sont normalement mis à jour à intervalles réguliers afin de contrer ces manipulations – qui ne cessent toutefois de se reproduire.

16 « Deputaty popali v Yandex.Novosti », *Kommersant'*, 16 août 2019, https://lenta.ru/news/2019/08/16/ya_novosti/, consulté le 17 février 2023).

17 Entretien avec D., journaliste, Moscou, septembre 2019.

Par exemple, selon une enquête du journal *RBK*[18], pendant les élections à la Douma de la ville de Moscou en 2014, des dizaines de sites de médias inconnus publient la même information sur le succès présumé de Sergeï Sobianine, maire de Moscou et candidat à sa réélection – nouvelle qui se retrouve dans les premiers résultats de Yandex.News. D'après cette enquête, plusieurs centaines de journaux de quartier, de sites web institutionnels et d'agences gouvernementales (dont beaucoup avaient été récemment créés) auraient été enregistrés dans la « base de données des médias et des sources officielles » de Yandex. Les informations en faveur du maire de Moscou auraient été transmises par la société *Moscow Information Technologies* (détenue par les autorités de Moscou) aux médias et sites. Ces derniers auraient réécrit les nouvelles pour s'assurer que les articles ne seraient pas identifiés comme des doublons par l'algorithme de Yandex, avant d'être publiés sur ces sites locaux.

En mars 2017, d'importantes manifestations ont lieu à Moscou et dans toute la Russie après la publication, par la Fondation anticorruption (FBK) d'Alekseï Navalny, d'une enquête d'investigation montrant de multiples exemples de détournements de fonds présumés par l'ex-Premier ministre Dmitri Medvedev. À Moscou, un millier de personnes sont arrêtées, mais étonnamment, selon le journaliste Alekseï Kovalev, les manifestations sont à peine mentionnées sur la page principale de Yandex.News et même sur le fil d'actualités locales pour Moscou[19]. Yandex fait valoir que ses algorithmes n'ont pas été altérés, mais qu'il s'agit d'une conséquence de la loi sur les agrégateurs qui a considérablement réduit le nombre de sources disponibles – illustrant ainsi comment la loi produit un mécanisme de contrôle indirect [Wijermars, 2021].

Les soupçons politiques à l'encontre de l'agrégateur de nouvelles refont surface en avril 2020. *TJournal* (un site russe consacré à la technologie) montre que lors d'une recherche sur Alekseï Navalny, le moteur de recherche Yandex et les services Yandex.News ne renvoient que des contenus négatifs[20]. Interrogé par *TJournal*, Yandex déclare que la priorité donnée aux publications négatives sur Navalny était une « expérience ». En 2021, après le retour de Navalny d'Allemagne et son emprisonnement, des manifestations éclatent à Moscou. Les militants soulignent la discrétion de Yandex.News sur ces événements. Un activiste proche de Navalny

18 Zh. Ulânova, D. Luganskaâ. « Rassledovanie RBK : kak činovniki perehitrili Yandex », РБК, 22 octobre 2014, http://top.rbc.ru/technology_and_media/22/10/2014/5447a659cbb20f1d5d33b94d, consulté le 17 février 2023.

19 A. Kovalev, « Hear no evil, see no evil, report no evil », *The Moscow Times*, 27 mars 2017, https://www.themoscowtimes.com/2017/03/27/hear-no-evil-see-no-evil-report-no-evil-a57550, consulté le 17 février 2023.

20 « Yandex vsemi svoimi servisami risuet obraz Naval'nogo », *TJournal*, 26 avril 2020, https://tjournal.ru/news/162614-yandeks-vsemi-svoimi-servisami-risuet-obraz-navalnogo, consulté le 17 février 2023.

considérait déjà en 2018 que : « Yandex.News transmet de la propagande d'État. L'agrégateur a été détruit ». Certains de ces observateurs soulignent que Yandex évite les conflits avec les autorités étatiques afin de ne pas mettre en péril ses multiples activités lucratives (Yandex.Taxi, Yandex.Eda, etc.)[21].

Objectiver la contrainte

Au cours du mois de juin 2020, pour tester ces suspicions, nous avons effectué une analyse quantitative des actualités sélectionnées par Yandex.News et présentées dans le Top 5 des nouvelles sur la page d'accueil. Nous avons procédé à une collecte systématique des actualités entre le 1er et le 30 juin 2020[22]. L'expérience montre que, durant cette période, seul un petit groupe de 14 médias est cité dans le Top 5 – un échantillon extrêmement limité si l'on considère les plus de 7 000 sources répertoriées dans la base de données Yandex.News. Nous avons ensuite étendu la collecte à la période juin-décembre 2020 et obtenu les mêmes résultats, avec les mêmes 14 médias apparaissant dans le Top 5 sur cette période [Daucé & Loveluck, 2021]. Les données montrent de manière frappante la concentration des informations sur Yandex.News entre quelques grands acteurs médiatiques : agences de presse publiques, médias financés par l'État, grands journaux et publications en ligne grand public.

Dans le cas de Google News, une surreprésentation de certains médias a également pu être mise en évidence [Schroeder & Kralemann, 2005 ; Haim, Graefe & Brosius, 2018], mais pas dans une telle mesure. Sur Yandex.News, l'éventail est beaucoup plus étroit que les résultats observés par Nechushtai et Lewis [2019] dans le cas de Google News aux États-Unis par exemple où, bien qu'une petite sélection de 14 sources domine également l'agrégateur, une « longue traîne » d'autres publications figure également dans les résultats. Trielli et Diakopoulos [2019], examinant Google Top Stories aux États-Unis, ont constaté que seulement vingt sources d'information représentaient plus de la moitié des articles présentés et qu'un « biais idéologique de gauche » pouvait être observé dans la sélection des sources ; cependant, là encore, une longue traîne considérable

21 Au-delà de son moteur de recherche Web, Yandex a développé une foule d'autres services tels qu'un portail Internet ou un service de messagerie électronique, ainsi que des entreprises plus spécifiques comme Yandex.Taxi (transport de personnes par taxi, qui a fusionné avec Uber en 2017), Yandex.Karty (cartes et géolocalisation), Yandex.Music (streaming musical) ou Yandex.Eda (livraison de nourriture).

22 Nous avons collecté automatiquement les classements de Yandex.News toutes les deux heures et répertorié un total de 3 011 références. Les données ont été collectées sur un serveur basé en France, mais nous avons contrôlé les éventuelles fonctionnalités de personnalisation et de localisation en vérifiant à différents moments les actualités dont les résultats apparaissent pour un utilisateur basé en Russie et n'avons trouvé aucune différence.

de plus de 650 autres sources d'information apparaissait au moins une fois dans la seconde moitié des 6 302 liens collectés sur une période d'un mois.

Dans le cas de la Russie, bien que des nuances puissent être décelées entre ces 14 grands médias, il apparaît clairement que seuls les médias « loyaux » accèdent aux classements de Yandex. La majorité de ces publications sont liées au Kremlin : elles sont soit directement financées par l'État, soit possédées par des personnalités ou des entités « loyalistes » et donc indirectement « gérées » par les autorités. Depuis 2014, le panorama médiatique russe est généralement divisé entre les médias « étatiques » et les médias « privés indépendants ». Les frontières de ces différentes catégories sont floues et discutables. Les médias d'État sont clairement identifiés (*RIA Novosti, RT, Rossijskaïa Gazeta, TASS, Interfax*). Les médias « loyaux privés patriotiques » désignent les médias d'information générale qui ont été transformés de l'intérieur par le départ et le remplacement de leurs équipes rédactionnelles entre 2012 et 2014 (*Izvestia, Lenta.ru, Gazeta.ru*). Une « façade » officielle demeure mais ils ont subi des interventions hostiles, leurs équipes étant remplacées par des journalistes fidèles au pouvoir [Chupin & Daucé, 2017 ; Daucé, 2020 ; Kovalev, 2020]. Les médias « loyaux privés libéraux » font référence aux médias d'affaires qui étaient considérés comme « libéraux » mais dont le service politique a été réorganisé entre 2018 et 2020 (cela concerne principalement *RBK, Kommersant, Vedomosti*). Yandex.News évolue dans un contexte de remaniement économique et politique de l'espace médiatique russe, où différents types de contraintes ont conduit à un rétrécissement du spectre médiatique [Wijermars & Lehtisaari, 2020]. En conséquence, les principales sources utilisées par Yandex.News, sur lesquelles l'algorithme s'appuie pour dresser un tableau de l'actualité quotidienne sur le Web, ont été profondément modifiées. À l'inverse, les médias indépendants sont mis à l'écart car ils ne bénéficient pas du trafic référencé par Yandex.News et des recettes publicitaires qui l'accompagnent, ce qui réduit la diversité de l'exposition et les rend moins viables commercialement [Kovalev, 2020 ; Wijermars, 2021].

Épilogue : la guerre inégale des agrégateurs

Avant même le déclenchement de la guerre contre l'Ukraine, de nombreux observateurs soulignent la perte de légitimité de l'algorithme de Yandex.News aux yeux des journalistes, ainsi que des professionnels du Web et des développeurs qui cherchent des moyens de le contourner. Certains d'entre eux considèrent que le service a perdu son sens. Comme le remarquait Lev Gershenzon en 2016 : « Les agrégateurs n'ont de sens (…) que lorsqu'il y a quelque chose à agréger. Si toutes les publications indépendantes, intéressantes et professionnelles à l'échelle fédérale peuvent être comptées sur les doigts d'une main, leur agrégation et leur traitement ne nécessitent pas de technologie sophistiquée – vous pouvez simplement les

ajouter à vos signets »[23]. L'idée de fermer le service semble avoir été envisagée par les dirigeants de Yandex eux-mêmes. Selon le journaliste A. Pliouchtchev, de la radio *Ekho Moskvy* (fermée en mars 2022) :

> « Vous savez, j'ai parlé une fois avec A. Voloj, le directeur de Yandex, et c'était avant que la loi sur les agrégateurs ne soit adoptée. Et il m'a dit que si la loi était adoptée, il fermerait le service. (…) Eh bien, la loi a été un peu adoucie, et le service, comme vous pouvez le voir, n'a pas fermé. Je doute toujours que ce soit la bonne décision. Parce que, eh bien, je pense que, malheureusement, l'État a tout fait pour manipuler à la fois les médias et l'extraction dans les moteurs de recherche »[24].

En mai 2018, dans une lettre ouverte adressée à Elena Bounina, PDG de Yandex, A. Pliouchtchev lui conseille de fermer le service Yandex.News ou de le rebaptiser Yandex.Propaganda.

Face à la mise en cause de Yandex.News, des projets de développement d'un agrégateur alternatif émergent. En 2019, le fondateur de Telegram, Pavel Dourov, annonce depuis l'étranger son intention de développer un agrégateur de nouvelles sur sa plateforme : « Nous avons une chance de créer le premier agrégateur de nouvelles efficace et gratuit de l'histoire d'Internet », déclare Dourov. « Nous pouvons créer un bloc d'articles recommandés après avoir lu chaque article dans Telegram, pour aboutir progressivement à un service avec une sélection horaire et une recherche globale de toutes les nouvelles du monde[25] ». P. Dourov annonce que son agrégateur échappera au contrôle des services de sécurité russes et à la censure politique, à la différence des services localisés en Russie. Il invite les développeurs de Yandex.News à participer à la création de son service et lance un concours, le Data Clustering Contest[26], visant à amorcer le développement d'un algorithme d'agrégation sur la plateforme. Bien que le concours ait effectivement été lancé, la mise en service de l'agrégateur est repoussée et le service promis n'était pas entré en service lorsque la guerre a éclaté.

À partir de février 2022, la guerre renforce ces controverses autour de l'algorithme. Dès le 27 février, Lev Gershenzon, depuis l'étranger, publie un long texte sur Facebook où il dénonce les méfaits de l'agrégateur de nouvelles de Yandex :

23 L. Gershenzon. « Nothing to aggregate », Republic, 20 avril 2016, https://republic.ru/posts/66965, consulté le 17 février 2023.

24 Entretien avec Aleksandr Pliušev, Moscou, mars 2019.

25 https://www.vedomosti.ru/technology/articles/2019/06/07/803708-durov-sozdast, consulté le 16 février 2023.

26 La première étape du concours a lieu en novembre 2019 et la seconde en mai 2020.

> « Aujourd'hui, chaque jour, la guerre de la Russie contre l'Ukraine est possible parce qu'il n'y a pas de manifestations massives contre la guerre dans les villes russes. Et s'il n'y en a pas, c'est non seulement à cause du danger de représailles envers ceux qui manifestent (grande admiration pour tous ceux qui manifestent), mais surtout parce que la grande majorité de la population ignore que les troupes russes mènent une guerre totale depuis quatre jours. Outre la télévision, Yandex, qui publie son bloc de cinq nouvelles sur sa page d'accueil, est la cause de cette ignorance. (…) Chaque heure et chaque jour qui passe de cette façon contribue à la guerre ».

Le 1er mars, il écrit à nouveau :

> « Aujourd'hui, c'est le sixième jour de la guerre de la Russie contre l'Ukraine. Des missiles et des lance-roquettes bombardent les quartiers résidentiels, les dortoirs et les maternités de Kharkiv. Onze morts, des dizaines de blessés. Aujourd'hui c'est le sixième jour où au moins 30 millions d'utilisateurs russes voient sur la page d'accueil de Yandex qu'il n'y a pas de guerre, qu'il n'y a pas de milliers de soldats russes morts, de dizaines de civils tués par les bombardements russes, de dizaines de prisonniers, d'énormes destructions dans diverses villes ukrainiennes. Le fait qu'une grande partie de la population russe puisse croire qu'il n'y a pas de guerre est la base et le moteur de cette guerre. Yandex est aujourd'hui un élément clé dans la dissimulation des informations sur la guerre ».

Le message a reçu plus de 3 700 likes et est suivi de nombreux commentaires.

Suite à ces prises de position, Lev Gershenzon annonce la création d'un agrégateur de nouvelles alternatif non censuré[27]. Il souhaite afficher ainsi la diversité des contenus et des points de vue disponibles en ligne. Le nouvel agrégateur est conçu par une équipe de volontaires d'une vingtaine de personnes qui avaient travaillé ensemble pour Yandex. Ils espèrent par la suite trouver des recettes économiques pour financer le projet. En août 2022, l'agrégateur est lancé sous le nom *The True Story* (https://thetruestory.news). Quatre jours plus tard, il est bloqué en Russie sur demande de Roskomnadzor. Il ne demeure accessible qu'à l'étranger, ou, en Russie même, qu'aux utilisateurs de VPN. Les représentants du pouvoir russe ont immédiatement dénoncé le nouvel agrégateur. Selon le vice-président de la commission de la politique économique de la Douma d'État, Artem Kiryanov :

> « L'agrégateur de nouvelles *The True Story* a servi à répandre la panique et les fausses informations sans refléter une image objective du monde. Il se présente comme une plateforme indépendante. Mais (…) pourquoi n'y a-t-il que des contenus négatifs dans les classements ? (…) La réponse tient peut-être à l'histoire de sa création, notamment de Lev Gershenzon, l'homme qui a créé *The True Story*. Apparemment, il

27 https://holod.media/2022/05/17/gershenzon-yandex/, consulté le 17 février 2023.

> s'agissait d'une tentative de créer une chaîne au service de la guerre de l'information contre la Russie, où l'objectif principal n'est pas la présentation objective d'informations, mais la promotion de *fake news* et le fait de semer la panique[28]».

Le nouvel agrégateur collecte les données de médias officiellement enregistrés en Russie (*RBK, Kommersant', Vedomosti, Fontanka, Interfax*) mais aussi de nombreux sites considérés comme «agents de l'étranger» ou interdits en Russie (*Doxa, Meduza, Radio Svoboda, RTVI, Golos Ameriki, Novaïa Gazeta…).* L'audience du nouvel agrégateur reste modeste puisqu'il n'est pas adossé à un moteur de recherche. En novembre 2022, il comptait environ 20 000 inscrits sur sa chaîne Telegram. Ce nouvel agrégateur suscite cependant l'intérêt des défenseurs de l'Internet libre. Pour renforcer sa visibilité, un projet de partenariat avec la Société pour la défense d'Internet (OZI) prévoit de l'afficher en page d'accueil d'un VPN promu par cette association[29].

Conclusion

L'histoire récente de Yandex.News en Russie met en évidence la manière dont la régulation des plateformes peut être utilisée pour mettre en place une forme de «gouvernance par les algorithmes» de la sphère publique. Présenté initialement comme un moyen technique de rendre compte «objectivement» de la diversité des contenus en ligne, l'agrégateur a suscité différentes controverses techno-politiques dans les années 2010 : les autorités lui reprochaient de promouvoir des nouvelles «antipatriotiques» ou «fausses», tandis qu'à l'inverse, les journalistes, les professionnels du Web et les utilisateurs soulignaient que les «vérités qui dérangent» avaient du mal à atteindre le haut des classements. L'adoption en 2016 d'une loi sur les agrégateurs de nouvelles, autorisant uniquement les sources officiellement «enregistrées» à être affichées par le service, a clairement montré l'intention de domestiquer la plateforme afin de limiter la visibilité des contestations et du mécontentement dans la sphère publique. Cette réglementation s'est appliquée dans un écosystème numérique complexe qui articule différents niveaux de contrôle, entre Yandex.News et d'autres plateformes, l'organisme de surveillance des télécommunications Roskomnadzor, ainsi que les médias et les journalistes eux-mêmes.

Les différents types de preuves présentées dans cette recherche – entre controverses publiques, audit sommaire de l'algorithme et étude des textes officiels – indiquent que Yandex, en tant que système de recommandation d'actualités, respecte des «codes de conduite» à la fois juridiques et techniques

28 Post de Lev Gershenzon sur Facebook, le 14 septembre 2022.

29 Entretien avec un responsable de la Société pour la défense d'Internet, Paris, novembre 2022.

garantissant que les informations qu'il promeut et amplifie restent sous contrôle. Ainsi, en 2020, le service n'a donné de la visibilité qu'à 14 médias qui sont eux-mêmes étroitement surveillés par les autorités russes par l'intermédiaire de Roskomnadzor. Le contrôle serré des classements de l'algorithme est évident par rapport à Google News qui, s'il fait la part belle à une petite sélection de grands organes de presse, comptabilise également une longue traîne de publications diverses et, en tout état de cause, n'affiche pas une sélection d'actualités par défaut sur la page d'accueil de son moteur de recherche. Yandex.News ne représente donc qu'une façade de pluralisme de l'information. De plus, il ne reflète plus la diversité des contenus qui circulent encore dans l'espace numérique russe. L'agrégateur apparaît comme un rouage important dans les dispositifs de renforcement du contrôle exercé par les autorités sur l'ensemble de l'écosystème médiatique russe. Les autorités justifient leurs efforts pour contrôler l'agenda médiatique et réaffirmer leur souveraineté sur la sphère publique en dénonçant les informations qualifiées de « non patriotiques », « fausses » ou autrement problématiques.

Les acteurs des médias et les professionnels de l'information, face aux nouveaux obstacles auxquels ils sont confrontés, développent une vision critique du rôle et du fonctionnement des plateformes et de leurs algorithmes – mettant au jour les enjeux politiques de ces infrastructures clés. Avec la guerre contre l'Ukraine engagée par la Russie, la mainmise politique sur l'agrégateur Yandex.News est devenue évidente à travers son rachat par la société VKontakte, directement inféodée au pouvoir. Dans un contexte de plus en plus menaçant, où de nombreux journalistes et spécialistes de l'Internet russe sont conduits à l'exil, ils cherchent des canaux alternatifs pour diffuser l'information, en s'appuyant sur les médias sociaux tels que Telegram ou Twitter. Pris dans un rapport de force inégal, certains d'entre eux, autour de L. Gershenzon, élaborent même un agrégateur alternatif pour rendre compte de la « vraie histoire », espérant ainsi mettre les algorithmes au service de leur cause et de la paix en Ukraine.

Références bibliographiques

[Alyukov, 2021] Alyukov, Maxim, « News reception and authoritarian control in a hybrid media system: Russian TV viewers and the Russia-Ukraine conflict », *Politics*, online first .

[Belair-Gagnon & Holton, 2018] Belair-Gagnon, Valerie & Holton, Avery E., « Boundary work, interloper media, and analytics in newsrooms: an analysis of the roles of web analytics companies in news production, » *Digital Journalism*, vol. 6, n°4, p. 492-508.

[Boyer, 2013] Boyer, Dominic, *The Life Informatic. Newsmaking in the Digital Era*, Ithaca, NY and London, Cornell University Press.

[Bozdag, 2013] Bozdag, Engin, «Bias in algorithmic filtering and personalization,» *Ethics and Information Technology*, vol. 15, n°3, p. 209-227.

[Bradshaw, 2019] Bradshaw, Samantha, «Disinformation optimised: gaming search engine algorithms to amplify junk news,» *Internet Policy Review*, vol. 8, n°4, p. 1-24.

[Brake, 2017] Brake, David R., «The invisible hand of the unaccountable algorithm: how Google, Facebook and other tech companies are changing journalism», in Tong, Jingrong & Lo, Shih-Hung (dir.), *Digital Technology and Journalism. An International Comparative Perspective*, Cham, Palgrave Macmillan, p. 25-46.

[Bruns, 2019] Bruns, Axel, *Are Filter Bubbles Real?* Cambridge, Polity Press.

[Bucher, 2016] Bucher, Taina, «Neither black nor box: ways of knowing algorithms», in Kubitschko, Sebastian & Kaun, Anne (dir.), *Innovative Methods in Media and Communication Research,* Basingstoke and New York, Palgrave Macmillan, p. 81-98.

[Bui, 2010] Bui, CamLy, «How online gatekeepers guard our view. News portals' inclusion and ranking of media and events,» *Global Media Journal*, vol. 9, n° 16, p. 1-41.

[Calzada & Gil, 2020] Calzada, Joan & Gil, Ricard, 2020. «What do news aggregators do? Evidence from Google News in Spain and Germany,» *Marketing Science*, vol. 39, n° 1, p. 134-167.

[Christin, 2020] Christin, Angèle, *Metrics at Work. Journalism and the Contested Meaning of algorithms*, Princeton, NJ, Princeton University Press.

[Chupin & Daucé, 2017] Chupin, Ivan & Daucé, Françoise, «Termination of journalists' employment in Russia: political conflicts and ordinary negotiation procedures in newsrooms,» *Laboratorium: Russian Review of Social Research*, vol. 9, n°2, p. 39-58.

[Daucé, 2017] Daucé, Françoise, «Political conflicts around the Internet in Russia: the case of Yandex.Novosti,» *Laboratorium: Russian Review of Social Research*, vol. 9, n°2, p. 112-32.

[Daucé, 2020] Daucé, Françoise. «Disguising the Internet? Website design and control in Russia,» *Digital Icons*, n° 20, https://www.digitalicons.org/issue20/disguising-the-Internet-website-design-and-control-in-russia

[Daucé & Loveluck, 2021] Daucé, Françoise & Loveluck, Benjamin, «Codes of conduct for algorithmic news recommendation: the Yandex.News controversy in Russia», *First Monday*, vol. 26, n° 5.

[Denisova, 2017] Denisova, Anastasia, «Democracy, protest and public sphere in Russia after the 2011-2012 anti-government protests: digital media at stake,» *Media, Culture & Society*, vol. 39, n° 7, p. 976-994.

[Diakopoulos, 2019a] Diakopoulos, Nicholas, *Automating the News. How Algorithms are Rewriting the Media*. Cambridge, MA and London, Harvard University Press.

[Diakopoulos, 2019b] Diakopoulos, Nicholas, «Audit suggests Google favors a small number of major outlets,» *Columbia Journalism Review,* 10 mai 2019, https://www.cjr.org/tow_center/google-news-algorithm.php

[Dovbysh et al, 2022] Dovbysh, Olga, Wijermars, Mariëlle & Makhortykh, Mykola, «How to reach nirvana: Yandex, news personalisation, and the future of Russian journalistic media,» *Digital Journalism*, online first.

[Epstein & Robertson, 2015] Epstein, Robert & Robertson, Ronald E., «The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections,» *PNAS – Proceedings of the National Academy of Sciences of the United States of America*, vol. 112, n° 33, p. E4512-E4521.

[Fedor, 2015] Fedor, Julie (dir.), «Russian media and the war in Ukraine,» special issue of the *Journal of Soviet and Post-Soviet Politics and Society*, vol. 1, n° 1.

[Flaxman et al, 2016] Flaxman, Seth, Goel, Sharad, & Rao, Justin M., «Filter bubbles, echo chambers, and online news consumption,» *Public Opinion Quarterly*, vol. 80, n° S1, p. 298-320.

[Fletcher & Nielsenl, 2018] Fletcher, Richard & Nielsen, Rasmus Kleis, «Automated serendipity: the effect of using search engines on news repertoire balance and diversity,» *Digital Journalism*, vol. 6, n° 8, p. 976-989.

[Gillespie, 2018] Gillespie, Tarleton, «Regulation of and by platforms», in Burgess, Jean, Marwick, Alice & Poell, Thomas (dir.), *The SAGE Handbook of Social Media,* London and Thousand Oaks, CA, Sage, p. 254-278.

[Haim et al, 2018] Haim, Mario, Graefe, Andreas & Brosius, Hans-Bernd, «Burst of the filter bubble? Effects of personalization on the diversity of Google News,» *Digital Journalism*, vol. 6, n° 3, p. 330-343.

[Helberger, 2012] Helberger, Natali, «Exposure diversity as a policy goal,» *Journal of Media Law*, vol. 4, n° 1, p. 65-92.

[Helberger, 2019]. Helberger, Natali, «On the democratic role of news recommenders,» *Digital Journalism*, vol. 7, n° 8, p. 993-1012.

[Helberger et al, 2018] Helberger, Natali, Karppinen, Kari & D'Acunto, Lucia, 2018, «Exposure diversity as a design principle for recommender systems,» *Information, Communication & Society*, vol. 21, n° 2, p. 191-207.

[Hindman, 2008] Hindman, Matthew S., *The Myth of Digital Democracy,* Princeton, NJ, Princeton University Press.

[Hindman, 2018] Hindman, Matthew S., *The Internet Trap. How the Digital Economy Builds Monopolies and Undermines Democracy,* Princeton, NJ, Princeton University Press.

[Hong & Kim, 2018] Hong, Sounman & Kim, Nayeong, «Will the Internet promote democracy? Search engines, concentration of online news readership, and e-democracy,» *Journal of Information Technology & Politics*, vol. 15, n° 4, p. 388-399.

[Introna & Nissenbaum, 2000] Introna, Lucas & Nissenbaum, Helen, «Shaping the Web: why the politics of search engines matters,» *The Information Society*, vol. 16, n° 3, p. 169-185.

[Jannach et al, 2011] Jannach, Dietmar, Zanker, Markus, Felfernig, Alexander & Friedrich, Gerhard, *Recommender Systems. An Introduction*, Cambridge and New York, Cambridge University Press.

[Jiang, 2014] Jiang, Min, «The business and politics of search engines: a comparative study of Baidu and Google's search results of Internet events in China,» *New Media & Society*, vol. 16, n° 2, p. 212-233.

[Just & Latzer, 2017] Just, Natascha & Latzer, Michael, «Governance by algorithms: reality construction by algorithmic selection on the Internet,» *Media, Culture & Society*, vol. 39, n° 2, p. 238-258.

[Karimi et al, 2018] Karimi, Mozhgan, Jannach, Dietmar, & Jugovac, Michael, «News recommender systems – survey and roads ahead,» *Information Processing & Management*, vol. 54, n° 6, p. 1203-1227.

[Kitchin, 2016] Kitchin, Rob, «Thinking critically about and researching algorithms,» *Information, Communication & Society*, vol. 20, n° 1, p. 14-29.

[Kovalev, 2020] Kovalev, Alexey, «The political economics of news making in Russian media: ownership, clickbait and censorship,» *Journalism*, vol.*22*, n°12, p. 2906-2918.

[Kulshrestha et al, 2019] Kulshrestha, Juhi, Motahhare Eslami, Johnnatan Messias, Muhammad Bilal Zafar, Saptarshi Ghosh, Krishna P Gummadi, & Karrie Karahalios, «Search bias quantification: investigating political bias in social media and web search,» *Information Retrieval Journal*, vol. 22, n° 1-2, p. 188-227.

[Latour, 2005] Latour, Bruno, *Reassembling the Social. An Introduction to Actor-Network-Theory*, Oxford and New York, Oxford University Press.

[Lessig, 1999] Lessig, Lawrence, *Code and Other Laws of Cyberspace*, New York, Basic Books.

[Lonkila et al, 2020] Lonkila, Markku, Shpakovskaya, Larisa & Torchinsky, Philip, «The occupation of Runet? The tightening state regulation of the Russian-language section of the Internet», in Wijermars, Mariëlle & Lehtisaari, Katja (dir.), *Freedom of Expression in Russia's New Mediasphere,* Abingdon and New York, Routledge, p. 17-38.

[Maréchal, 2017] Maréchal, Nathalie, «Networked authoritarianism and the geopolitics of information: understanding Russian Internet policy,» *Media and Communication*, vol. 5, n° 1, p. 29-41.

[Marrese, 2007] Marres, Noortje, «The issues deserve more credit: pragmatist contributions to the study of public involvement in controversy,» *Social Studies of Science*, vol. 37, n° 5, p. 759-780.

[Mejias & Vokuev, 2017] Mejias, Ulises A & Vokuev, Nikolai E., «Disinformation and the media: the case of Russia and Ukraine,» *Media, Culture & Society*, vol. 39, n° 7, p. 1027-1042.

[Musiani, 2013] Musiani, Francesca, «Governance by algorithms,» *Internet Policy Review*, vol. 2, n° 3.

[Musiani et al., 2019] Musiani, Francesca, Loveluck, Benjamin, Daucé, Françoise & Ermoshina, Ksenia, «'Digital sovereignty': can Russia cut off its Internet from the rest of the world? ,» *The Conversation* (https://theconversation.com/digital-sovereignty-can-russia-cut-off-its-Internet-from-the-rest-of-the-world-125952, consulté le 17 février 2023).

[Napoli, 2014] Napoli, Philip M., «Automated media: an institutional theory perspective on algorithmic media production and consumption,» *Communication Theory*, vol. 24, n° 3, p. 340-360.

[Nechushtai & Lewis, 2019] Nechushtai, Efrat & Lewis, Seth C., «What kind of news gatekeepers do we want machines to be? Filter bubbles, fragmentation, and the normative dimensions of algorithmic recommendations,» *Computers in Human Behavior*, vol. 90, p. 298-307.

[Nielsen & Ganter, 2018] Nielsen, Rasmus Kleis & Ganter, Sarah Anne, «Dealing with digital intermediaries: a case study of the relations between publishers and platforms,» *New Media & Society*, vol. 20, n° 4, p. 1600-1617.

[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 and New York, Oxford University Press.

[O'Callaghan et al, 2015] O'Callaghan, Derek, Greene, Derek, Conway, Maura, Carthy, Joe & Cunningham, Pádraig, «Down the (white) rabbit hole: the extreme right and online recommender systems,» *Social Science Computer Review*, vol. 33, n° 4, p. 459-478.

[Pariser, 2011] Pariser, Eli, *The Filter Bubble. What the Internet is Hiding From You*, New York, Penguin Press.

[Pasquale, 2015] Pasquale, Frank, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Boston, MA, Harvard University Press.

[Ricci et al, 2015] Ricci, Francesco, Rokach, Lior & Shapira, Bracha, *Recommender Systems Handbook*, New York, Springer.

[Robertson et al, 2018] Robertson, Ronald E., Lazer, David & Wilson, Christo, « Auditing the personalization and composition of politically-related search engine results pages, » *Proceedings of the 2018 World Wide Web Conference*, Lyon, France, p. 955-965.

[Saurwein et al, 2015] Saurwein, Florian, Just, Natascha & Latzer, Michael, « Governance of algorithms: options and limitations, » *info*, vol. 17, n° 6, p. 35-49.

[Schroeder & Kralemann, 2005] Schroeder, Roland & Kralemann, Moritz, « Journalism ex machina—Google News Germany and its news selection processes, » *Journalism Studies*, vol. 6, n° 2, p. 245-247.

[Seaver, 2019] Seaver, Nick, « Knowing algorithms », in Vertesi, Janet & Ribes, David (dir.), *DigitalSTS. A Field Guide for Science & Technology Studies*, Princeton, NJ, Princeton University Press, p. 412-422.

[Sivetc, 2019] Sivetc, Liudmila, « State regulation of online speech in Russia: the role of Internet infrastructure owners, » *International Journal of Law and Information Technology*, vol. 27, n° 1, p. 28-49.

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

[Thorson & Wells, 2015] Thorson, Kjerstin & Wells, Chris, « How gatekeeping still matters: understanding media effects in an era of curated flows », in Vos, Timothy & Heinderyckx, François (dir.), *Gatekeeping in Transition*, Abingdon and New York, Routledge, p. 25-44.

[Thorson & Wells, 2016] Thorson, Kjerstin & Wells, Chris, « Curated flows: a framework for mapping media exposure in the digital age, » *Communication Theory*, vol. 26, n° 3, p. 309-328.

[Vendil Pallin, 2017] Vendil Pallin, Carolina, « Internet control through ownership: the case of Russia, » *Post-Soviet Affairs*, vol. 33, n° 1, p. 16-33.

[Wijermars & Lehtisaari, 2020] Wijermars, Mariëlle & Lehtisaari, Katja (dir.), *Freedom of Expression in Russia's New Mediasphere*, Abingdon and New York, Routledge.

[Wijermars, 2021] Wijermars, Mariëlle, « Russia's law 'On news aggregators': control the news feed, control the news, » *Journalism*, vol. 22, n°12, p. 2938-2954.

Chapitre 4

Les formations à la sécurité numérique : GAFAM/MAGMA, protection des données et chiffrement

Olga Bronnikova, Ksenia Ermoshina, Anna Zaytseva

> «Nous tenons à faire part de notre inquiétude face aux appels de plus en plus nombreux à limiter l'accès de la population russe à Internet. Nous craignons que cela nuise aux personnes qui tentent de s'organiser pour s'opposer à la guerre, de rendre compte ouvertement et honnêtement des événements en Russie et d'accéder à des informations sur ce qui se passe en Ukraine et à l'étranger. Ces mesures ne feraient que faciliter encore les répressions du gouvernement russe. (…) Des restrictions trop larges de l'accès de la population russe à Internet isoleraient encore davantage les militants pro-démocratie et anti-guerre, et empêcheraient les ONG, les groupes de défense des droits humains, les journalistes et les avocats, à l'intérieur et à l'extérieur de la Russie, de fournir aux citoyens des informations essentielles sur l'état actuel des choses et sur leurs droits. Contrairement à leur intention, ces actions accéléreraient ce que le Kremlin s'était donné pour objectif : un contrôle total de l'espace d'information à l'intérieur de la Russie»[1].

En lançant cette pétition le 10 mars 2022, signée par plus de cinquante associations de défense des droits humains (DDH) et des libertés Internet, l'organisation Access Now réagissait à la coupure ou aux restrictions d'accès, par certaines compagnies technologiques américaines (des FAI majeurs comme Cogent et Lumen, des plateformes comme Slack, YouTube, Google Pay et AppStore) à leurs services en Russie, au lendemain du déclenchement par le Kremlin d'une guerre sur l'ensemble du territoire ukrainien. L'appel rend visible l'antagonisme principal entre l'État et une partie de la société russe, avec pour troisième acteur clef les plateformes (GAFAM/MAGMA)[2] incarnant l'accès à la libre information, compris par les acteurs comme un outil de lutte contre la censure d'État. Notre

1 Voir la pétition originale en anglais, traduite par les auteures, à : https://www.accessnow.org/letter-us-government-Internet-access-russia-belarus-ukraine/, consulté le 16 février 2023.

2 GAFAM est un acronyme communément utilisé pour désigner cinq grandes compagnies technologiques américaines : Google, Apple, Facebook, Amazon et Microsoft. Depuis 2022, suite à l'introduction de la marque Meta pour regrouper Facebook, WhatsApp et autres services, est également utilisé l'acronyme MAGMA (Microsoft, Apple, Google, Meta, Amazon).

terrain éclaire cet antagonisme par une autre entrée : celle de la sécurité numérique, perçue comme un enjeu central des relations entre les acteurs de la société civile critique et l'État russe. Si ce dernier, prenant un tournant autoritaire et dictatorial, déploie des mesures de « sécurité informationnelle », notion qui sous-entend dans la doctrine russe le contrôle des flux d'information et le démantèlement de toute force politique ou sociale indépendante, les acteurs de la société civile sont contraints à se saisir des outils et pratiques de la sécurité numérique développés au niveau international, pour se protéger contre cette offensive.

Dans ce chapitre, nous cherchons à comprendre comment certains acteurs de la société civile russe critique en viennent à s'adapter ou à contourner les multiples contraintes d'ordre juridique, policier et technique que l'autoritarisme numérique croissant fait peser sur leurs activités, et cela via des pratiques et apprentissages évolutifs en matière de sécurité numérique. Nous prêtons à cette fin une attention particulière au rôle des outils et infrastructures fournis par les compagnies technologiques transnationales.

Notre analyse se fonde sur une enquête de terrain effectuée entre 2018 et 2022. Nous avons rencontré des formateurs en sécurité numérique et des militants pour l'Internet libre ainsi que des destinataires de ces formations en Russie même ou en exil : journalistes indépendants (médias non contrôlés par l'État), défenseurs des droits humains[3], mais aussi des militants écologistes et anti-corruption (Transparency International, Fondation de lutte contre la corruption fondée par Alekseï Navalny). Une autre partie de la société civile critique, la gauche radicale et les anarchistes, n'est pas concernée par ces formations : cible de répressions depuis plus longtemps et évoluant plus souvent dans un contexte de semi-clandestinité, elle a forgé une culture de sécurité numérique différente (caractérisée, entre autres, par une attitude critique à l'égard des GAFAM/MAGMA et par un intérêt pour les solutions *open source*). Sans être au centre de notre propos, l'exemple de ces militants nous servira parfois de point de comparaison afin de mettre en lumière la spécificité des pratiques des militants anti-corruption, défenseurs des droits humains et journalistes indépendants.

Ce chapitre est fondé sur une enquête « multi-site » qui rend visible la dimension internationale à la fois des outils et des pratiques d'auto-défense numérique. Outre Moscou et Saint-Pétersbourg, nous avons réalisé un terrain à Minsk (Bélarus) en 2019. Les formateurs bélarusses sont en effet des acteurs importants de l'écosystème des formations en sécurité au sein de l'espace post-soviétique, du fait de l'ampleur des répressions dans le pays et des savoir-faire acquis par ces formateurs. Des organisations internationales comme Access Now, Frontline

3 Pour des raisons de sécurité et compte tenu des menaces qui pèsent actuellement sur ces associations, nous ne les nommons pas ici.

Defenders, Civil Rights Center ou Reporters sans frontières constituent d'autres acteurs clés, dont nous avons interviewé des représentants, en Russie, à Prague, à Berlin, à Paris et en ligne. Nous avons noué des relations de confiance avec des porte-parole d'associations militant pour l'Internet libre, comme Roskomsvoboda, le Centre des droits numériques, la Société de Protection de l'Internet, mais aussi avec des membres de la Serre des technologies sociales (Teplitsa), projet de *civic tech* qui propose des solutions technologiques répondant aux problèmes politiques et organisationnels des ONG en Russie. Depuis 2019, dans un contexte de répressions de plus en plus violentes, et sans précédent à partir du 24 février 2022, nombre de ces militants ont dû quitter la Russie. Nous les avons rencontrés dans les lieux d'exil de Varsovie à Tbilissi, en passant par Vilnius.

Nous avons en outre participé à des événements organisés par nos interlocuteurs sur ces questions, comme le forum Privacy day à Minsk et Moscou et Internet sans frontières dans divers lieux d'exil, à des formations en sécurité numérique (en ligne et hors ligne) mises en place par différentes organisations, à un hackathon coordonné par la Société de Protection de l'Internet dont l'un des objectifs était de proposer un dispositif de sécurité, etc. Aux entretiens semi-directifs et observations participantes s'ajoutent le suivi des chaînes Telegram de quelques acteurs importants des libertés et de la sécurité numérique, une analyse de guides en sécurité numérique à destination de la société civile, ainsi que des vidéos de conseils en sécurité diffusées sur YouTube par les organisations mentionnées. Ces terrains ont également été mis en perspective avec une enquête menée dans le cadre du projet européen Nextleap en 2016-2018 sur les usages des messageries sécurisées de bout en bout [Ermoshina & Musiani, 2018 ; 2022] ainsi qu'une étude sur les évolutions des formats des formations en sécurité numérique qui inclut une série d'entretiens avec des formateurs menés en 2020.

Pour mieux cerner les évolutions des pratiques, nous analysons d'abord comment, dans le contexte politique russe, la notion même de « sécurité numérique » s'est définie par contraste avec celle de « sécurité de l'information » forgée dans le discours officiel russe et dans le but de désigner essentiellement les pratiques d'auto-défense vis-à-vis de l'État. Dans un deuxième temps, nous expliquons l'écosystème des formations en sécurité, distribué entre plusieurs types d'acteurs et d'échelles géographiques, ainsi que les méthodes et les formats évolutifs de ces formations, à l'aune de la prolifération des contraintes pesant sur la société civile critique. Enfin, sont étudiées les plus récentes recompositions des pratiques de sécurité numérique à la suite du début de l'invasion russe de l'Ukraine, l'instauration *de facto* de la loi martiale en Russie et l'exil massif de nombreux acteurs concernés par notre recherche.

« Sécurité de l'information » versus « sécurité numérique »

Pour comprendre la spécificité des apprentissages de la « sécurité numérique » et sa construction incertaine dans les discours et pratiques des acteurs de la société civile, il convient d'abord de l'inscrire dans le contexte d'adversité croissante qui la façonne. Dans les milieux rencontrés, le terme de « sécurité numérique » (*cifrovaâ bezopasnost'*), calqué sur le terme anglais « *digital security* », est davantage utilisé que celui de « sécurité de l'information » (*informacionnaâ bezopasnost'*). Or, c'est ce dernier qui prédomine de manière plus générale : les statistiques du moteur national de recherche Yandex donnent respectivement 17 000 résultats contre 8 000. Cela peut s'expliquer par le fait que la « sécurité de l'information » est un terme plus englobant qui désigne d'après la Wikipédia russe « la pratique consistant à empêcher l'accès, l'utilisation, la divulgation, l'altération, l'étude, l'enregistrement ou la destruction non autorisés d'informations » et ce, « quelle que soit la forme que peuvent prendre les données, électronique ou physique »[4]. La « sécurité numérique », pour sa part, ne renverrait qu'aux « différentes manières de protéger son compte Internet et les fichiers de son ordinateur contre l'intrusion d'un utilisateur externe ou d'un hacker »[5].

« Sécurité de l'information »

En contexte, les deux termes semblent néanmoins souvent interchangeables, à l'exception d'emplois spécifiques du terme « sécurité de l'information » dans des textes officiels relevant de l'État, notamment dans les Doctrines de la sécurité de l'information datant de 2000 et de 2016. La seconde « Doctrine », à la différence de la première, s'appuie sur le concept de sécurité nationale (2015) adopté par le Conseil de sécurité d'État à la suite de l'annexion de la Crimée, du déclenchement de la guerre dans le Donbass et de plusieurs trains de sanctions occidentales. Le discours étatique sur la sécurité de l'information a également été façonné par les révélations de Snowden de 2013. Mettant en évidence la surveillance de masse effectuée par la NSA depuis les États-Unis à travers le monde, ces révélations ont apporté une nouvelle pièce à l'argumentaire des autorités russes visant à maîtriser le Runet et à le protéger contre des menaces extérieures devenues plus plausibles. Cette revendication d'une autorité étatique sur le cyberespace semble faire désormais partie d'un cadre d'interprétation global de la cybersécurité qui atteste d'une nette tendance à la militarisation des méthodes et va parfois jusqu'à annoncer une course aux cyber-armements [Ristolainen, 2017].

4 https://ru.wikipedia.org/wiki/Информационная_безопасность (consulté le 16 février 2023).

5 https://ru.wikipedia.org/wiki/Информационная_безопасность (consulté le 16 février 2023; notons que cette page Wikipedia n'existe qu'en tant que page automatiquement traduite depuis la page anglophone « *digital security* ».)

L'approche russe s'inscrit dans cette tendance générale. Le terme russe désignant le « cyberespace » semble pourtant de prime abord spécifique : la notion d'« espace informationnel » (*informacionnoie prostranstvo*), ne se limitant pas à Internet et aux réseaux numériques, englobe tous les supports et médias (presse écrite, audiovisuel). Ainsi, ce « n'est pas un champ d'action en soi, mais le prolongement des divers terrains d'action politiques, économiques ou militaires de l'État » [Limonier, 2016, p. 132]. Or, dans la doctrine américaine le « *cyberspace* » et la cybersécurité englobent également des niveaux différents : ceux-ci vont de la couche des infrastructures au *soft powe*r des discours médiatiques, voire cinématographiques. La véritable spécificité russe réside en effet dans la genèse défensive et réactive du terme de « sécurité de l'information » qui est construit en rapport avec la notion de « confrontation informationnelle » (*informacionnoe protivoborstvo*) [Doktrina, 2016]. Cette confrontation oppose la Russie et les États membres de l'OTAN, en premier lieu les États-Unis, des pays mentionnés dans le texte de la Doctrine de la sécurité de l'information comme « certains États » qui utilisent leurs « technologies de l'information avancées » afin de « nuire à la stabilité stratégique », d'employer des moyens de « surveillance technique contre les organes de l'État russe, les organisations scientifiques et les entreprises du complexe militaro-industriel », mais aussi de « déstabiliser la situation politique et sociale interne », de « porter atteinte à la souveraineté et à l'intégrité territoriale » et d'« éroder les valeurs spirituelles et morales traditionnelles russes ». Aux fins de cette déstabilisation, l'ennemi (« certains États » et leurs « services spéciaux ») utilise des « moyens d'information et d'influence psychologique » et agit par l'intermédiaire des « organisations religieuses, ethniques, de défense des droits de l'homme, ainsi que des groupes individuels de citoyens ». Il fait « un large usage des technologies de l'information », notamment des médias, qui diffusent une « évaluation biaisée de la politique d'État de la Fédération de Russie » [Doktrina, 2016].

Ainsi, le discours étatique sur la sécurité de l'information, tout comme les actes législatifs et les pratiques judiciaires qui en découlent (que nous décrivons plus loin), érigent *in fine* « l'espace informationnel » en champ de bataille de première importance. Dès lors, les infrastructures de l'Internet global (dominées par les compagnies enregistrées aux États-Unis), mais aussi des médias (étrangers ou indépendants de l'État russe) et des organisations de la société civile, sont considérés comme autant d'outils de diversion entre les mains de certains États hostiles, menaçant la sécurité nationale et visant, plus globalement, à déstabiliser l'ordre mondial.

Afin de les contrer, la souveraineté technologique est affirmée comme une des priorités de la sécurité nationale et de l'information. Or, sa mise en place étant liée à des efforts difficiles et des investissements importants sur le moyen et le

long termes, ce sont, *de facto*, les acteurs de la société civile critique qui deviennent les cibles les plus faciles à atteindre dans la lutte menée au nom de la sécurité nationale. Dans ce contexte de souverainisation numérique voulue par l'État [Bronnikova et al., 2022], ces acteurs, se sentant ciblés à partir du milieu des années 2010, s'appuient précisément dans leur quête de sécurité ou de simple survie face à l'État sur des services et réseaux numériques fournis par les multinationales américaines, ces dernières bénéficiant de plus d'autonomie vis-à-vis des autorités russes, au moins dans un premier temps.

« Sécurité numérique »

Avec le développement des pratiques de surveillance et une répression accrue, les militants de la société civile se tournent ainsi de plus en plus vers des plateformes étrangères, considérées comme plus sécurisées que leurs homologues russes (VKontakte, Mail.ru, Yandex). La coercition autoritaire touche des groupes et collectifs militants plus variés qu'avant. À partir du début des années 2010, l'éventail des répressions ne cesse de s'élargir, donnant lieu à tout un assemblage de mesures juridiques et techniques appliquées aux journalistes des médias indépendants, ONG et militants des droits humains. Les mobilisations contre les élections truquées en 2011-2012, que les autorités russes accusent d'avoir été fomentées par les gouvernements et fondations à l'étranger, aboutissent à une hyperactivité du législateur en termes de lois liberticides.

En 2018, la FIDH recense pour la Russie « cinquante lois anti-démocratiques » entrées en vigueur en six ans entre 2012 et 2018 [FIDH, 2018], parmi lesquelles la loi sur les « agents de l'étranger » qui vise les organisations financées totalement ou en partie depuis l'étranger, les amendements à la loi sur le terrorisme et l'extrémisme qui sont systématiquement utilisés contre les militants contestataires, la loi limitant les rassemblements publics, ou encore la loi sur les « organisations indésirables » qui permet d'interdire les activités des organisations étrangères gênantes. Si ces lois ne concernent pas directement l'espace numérique, ce dernier est passé au crible afin d'incriminer les professionnels de l'espace public prenant ouvertement position contre l'arbitraire des autorités ou même échangeant de manière confidentielle sur des plateformes comme VKontakte, de plus en plus investies par les forces de l'ordre. En effet, des associations de défense des libertés numériques, telles que la Société de protection de l'Internet et Agora (renommée Setevye Svobody - Libertés Numériques), recensant depuis plusieurs années les violations des droits numériques en Russie, pointent le rôle joué par les plateformes russes dans la mise en place de la surveillance et du contrôle

de l'expression[6]. Des milliers de cas d'incrimination administrative ou pénale pour de simples « *reposts* » ou même pour des informations qualifiées d'extrémistes échangées en privé sont signalés par ces associations. Cette répression numérique a pris une ampleur inédite après le début de l'invasion de l'Ukraine par la Russie, le 24 février 2022. Depuis lors, des personnes ordinaires, non militantes, sont pénalisées par milliers pour avoir posté dans leurs réseaux sociaux des messages dénonçant la guerre.

Les militants et journalistes indépendants en Russie font, en outre, l'objet de perquisitions violentes lors desquelles tous les appareils sont systématiquement saisis. Le chapitre 8 de cet ouvrage retrace en détail la forme que prennent ces perquisitions et leurs conséquences. Elles interviennent souvent à la suite de la participation à des actions contestataires de militants identifiés grâce aux systèmes de surveillance, très développés dans les grandes villes russes, ou à la circulation d'images sur les réseaux sociaux. Les données personnelles non ou mal protégées, mettant en danger des personnes ressources pour les journalistes et des bénéficiaires d'aide en ce qui concerne les ONG, se retrouvent régulièrement entre les mains des autorités et permettent l'amplification des répressions.

Face à ces dangers, les défenseurs des droits numériques et les formateurs en sécurité, mais aussi les blogueurs d'opposition, appellent les acteurs de la société civile à se retirer des services russes, au premier chef de VKontakte, au profit de leurs homologues transnationaux tels que Facebook ou Twitter, ou au profit de plateformes décentralisées et auto-hébergées comme Mastodon.

Ainsi, à partir de 2016-2017, les défenseurs des droits humains et les journalistes indépendants embrassent une vision de la « sécurité numérique » conçue comme l'ensemble des pratiques d'auto-défense vis-à-vis de l'État russe, que les milieux de la gauche radicale avaient intégrée dès 2010-2012. Or, à la différence de ces derniers, qui aspirent à des solutions *open source* comme XMPP (protocole de messagerie instantanée), Tor (réseau de communications décentralisé et anonymisé), PGP (logiciel de chiffrement) ou Briar (messagerie chiffrée distribuée) et rejettent les solutions privées des compagnies technologiques américaines, les défenseurs des droits humains perçoivent progressivement ces dernières comme des alliés « naturels » dans leur lutte pour la survie. La perception positive des services proposés par les acteurs de la Big Tech est à mettre en relation avec les efforts que ces dernières déploient, notamment depuis les révélations de Snowden, pour se construire une image de défenseurs des droits humains (Google est particulièrement engagé dans ce processus) mais aussi avec les conseils apportés par des experts internationaux en sécurité numérique qui les présentent comme

6 Par exemple, la Carte des répressions mise en place par la Société de protection de l'Internet depuis 2017 (https://ozi-ru.org/proekty/Internet-repressii/karta/, consulté le 16 février 2023).

une alternative fiable aux services contrôlés par les États autoritaires [Bronnikova & Zaytseva, 2021]. La confiance repose sur le suivi régulier des rapports de transparence de Google et des autres GAFAM/MAGMA. Contrairement aux critiques émises par des militants européens ou américains contre ces plateformes numériques dominantes, les utilisateurs provenant des pays autoritaires de l'espace post-soviétique relativisent les risques associés à leur usage, compte tenu de la confrontation en cours entre, d'un côté, la Russie et le Bélarus, et de l'autre les États et entreprises occidentaux. Comme le note un formateur bélarusse ayant travaillé pour plusieurs pays de l'espace postsoviétique, dont la Russie, « alors que pour les pays (…) participant à l'alliance des services de renseignement des '*five eyes*'[7], 80 à 90% des demandes d'information des autorités sont satisfaites, pour la Russie, ces chiffres ne représentent que quelques pourcents et pour le Bélarus 0% »[8].

Au-delà même de cette préférence pour les services des GAFAM/MAGMA en Russie ou dans d'autres pays post-soviétiques, le développement des compétences en sécurité numérique et physique est progressivement érigé en priorité par les grandes organisations et les ONG internationales spécialisées dans le soutien à la société civile indépendante. Cette dernière devient en effet une des cibles privilégiées des États ainsi que de diverses milices para-étatiques dans des contextes nationaux dits « à hauts risques », terme employé pour désigner plusieurs régimes autoritaires, comme ceux de l'Iran, la Chine, le Pakistan, le Vénézuela, l'Erythrée, et d'autres. Les risques informatiques, mais aussi physiques et psychologiques, subis par les acteurs de la société civile ont conduit les ONG internationales spécialisées en protection des défenseurs des droits humains ainsi que dans le domaine des libertés numériques (comme Frontline Defenders, Access Now ou Electronic Frontier Foundation) à multiplier les formations en sécurité ainsi qu'à inciter les bailleurs de fonds (notamment, Open Technology Fund, Ford Foundation ou encore le bureau du département d'État des États-Unis pour la démocratie, les droits humains et le travail - DRL) à financer massivement ce genre de formations.

Formations en sécurité numérique

Ces formations pour la société civile s'inscrivent donc dans un écosystème complexe combinant les échelles locale, nationale et internationale. Après avoir décrit ce système tel qu'il se constitue à partir des années 2010 ainsi que ses

7 Une alliance qui regroupe cinq pays anglophones (le Royaume-Uni, les États-Unis, le Canada, l'Australie et la Nouvelle-Zélande), avec pour but l'échange de renseignements.

8 Entretien avec un formateur en sécurité numérique, mars 2019, Minsk.

acteurs clefs, nous nous penchons sur les modes d'apprentissage et les méthodes évolutives, qui se forgent via une série d'épreuves pratiques et d'échecs.

Un écosystème

Nous pouvons distinguer au moins trois types d'acteurs au sein de l'écosystème des formations en sécurité numérique (en dehors de leurs bénéficiaires, les associations et militants) : les formateurs, les ONG spécialisées et les organisations-bailleurs de fonds. Les experts et formateurs en sécurité numérique travaillent pour la plupart sur le mode du consulting *outsourced*. En effet, très peu d'ONG et de médias russes peuvent se permettre de salarier leur propre spécialiste en sécurité numérique (voire tout simplement d'avoir un administrateur système) : leurs financements sont trop réduits et sont fléchés « par projet », ce qui ne permet pas de financer un salarié sur une période indéfinie.

Les relations entre ces experts et les ONG sont en effet médiées par les organisations internationales spécialisées dans le soutien aux défenseurs des droits humains et aux journalistes dans le monde entier, et qui sont essentiellement de deux types. Premièrement, des organisations, tant gouvernementales que non gouvernementales[9], jouant le rôle de bailleurs de fonds octroyant des financements de quelques mois jusqu'à plusieurs années pour tel ou tel programme réalisé dans le cadre d'une ONG locale et ayant un droit de regard sur les dépenses budgétaires de celle-ci. Ces organisations peuvent préconiser à une ONG une formation ou un audit en sécurité numérique et la diriger vers une des ONG spécialisées dans la sécurité numérique, lesquelles constituent le deuxième type principal d'acteurs internationaux. Il s'agit d'organisations américaines (Electronic Frontier Foundation, Access Now), canadiennes (eQualit.ie) et européennes (Huridocs, Tactical Tech, Frontline Defenders, Civil Rights Defenders), qui opèrent au niveau international et se spécialisent dans le soutien technique (y compris informatique) et juridique aux défenseurs des droits humains et journalistes. Sans être bailleurs de fonds, elles fournissent aux militants des outils de protection, y compris numériques, une assistance pratique à long terme, des infrastructures fiables (hébergement, maintenance des serveurs mail ou messagerie, mise en place des VPN), des formations et de petites subventions. Elles organisent des événements spécialisés, des « formations pour formateurs », des conférences et forums. Le soutien en sécurité numérique octroyé à des ONG peut prendre plusieurs formes, allant de conseils ponctuels donnés par des experts en sécurité numérique rémunérés par une des ONG spécialisées dans

9 Par exemple la Fondation Soros, le Norwegian Helsinki Committee, Freedom House, la Commission européenne, l'ambassade britannique, l'ambassade de Norvège, l'UNHCR (Haut Commissariat des Nations unies pour les réfugiés), etc.

la protection des DDH que nous avons mentionnées, à des formations plus ou moins généralistes ou spécialisées, en passant par des « fellowships » en sécurité informatique, ou l'aide plus durable d'un expert extérieur qu'une ONG peut rémunérer sur cette période grâce à un financement obtenu de la part du bailleur de fonds, pour un objectif précis. Enfin, au-delà des ONG internationales, comme nous l'avons déjà démontré [Bronnikova & Zaytseva, 2021], de grandes entreprises de l'informatique (comme Google ou Microsoft) peuvent jouer un rôle dans l'équipement des associations en outils de bureautique mais aussi de sécurité numérique, dans le cadre de programmes comme TechSoup coordonné (avant février 2022) en Russie par l'association La Serre des technologies sociales.

Les associations ne formulent pas toujours spontanément des demandes de formation précises. C'est souvent un incident de sécurité (fuite d'informations sensibles à la suite d'un hameçonnage, attaques DDoS révélant des vulnérabilités du site web, etc.) qui en est le déclencheur : l'aide d'urgence d'une organisation comme Access Now ou Frontline Defenders peut alors être sollicitée. Ces organisations envoient ensuite leur conseiller en sécurité numérique sur place, afin qu'il repère les points sensibles et besoins de protection. Cette observation par un conseiller peut aboutir à une demande de subvention auprès du bailleur de fonds et/ou à une formation en sécurité numérique proposée par l'organisation.

Formats et méthodes

Les formations peuvent se dérouler selon plusieurs formats. Soit il s'agit d'une formation thématique destinée à plusieurs organisations (représentées par un ou plusieurs membres, dont souvent un administrateur IT) ou militants individuels, focalisée sur un défi particulier dont on constate l'importance sur le terrain (par exemple, « être journaliste dans des zones de conflit » ou « voyage d'affaires à l'étranger »). Soit il s'agit d'une formation destinée à une seule association dans son ensemble, qui peut durer plusieurs jours : le formateur se rend alors sur place et commence par un audit des problèmes de sécurité (analyse des risques et évaluation des besoins). Ce processus consiste à parler séparément avec la direction de l'organisation et son directeur IT, avant de faire le tour de différents collaborateurs afin d'établir une liste des points sensibles, puis de passer à un *debriefing* collectif. Ce genre de formation débouche sur la mise en évidence d'un « modèle de menaces » (*threat model*) et la constitution d'un « protocole de sécurité » propre à l'organisation, que ses membres sont invités à respecter :

> « Nous avons eu un audit très rigoureux concernant nos communications internes, l'utilisation des smartphones et ordinateurs, le travail avec les messageries instantanées, le chiffrement des données et des appareils. On nous

> a fortement recommandé un certain type de messageries instantanées avec chiffrement, par exemple Signal ou Telegram. La messagerie de VKontakte.ru a été définitivement interdite, alors que jusqu'à il y a trois ans, certains de nos employés utilisaient VKontakte pour communiquer. L'utilisation de smartphones pour des communications sensibles a été bannie. Si une personne se met à parler au téléphone, elle peut être réprimandée, et le protocole à suivre lui être rappelé»[10].

Néanmoins, mises à part les réprimandes, les organisations ont peu de moyens pour sanctionner les fautifs[11]. En effet, compte tenu d'un manque notable de ressources humaines, d'un *turn-over* important dans les associations, de la part considérable du bénévolat, les sanctions comme le licenciement, la suppression des primes ou la restriction du périmètre d'accès à l'information, habituelles dans le secteur privé, ne sont ici guère applicables.

Dès lors, le travail de persuasion, la pédagogie personnelle et adaptée au cas par cas, déployée par le formateur, acquiert une importance cruciale. Certains disent que pour forger des recommandations qui marchent et un protocole de sécurité qui sera suivi, il importe de les élaborer à partir de l'histoire des incidents de sécurité, individuelle ou propre à l'organisation. C'est ce vécu personnel des failles de sécurité et des conséquences qu'elles ont engendrées, et non pas le niveau de compétence technique des usagers, qui façonne en premier lieu leurs manières de mettre en pratique les outils de protection numérique [Kang et al., 2015]. Ainsi, des enseignements tirés d'exemples réels d'incidents de sécurité (anonymisés) alimentent les formations et les manuels de sécurité numérique. Diverses mises en situation et jeux de rôle nourrissent également ces formations, aboutissant même à une méthodologie innovante de «sécurité holistique». Cette méthodologie, promue notamment par des organisations internationales comme Frontline Defenders, signale la volonté de s'émanciper des méthodes de *risk management* développées au sein du secteur privé, jugées peu adaptées à l'univers de la militance et des ONG DDH.

L'approche en termes de «sécurité holistique» constitue en effet un résultat du travail réflexif et critique mené par la communauté internationale des formateurs, qui échangent leurs expériences lors des conventions spécialisées comme l'Internet Freedom Festival ou le RightsCon (organisé par l'ONG Access Now). L'approche holistique se distingue notamment de l'approche «orientée outil» (*tool-centered approach*) qui construisait les formations avant tout autour de recommandations d'outils ou de protocoles de chiffrement spécifiques (par exemple Tor, Signal ou PGP), indépendamment du contexte précis et du modèle de menace des personnes en question. Le cap a dès lors été mis sur «l'intégration des questions

10 Entretien avec un employé d'une ONG internationale, août 2019, Moscou.

11 Il y a néanmoins quelques rares cas de sanctions pour faute grave causant une faille de sécurité.

d'autodéfense numérique dans des approches plus globales de sécurité» [Hankey & Clunaigh, 2013]. Le rôle central du «numérique» dans les formations plus anciennes a été amplement critiqué par les formateurs, qui ont commencé à prioriser les aspects psychologique, juridique et physique, en présentant la sécurité non pas en tant qu'objet stabilisé et bien défini, mais en tant que processus «en construction permanente», relationnel et contextuel [Ermoshina & Musiani, 2018]. Cela a, à son tour, eu un impact sur les financements et le contenu des supports éducatifs (guides de bonnes pratiques). L'approche holistique a été très bien reçue par les formateurs russes, entre autres, compte tenu du contexte juridique et politique du pays. Dans ce contexte, le risque le plus répandu n'est pas une attaque informatique sophistiquée, mais la saisie des appareils électroniques et l'usage de la torture et de diverses formes de pression psychologique pour accéder aux données. Ainsi, les aspects psychologiques, physiques et juridiques ont commencé à occuper une place centrale dans les formations, qui se sont dès lors centrées sur des mises en situation concrète.

> «Je propose un exercice à ceux que je forme : on vous force la porte de votre bureau, et qu'est-ce qui se passe ensuite, des points de vue différents ? Le logiciel VeraCrypt est certainement une partie de votre défense et pas la moindre, mais probablement, il s'agit aussi de votre porte qui est forcée, et de la surveillance vidéo qui aurait enregistré tout ça et l'enverrait quelque part chez la compagnie de sécurité, pour qu'il y ait une trace vidéo de cette violence. Du point de vue psychologique, comment réagit-on au stress engendré par cette violence ? Puis du point de vue juridique, si nous avons une clef usb dans la poche, est-ce que les policiers, avec leur permis de perquisition, ont le droit de fouiller nos poches ?»[12]

À l'issue de ces formations, les formateurs peuvent, par exemple, non pas préconiser d'employer des outils cryptographiques complexes, mais tout simplement d'installer une porte blindée solide et une caméra de surveillance à l'entrée du bureau.

Après le 24 février 2022 : nouveaux défis et recomposition des pratiques

Déjà difficile avant 2022, la situation du point de vue des droits humains et politiques en Russie s'est encore aggravée après le 24 février. Les acteurs de la société civile ont été accablés par de nouvelles lois et régulations en matière d'expression publique. Une censure spécifique a été instaurée pour toutes les questions touchant de près ou de loin à l'invasion de l'Ukraine. Sur fond de guerre, d'autres lois ont été adoptées comme la loi interdisant la «publicité» des

12 Entretien avec un formateur en sécurité numérique et physique, mars 2020, Paris.

identités LGBTQ+ auprès de toute la population russe et non plus seulement des mineurs. La surveillance des discussions en ligne susceptibles de porter atteinte à l'intégrité du territoire russe a été renforcée. Enfin, des répressions sans précédent depuis la fin de l'URSS s'abattent aujourd'hui sur tous ceux et celles qui critiquent la politique intérieure et/ou étrangère russe.

L'anonymat et la vie privée en débat

Dans ce contexte, la question de l'anonymat, débattue dans les milieux militants bien avant 2022, a été soulevée de manière radicale par des formateurs en sécurité numérique. En effet, les formateurs semblent craindre de se retrouver, à leur tour, dans le collimateur de l'État, à l'image des avocats défendant les personnes jugées et qui sont menacés pour « discréditation de l'armée russe » après avoir prononcé le mot « guerre » pendant les procès[13]. Ils s'inquiètent également pour la sécurité des personnes formées qui « croient encore que nous devons rester comme des chevaliers avec la visière ouverte »[14]. Une fois exilées, ces personnes pensent être protégées de l'arbitraire des autorités russes : « elles ne prennent absolument pas en compte les dangers que représentent leurs publications sur VKontakte pour leur entourage resté en Russie ou pour les personnes qui re-postent leurs publications. Elles ne comprennent pas non plus que la pression exercée sur leurs proches restés en Russie est un moyen d'atteindre les exilés »[15]. Certains militants préparent leurs proches à l'éventualité de perquisitions : « J'ai envoyé à ma mère des instructions sur les perquisitions. Je l'ai abonnée à OVD Info et à Meduza. Parce qu'ils continuent à vous terroriser de toute façon, même quand on pense être à l'abri »[16].

Les exilés russes deviennent parfois victimes de répressions transnationales mises en place par l'État impliquant la surveillance en ligne, phénomène qui a déjà été étudié notamment pour les militants iraniens exilés, ciblés par les autorités à la fois pour les discréditer à l'échelle internationale et couper leur lien avec les contacts restant au pays [Michaelsen, 2018]. Une citoyenne russe s'est vue refuser les services consulaires de l'Ambassade de Russie au Canada pour avoir

13 « Presledovanie rossijskih advokatov posle načala Rossiej vojny protiv Ukrajny [La persécution des avocats russes après le commencement par la Russie de la guerre contre l'Ukraine], Pravo na zaŝitu, 16 juin 2022, https://www.defenders.by/presledovanie_rus_advokatov (consulté le 16 février 2023); Bontsler, Maria, « Ne nadjtes' - â ne uedu » štraf advokaty is Kaliningrada po donosu sud'y [« Ne comptez pas sur mon départ ». Une avocate de Kaliningrad écope d'une amende suite à une dénonciation par le juge], Sever.Realii, 24 août 2022, https://www.severreal.org/a/ne-nadeytes-ya-ne-uedu-shtraf-advokatu-po-donosu-sudi/31990844.html (consulté le 16 février 2023).

14 Entretien avec un formateur russe en ligne, octobre 2021.

15 *Ibid.*

16 Entretien avec une militante du mouvement anti-guerre, septembre 2022, Tbilissi.

participé au groupe Facebook « Nous sommes pour une Russie meilleure » animé par des exilés russes, proches de l'équipe de Navalny. Le refus a été justifié par le danger que cette exilée représente pour la sécurité de la Russie[17]. D'autres exilés, parmi lesquels des défenseurs des libertés numériques (comme le directeur de la Société de protection d'Internet) sont recherchés par les autorités russes, pour avoir « enfreint à plusieurs reprises la loi pénalisant la discréditation de l'armée russe » dans des émissions diffusées sur YouTube et sur leurs chaînes Telegram. De telles accusations peuvent poser problème aux personnes se trouvant dans des pays de l'espace post-soviétique, comme la Géorgie, l'Arménie et les pays d'Asie centrale, car ils risquent le renvoi en Russie. Mais elles sont aussi potentiellement problématiques pour des personnes résidant dans les pays de l'Union européenne lors de déplacements dans des pays jugés peu sûrs, comme la Turquie par exemple.

Il y a deux ans encore, les formateurs prônaient un usage précautionneux des réseaux sociaux reposant sur la publication limitée de données et informations personnelles [Bronnikova & Zaytseva, 2022] ; aujourd'hui, ils préconisent l'anonymat maximal pour toute personne craignant des persécutions en Russie, même quand il s'agit de personnes exilées.

Cette recommandation ne suscite pas beaucoup d'enthousiasme chez les journalistes notamment, pour lesquels l'anonymat équivaut à la fin de leur carrière, d'autant plus après la fermeture de nombreux médias russes indépendants en Russie (*Écho de Moscou*, *Dojd* avant sa recomposition à Riga et ensuite à Amsterdam). En effet, plusieurs journalistes ont été obligés de lancer sur YouTube leurs propres projets dont le succès repose entièrement sur leur renommée avant la guerre. Cette tactique est souvent appelée « sécurité par publicité » et peut s'avérer efficace, notamment en cas de poursuites ; la notoriété peut jouer un certain rôle dans le succès d'une campagne de soutien et dans la collecte de fonds pour les frais juridiques.

En revanche, les militants, surtout ceux restés en Russie, adoptent massivement la recommandation d'anonymat en raison des dangers qu'encourt aujourd'hui toute personne opposée à la guerre en Russie. Cela implique, entre autres, une migration vers des messageries chiffrées qui permettent de créer des comptes sans renseigner de numéro de téléphone : « Je vois aujourd'hui de plus en plus de militants anti-guerre qui utilisent [la messagerie] Element. Ils ont décidé

17 « Posol'stvo RF v Kanade otkazalo rossiânke v prieme iz-za "ugrozy bezopasnosti". Povodom dlâ otkaza stala podpiska na gruppu "Za prekrasnuû Rossiû buguŝego". » [« L'Ambassade de la Fédération de Russie au Canada a refusé d'accueillir une citoyenne russe pour « menace à la sécurité ». En cause, sa souscription au groupe « Pour la merveilleuse Russie du futur »], *Meduza,* 27 janvier 2023, https://meduza.io/news/2023/01/27/posolstvo-rf-v-kanade-otkazalo-rossiyanke-v-prieme-iz-za-ugrozy-bezopasnosti-povodom-dlya-otkaza-stala-podpiska-na-gruppu-za-prekrasnuyu-rossiyu-buduschego (consulté le 16 février 2023).

d'eux-mêmes que ce serait leur moyen de communication en interne. C'est très prometteur, j'espère que ça rentrera dans les pratiques après la fin de tout ça »[18]. Les formateurs notent avec satisfaction que les militants et ONG en Russie ont enfin commencé à prendre au sérieux la vérification de l'identité des participants et le contrôle des conditions matérielles (accès à la salle, présence des caméras de surveillance). Tout porte à croire que la guerre constitue un point de bascule obligeant les militants, restés sceptiques quant à la mise en œuvre de recommandations maintes fois répétées en matière de sécurité numérique, à s'approprier sur le tas des outils et pratiques d'auto-défense vis-à-vis de l'État russe. Cet effet de « culture de la sécurité induite par la crise » a déjà été observé lors de notre enquête sur les journalistes exilés de Crimée après son annexion par la Russie en 2014. Lors des entretiens, ces journalistes témoignaient du rôle de l'annexion comme point de bifurcation qui les avait conduit à enfin « prendre au sérieux » les conseils des formateurs [Ermoshina, 2023].

Dans l'exil, certaines habitudes restent cependant prégnantes. Des bénévoles russes des associations d'aide aux réfugiés ukrainiens continuent par exemple d'utiliser les services de Yandex (messagerie), notamment pour communiquer au sujet des réfugiés ayant quitté les territoires occupés par la Russie. D'autres rechignent à l'usage de Signal et de messageries sécurisées en général pour communiquer avec des financeurs potentiels, dont certains ont été reconnus « organisations indésirables » en Russie, en leur préférant Telegram ou WhatsApp. Nombreux sont ceux qui gardent encore un numéro de téléphone russe à l'étranger auquel sont rattachés les différents services et outils de communication, et cela en dépit des incidents de sécurité identifiés dès 2016 au sein de l'équipe d'Alekseï Navalny lorsqu'un accès aux échanges sur Telegram a été obtenu par les autorités grâce aux duplicata de carte-sim[19]. Un autre aspect qui implique une certaine perte de vigilance numérique est le temps : dans notre étude sur la Crimée, nous avons pu constater que les rapports à la fois à l'espace et à la temporalité de l'exil (notamment, pour des conflits longs, comme l'occupation de la Crimée) contribuaient à une certaine fatigue et à une baisse de l'attention, induisant un retour aux outils et pratiques d'avant la crise[20].

Des conflits autour de la confidentialité et de la sécurité des règlements internes aux associations éclatent régulièrement : entre ceux qui prônent la nécessité de se méfier des dangers, même très hypothétiques, d'une part, et les adeptes du « nous devons afficher notre transparence », d'autre part. À cet égard, les formateurs soulignent qu'il s'agit là d'un « débat éternel » dans lequel les personnes novices en

18 Entretien avec un formateur russe, novembre 2022, en ligne.

19 https://medialeaks.ru/2904yut_durov/ (consulté le 16 février 2023).

20 *Ibid.*

matière d'engagements associatifs[21], qui n'ont pas été marquées par l'expérience des années de perquisitions et de répressions, tendent invariablement à défendre la position du « nous n'avons rien à cacher » [Bronnikova & Zaytseva, 2021 ; 2022]. Les droits à l'anonymat et à la vie privée sur Internet n'étaient pas, jusqu'à très récemment, considérés comme des valeurs à défendre, hormis dans les cercles des militants de la gauche radicale, qui par ailleurs, et depuis au moins 2010, avaient essayé de promouvoir une « culture de la sécurité » ; et tout cela en dépit des efforts de publicisation de ces notions par des défenseurs des droits numériques, comme Roskomsvoboda et les formateurs de sécurité numérique[22]. Le « paradoxe de la vie privée », observé par des chercheurs en sciences informatiques au sujet des usagers lambda (« *lay users* »), semble ainsi s'appliquer aux militants et journalistes étudiés : alors que les usagers sont constamment mis en alerte, par différents experts et militants, quant aux menaces à la vie privée dans les environnements numériques (notamment, sur les réseaux sociaux), ces risques restent à leurs yeux abstraits et incertains. Ils connaissent mal les technologies de protection de la vie privée et les utilisent très peu. En revanche, ils tendent à révéler beaucoup d'informations personnelles sans y être contraints [Carey & Burkell, 2009].

À ceci il faut ajouter que dans le contexte très particulier de l'exil, les personnes forcées de quitter leur pays et d'abandonner leur vie antérieure ressentent généralement le besoin pressant de garder un certain nombre de repères leur permettant de continuer à vivre. Les groupes et tchats Telegram ou WhatsApp avec des personnes proches, restées en Russie ou disséminées à travers le monde, ont cette fonction d'ancrage et de stabilité dans des conditions sans cesse changeantes : « il ne faut pas mettre la pression sur les gens. Après tout, ces groupes WhatsApp c'est à peu près la seule chose qu'il leur reste dans ce nouveau monde »[23].

Le nouveau rôle des organisations russes localisées à l'étranger

Dans ce contexte, les ONG russes de défense des libertés numériques et d'accompagnement technologique des militants, désormais à l'étranger, acquièrent un rôle pivot de relais entre les acteurs de la société civile restés en Russie et le reste du monde. Si des ONG comme la Société de protection d'Internet ou Roskomsvoboda n'ont jamais caché leur caractère politique, ou du moins, leur

21 Dans l'association où nous avons réalisé l'observation participante, fondée en avril 2022 dans un des pays de l'exil russe et d'arrivée des réfugiés ukrainiens, la majorité des bénévoles n'avait aucune expérience préalable du travail ou du bénévolat dans le domaine de la défense des droits humains.

22 https://roskomsvoboda.org/about/en/ (consulté le 16 février 2023).

23 Entretien avec un formateur russe en ligne, octobre 2021.

travail auprès de l'opinion (la première était proche de l'équipe de Navalny, la deuxième est issue du Parti pirate russe[24]), La Serre des technologies sociales revendiquait un ancrage dans les champs de l'entrepreneuriat social et de la *civic tech*. Depuis le 24 février, les membres de La Serre ont complètement changé de discours en évoquant l'impossibilité de garder la neutralité politique dans le contexte de la guerre[25]. Les autorités russes ont immédiatement reconnu la politisation de l'ONG en labellisant « agent de l'étranger » Natalia Baranova, directrice des contenus de la Serre et militante du mouvement féministe anti-guerre (FAS), et en bloquant le site de La Serre (d'abord en extension .ru et maintenant en .org) à la suite de la diffusion d'un article intitulé « Comment échapper à la mobilisation »[26]. Les prises de position politiques de l'association n'ont pas suivi immédiatement le début de la guerre généralisée car il a d'abord fallu exfiltrer les employés et autres membres dans des lieux sûrs.

> « Les premiers mois nous n'avons quasiment rien fait car il fallait organiser l'exil de La Serre, en partant de questions très pratiques comme les négociations pour les visas européens, la recherche de points de chute, l'ouverture de comptes bancaires. C'était très dur car le contexte n'était pas du tout propice et il fallait agir vite »[27].

L'ONG joue aujourd'hui un rôle crucial dans le maintien des liens avec les acteurs de la société civile restés en Russie, notamment en matière de sécurité. Depuis le 24 février, elle a organisé de multiples webinars et formations sur les nouveaux enjeux en sécurité numérique, en direction en particulier des équipes disséminées entre la Russie et les divers lieux d'exil. Le recrutement d'un formateur en sécurité à temps plein montre l'importance que cette question acquiert désormais au sein de l'ONG. Dans le contexte russe où il ne reste quasiment plus aucun formateur ou expert en sécurité sur place, la possibilité d'accéder à ces formations à distance permet aux associations restées en Russie de continuer leurs activités. Les membres de La Serre notent cependant une certaine tendance à la simplification des architectures numériques de ces associations, y compris des protocoles de sécurité. Dans des conditions de manque chronique de ressources, notamment financières, après le départ de toutes les fondations et organisations internationales et russes indépendantes de l'État, et face au renforcement des répressions, la majorité des associations adoptent des règles de survie ou, tout simplement, disparaissent :

24 Voir [Daucé, 2022].

25 Entretien avec Alekseï Sidorenko, juin 2022, Varsovie.

26 https://storage.googleapis.com/get_site_copy/te-st.org/e3f8393091707865881e0749161be648ed7d4eb4.html (consulté le 16 février 2023).

27 Entretien avec Alekseï Sidorenko, juin 2022, Varsovie.

> « Nous observons plusieurs types de comportement. Le premier est la survie. Respect total de toutes les lois, autocensure, auto-limitation. L'attentisme est la position la moins risquée, mais c'est aussi la moins militante. La deuxième position est la collaboration avec le régime (…). Le troisième modèle est celui des organisations anti-guerre clandestines qui fonctionnent dans l'anonymat absolu et en autonomie totale. Le quatrième résultat est la dissolution progressive du secteur. Depuis dix ans, il était devenu prestigieux de faire partie des ONG de la société civile : nous avons vu des personnes arriver dans le secteur depuis le monde des affaires, quittant de grandes entreprises. Maintenant, ils partent tout simplement »[28].

De même, La Serre apporte un soutien médiatique et logistique aux collectifs restés en Russie qui essaient d'agir dans un contexte d'extrême précarité économique et politique :

> « Souvent, nous ne pouvons même pas imaginer à quel point la situation à l'intérieur du pays est difficile. Les financeurs étrangers partent, SWIFT[29] a été coupé, les dons diminuent. Il n'y a plus de médias indépendants à l'intérieur et les ONG n'ont nulle part où aller pour raconter leurs histoires. Certaines équipes sont éclatées : par exemple, les services informatiques sont partis, tandis que les avocats, les psychologues, les professions d'assistance continuent à travailler sur le terrain. Les nouvelles lois risquent de criminaliser toute coopération avec des projets de défense des droits de l'homme. »[30]

Ce soutien est rendu encore plus compliqué par le départ de Russie de nombreuses entreprises technologiques étrangères ainsi que par le blocage des systèmes de paiement (tels que Google et Apple Pay) par les géants numériques et les problèmes avec le registre des noms de domaine pour les sites russes[31]. Il devient en outre impossible de soutenir technologiquement les acteurs de la société civile russe du fait de la disparition du programme TeploDigital coordonné par La

28 Alekseï Sidorenko dans : « Počinit' Rossiû po čut'-čut' uže ne polučit'sâ : kak vojna povliâla na graždanskie iniciativy [« On ne pourra pas réparer la Russie » : comment la guerre a impacté les initiatives de la société civile], 19 janvier 2023, https://reforum.io/blog/2023/01/19/pochinit-rossiyu-po-chut-chut-uzhe-ne-poluchitsya-kak-vojna-povliyala-na-grazhdanskie-inicziativy/ (consulté le 16 février 2023).

29 La Society for Worldwide Interbank Financial Telecommunication, le réseau par lequel les messages permettant d'initier les paiements internationaux sont échangés.

30 Natalia Baranova, « Graždanskie iniciativy v god vojny » [Les initiatives de la société civile pendant l'année de guerre], https://www.youtube.com/watch? v=TMa24gu_IlE&t=2836s (consulté le 16 février 2023).

31 D'après un des formateurs interviewés, le site de son client (ONG des droits humains) a été déconnecté par son hébergeur situé à l'étranger car l'ONG était russe. Entretien, en ligne, novembre 2022.

Serre qui permettait aux ONG d'accéder de manière quasi gratuite aux services et logiciels de Google et Microsoft, prisés pour le confort qu'ils offrent dans l'organisation des écosystèmes numériques (par exemple, Google Workspace) ou pour la promotion en ligne (Google Ads) [Bronnikova & Zaytseva, 2021].

À l'étonnement d'associations telles que La Serre, leurs audiences ont très fortement chuté depuis les blocages massifs en Russie de Facebook et Twitter, mais aussi de leurs propres sites[32]. Malgré les efforts qu'elles avaient consenti ces dernières années, elles ont découvert que la majorité des autres associations russes ne savaient toujours pas utiliser les outils de contournement de blocage tels que les VPN, ce qui rend impossible l'accès aux informations sur la sécurité numérique publiées sur le site de La Serre. Pour pallier ce problème, cette dernière, épaulée par ses partenaires à l'étranger, a rejoint le comité d'organisation des conférences « Internet sans frontières » qui ont pour objectif de faire se rencontrer les associations, journalistes et militants avec des spécialistes en développement informatique, spécialisés en outils de contournement de blocages.

Toutefois, les efforts que ces ONG et militants en exil déploient pour aider celles et ceux restés en Russie, sont insuffisants pour garantir la sécurité à tout leur réseau, en particulier lorsqu'on a affaire à de jeunes initiatives horizontales, faiblement structurées, comme le FAS[33], le mouvement féministe anti-guerre :

> « Nous avons des militantes qui ont été victimes de répressions, d'arrestations, de tortures. Elles sont conscientes des risques. Les coordinatrices peuvent seulement aider à mieux préparer les actions, les protocoles de sécurité, à rappeler l'existence de certains dangers. Mais il y a des militantes, ne faisant pas partie du FAS, qui nous accusent en raison des affaires pénales en cours. Pourtant, nous publions sans cesse sur notre chaîne Telegram des conseils en sécurité numérique, sur la sécurité hors-ligne. Cette façon de mettre la responsabilité, qui incombe à l'État répressif, sur le dos du mouvement anti-guerre, n'est pas acceptable »[34].

Conclusion

Au cours des dernières années, nous avons pu observer un durcissement continu des pratiques sécuritaires et policières de l'État russe. Alors que le projet de souveraineté numérique impliquait une construction progressive de la doctrine de sécurité de l'information, la société civile critique s'est positionnée par rapport à l'offensive de l'État en déployant une panoplie d'outils, de pratiques et de

32 Discussion avec des membres de La Serre, novembre 2022, Paris.

33 FAS pour « Feministskoie antivoennoe soprotivlenie ».

34 Discussion avec une des militantes du FAS, septembre 2022, Tbilissi.

savoir-faire en sécurité numérique. Le rejet des plateformes russes au profit des outils proposés par les GAFAM/MAGMA, et plus récemment, des solutions décentralisées et auto-hébergées, a été une des caractéristiques fortes de cette culture de la sécurité.

En dix ans, les questions de sécurité sont progressivement devenues un enjeu majeur pour la société civile de manière générale, et non plus seulement une préoccupation marginale d'une petite minorité considérée par d'autres comme « paranoïaque ». Ce fut le fruit d'un processus long et laborieux, mené par des groupes d'acteurs dont nous avons essayé de dresser à grands traits un portrait de groupe : formateurs, experts techniques, ONG, professionnels de l'espace public médiatique. Le rôle des organisations internationales a été crucial et il le reste aujourd'hui, malgré le contexte des sanctions internationales.

Caractérisé par des échanges internationaux et circulations des normes, outils et pratiques, ce mouvement met en évidence plusieurs aspects importants de la sécurité numérique en tant que telle. Premièrement, son caractère processuel, temporel, dynamique : il ne s'agit pas d'un état donné une fois pour toutes, mais d'un travail d'apprentissage et de réadaptation permanent, ponctué de mises à l'épreuve, d'échecs et de recherche de nouvelles voies. Deuxièmement, son caractère contextuel et relationnel : les risques et surtout les conséquences des failles de sécurité ne sont jamais individuels mais dépendent largement des réseaux dans lesquels les organisations opèrent.

Alors que les organisations militantes et journalistiques russes que nous avons étudiées avant février 2022 avaient la capacité organisationnelle d'appliquer des recommandations de sécurité de façon plus ou moins contrôlée, l'exil a impacté les architectures des mouvements et leur structure administrative. En effet, le caractère international et décentralisé du mouvement antiguerre introduit de nouveaux risques et redéfinit les responsabilités. Les nouvelles organisations militantes, comme le FAS, se retrouvent entre un devoir de protéger leurs activistes et l'impossibilité de gérer une mise en place cohérente des protocoles de sécurité, du fait de l'architecture même et de la dynamique de ces mouvements horizontaux, dont les membres sont disséminés entre des pays différents et dans lesquels les degrés de maîtrise des outils numériques et de perception de la « culture de la sécurité » s'avèrent très hétérogènes.

La guerre et l'exil ont fortement impacté les formateurs en sécurité, en les exposant eux-mêmes aux risques. Les thématiques et les formats des formations ont également été redéfinis (même si la pandémie de Covid-19 avait en partie préparé cette transition, avec une majorité de formations ayant lieu à distance en 2020-2021). Néanmoins, comme nous l'avons montré, les savoir-faire en sécurité

numérique se sont accumulés, ils ont été analysés et ont été partagés non seulement par des ONG spécialisées comme la Serre, mais aussi par des organisations et individus (leaders d'opinion) se trouvant à l'étranger. Ces savoir-faire communs semblent acquérir aujourd'hui, encore plus qu'hier, une importance vitale pour des communautés dispersées et en détresse.

Références bibliographiques

[Bronnikova et al., 2022] Bronnikova, Olga, Ostromooukhova, Bella, Poupin, Perrine & Zaytseva, Anna (coord.), « Militants face à la 'souverainisation' numérique Réactions et nouvelles mobilisations dans l'ex-bloc socialiste (Russie, Ukraine, Cuba) », *Terminal*, n° 134-135.

[Bronnikova & Zaytseva, 2022] Bronnikova, Olga & Zaytseva, Anna, « 'Se protéger ou périr'. Transformations des savoir-faire en sécurité numérique des militants et journalistes russes indépendants (2017-2022) », *Terminal*, n° 134-135.

[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.

[Carey & Burkell, 2009] Carey, Robert F. & Burkell, Jacquelyn Ann, « A heuristics approach to understanding privacy-protecting behaviors in digital social environments », in Kerr, Ian, Steeves, Valerie & Lucock, Carole (dir.), *Lessons From the Identity Trail. Anonymity, Privacy and Identity in a Networked Society,* Oxford, Oxford University Press.

[Daucé, 2022] Daucé, Françoise, « Pirater l'autoritarisme ». *Terminal*, n° 134-135.

[Doktrina, 2000] *Doktrina informacionnoj bezopasnosti Rossiiskoj Federacii* (doctrine de la sécurité d'information de la Fédération de Russie), adoptée par le Président de la Fédération de Russie le 9 septembre 2000, http://base.garant.ru/182535/

[Doktrina, 2016] *Doktrina informacionnoj bezopasnosti Rossiiskoj Federacii* (doctrine de la sécurité d'information de la Fédération de Russie), adoptée par le Président de la Fédération de Russie le 5 décembre 2016, http://static.kremlin.ru/media/acts/files/0001201612060002.pdf

[Ermoshina, 2023] Ermoshina, Ksenia, « Voices from the island: informational annexation of Crimea and transformations of journalistic practices », *Journalism*, online first

[Ermoshina & Musiani, 2022] Ermoshina, Ksenia & Musiani, Francesca, *Concealing for Freedom: The Making of Encryption, Secure messaging, and Digital Liberties,* Mattering Press.

[Ermoshina & Musiani, 2018] Ermoshina, Ksenia & Musiani, Francesca, « Hiding from Whom? Threat Models and In-The-Making Encryption Technologies ». *Intermédialités / Intermediality,* 32

[FIDH, 2018] FIDH, « Russie : 50 nouvelles lois antidémocratiques lors du dernier mandat Poutine », communiqué du 11 mars 2018, https://www.fidh.org/fr/regions/europe-asie-centrale/russie/russie-50-nouvelles-lois-antidemocratiques-lors-du-dernier-mandat

[Hankey & Clunaigh, 2013] Hankey, Stephanie & Clunaigh, Daniel O', « Rethinking Risk and Security of Human Rights Defenders in the digital age, » *Journal of Human Rights Practice* vol. 5, n° 3.

[Kang et al., 2015] Kang, Ruogu, Dabbish, Laura, Fruchter, Nathaniel & Kiesler, Sara, « 'My Data Just Goes Everywhere': User Mental Models of the Internet and Implications for Privacy and Security ». Paper presented at the Symposium on Usable Privacy and Security, (SOUPS) Ottawa, Canada, 22-24 July 2015.

[Limonier, 2016] Limonier, Kevin, « Le cyberespace, nouveau lieu d'affirmation de la puissance russe » in Raviot, Jean-Robert (dir.), *La Russie : vers une nouvelle guerre froide ?* , Paris, La Documentation française, p. 125-149.

[Michaelsen, 2018] Michaelsen, Marcus, « Exit and voice in a digital age: Iran's exiled activists and the authoritarian state », *Globalizations* vol. 15, n° 2, p. 248-264.

[Ristolainen, 2017] Ristolainen, M., « Should 'RuNet 2020' be taken seriously? Contradictory views about cyber security between Russia and the West », *Journal of Information Warfare* vol. 16, n° 4, p. 113-131.

Chapitre 5

Le data-journalisme : enquêter et intervenir dans un espace public censuré

Françoise Daucé

En décembre 2022, dans un article intitulé « La guerre en chiffres », les journalistes du média *Istories* (*Vajnye istorii*) tentent d'évaluer les pertes de l'armée russe en Ukraine. Travaillant avec des volontaires, ils collectent et vérifient les informations sur le nombre de morts à partir de sources ouvertes. Ils dénombrent 9 023 noms. Comme l'explique la rédaction, « Ce chiffre ne reflète pas les pertes réelles de l'armée russe en Ukraine (estimées par les forces ukrainiennes à plus de 100 000 morts), il ne parle que des cas connus publiquement. Mais il dépasse déjà largement les estimations officielles du ministère de la Défense »[1]. Comme bien d'autres articles de la presse russe, le texte collationne des données numériques pour mettre au jour la campagne meurtrière du régime russe en Ukraine. Cette couverture numérique de la guerre s'inscrit dans une dynamique engagée depuis les années 2010 dans les médias russes. Dans un contexte où les principaux journaux russes ont été repris en main [Koltsova, 2006 ; Roudakova, 2017 ; Chupin & Daucé, 2016 ; Daucé, 2019], le recours aux données numériques constitue un espoir de relance du journalisme d'enquête. Pour en donner une définition proposée par les médias russes eux-mêmes, les journalistes de données sont ceux qui, en plus des compétences journalistiques traditionnelles, savent travailler avec des sources numériques : ils connaissent les bases des statistiques, de l'analyse des données et de la programmation et les utilisent dans leur travail[2].

Le *data journalism,* comme nouvelle forme de journalisme d'investigation, se développe au niveau international dans une période de profonde inquiétude à l'égard des informations circulant sur Internet, dont la véracité est souvent mise en cause [Giry, 2017]. Le terme est lui-même polysémique et regroupe des pratiques médiatiques diverses allant de l'usage statistique de données numériques au renseignement de sources ouvertes (OSINT) [*Hérodote*, 2022]. Confronté aux effets suspicieux des « fausses nouvelles », le journalisme de données nourrit une

1 Vojna v cifrah. *IStories*, 16 mai 2022 (actualisé le 10 novembre 2022) https://istories.media/reportages/2022/05/16/voina-v-tsifrakh/ (consulté le 13 février 2023).

2 https://istories.media/workshops/2021/11/05/zhurnalistika-dannikh-chast-1-istoriya/

« nouvelle rhétorique de l'objectivité » [Vauchez, 2019] fondée parfois sur une « fétichisation de la donnée » elle-même [Lapoix, 2014]. L'enquête par les *data* s'inscrit dans un mouvement ancien de numérisation des savoirs [Anderson, 2018], qui touche tant le journalisme que les sciences sociales [Boullier, 2015] ou l'expertise. Les journalistes s'appuient sur les données pour réduire leur dépendance aux sources, limiter leur subjectivité et garantir la précision de leurs travaux. Ils incarnent un modèle de journalisme sobre et factuel, fondé sur l'exhaustivité et l'exactitude, opposé à l'outrecuidance du journalisme politique, inspiré et corrosif (à l'image des deux modèles historiques identifiés par C. Lemieux [1992]). L'usage des données fait l'objet de formations techniques (apprentissage du code) et infographiques qui mettent en équivalence des données et des faits. Les sources sont diverses, qu'il s'agisse de données ouvertes, achetées ou fuitées [Loveluck, 2016]. De nombreux médias révèlent ainsi des réalités scandaleuses en prenant appui sur les formes sociotechniques particulières que sont les bases de données. Ces sources nouvelles permettent aux journalistes de « surveiller les surveillants » dans une logique de « sousveillance », pour reprendre l'expression de Steve Mann [2002] (voir également [Alloing, 2016]), qui y voit un « panoptique inversé ». Il permet aux citoyens d'user des dispositifs numériques pour « regarder d'en bas » les pouvoirs étatiques et commerciaux. Si le *data journalism* se développe dans les rédactions occidentales, son avenir reste discuté. Plusieurs scénarios se dessinent : celui du développement large du journalisme de données, celui du maintien de ce type de journalisme de niche et enfin, celui de l'externalisation du data journalisme à des entreprises extérieures aux rédactions [Stalph & Borges-Rey, 2018]. Dans une perspective critique, ce « journalisme sur écran » peut même être considéré comme un aboutissement du « libéralisme numérique » [Boyer in Bounegru & Gray, 2021].

Une vaste littérature sur le *data journalism* dans les contextes anglo-saxons est désormais disponible [Gray et al, 2012 ; Anderson, 2018 ; Young et al, 2018 ; Ausserhofer et al, 2020] mais elle reste limitée dans le cas de la Russie. Le cas russe fait pourtant surgir d'intéressants enjeux. Dans un contexte d'emprises politiques et infrastructurelles fortes [Oates, 2013 ; Daucé & Musiani, 2021], les journalistes russes manifestent un intérêt croissant pour les données, comme en témoigne, dans les années 2010, l'apparition de plusieurs médias en ligne (*pure players*), se revendiquant de cette nouvelle spécialité. Quelques travaux académiques actuellement disponibles documentent ces dynamiques [Begtin, 2013 ; Valeeva, 2017 ; Šilina & Šilina, 2020 ; Dovbysh, 2021]. Avec le déclenchement de la guerre contre l'Ukraine en février 2022, les contraintes pesant sur les citoyens et les journalistes s'alourdissent, notamment avec l'adoption de la loi sur les « fausses nouvelles militaires » en mars 2022. Dans ce contexte, l'accès aux données numériques devient une ressource déterminante pour les enquêtes relatives au front et au mouvement des troupes. Réfugiés à l'étranger pour échapper aux

poursuites criminelles qui les menacent en Russie, les journalistes sont éloignés de leurs terrains d'enquête et poursuivent l'investigation à distance, par l'intermédiaire des sources disponibles en ligne. Les uns pratiquent le traitement statistique des données accessibles, d'autres mènent des investigations collaboratives à l'exemple de l'organisation citoyenne *Conflict Intelligence Team* (fondée par des citoyens russes après le début de la guerre au Donbass en 2014) qui témoigne de l'intérêt pour les enquêtes *open source* en contexte de conflits armés. Le traitement des données suscite en retour des luttes opposant les pouvoirs publics et les journalistes. Ces dernières portent sur l'accès aux données publiques, sur la qualité des sources, sur l'achat de données privées ou sur la maîtrise des données fuitées. Les données sont donc enrôlées, au sens employé par Michel Callon et Bruno Latour [2006], dans des conflits d'appropriation et d'interprétation qui montrent les enjeux politiques liés à leur production et à leur usage.

Ce chapitre propose une socio-histoire du journalisme de données en Russie dans une perspective qui fait place aux innovations, aux résistances et aux épreuves qu'il rencontre. Il décrit les pratiques et les réflexions des acteurs, notamment à partir d'entretiens réalisés entre 2018 et 2022 (à Moscou, en ligne ou hors des frontières russes) avec des journalistes d'investigation par les données (dont certains ont été déclarés « agent de l'étranger » par les autorités russes) travaillant pour les rédactions des médias *Proekt*, *RBK*, le service russe de la *BBC, Istories* ou *The Insider* ainsi que des entretiens avec des militants russes pour l'ouverture des données de la fondation *InfoKultura* et des collaborateurs de la Fondation de Lutte contre la corruption d'A. Navalny. Le texte est aussi basé sur l'observation des sources en ligne en russe (ethnographie des réseaux sociaux, étude des chaînes Telegram, dont la chaîne « Données ouvertes RU »).

Le journalisme de données, une dynamique transnationale

Le développement du *data journalism* en Russie s'inscrit dans des dynamiques internationales qui, depuis le début des années 2010, convergent avec les préoccupations du *data activism* [Milan & Van der Velden, 2016]. De nouvelles formes d'objectivation de l'investigation, destinées à exposer les abus de pouvoir dans la société [Carson, 2019], sont apparues. L'enquête journalistique par les données, bénéficiant des traces numériques massives désormais disponibles, est venue renouveler la pratique du journalisme, en rupture avec les méthodes traditionnelles frappées d'obsolescence[3]. Les sources numériques ont constitué une réponse aux multiples épreuves rencontrées par les journalistes : déficit de

3 Les débats sur le renouvellement du journalisme par le recours aux données font écho aux débats sur le renouvellement des sciences sociales par le numérique [Venturini et Latour, 2009, Boullier, 2015].

légitimité, soupçon des *fake news,* accélération du temps médiatique… Depuis le milieu des années 2010, le « tournant quantitatif » [Coddington, 2015] du journalisme de données est considéré par ses promoteurs comme porteur d'opportunités nouvelles, permettant d'offrir des interprétations indépendantes des données officielles, d'agir comme filtre raisonné face au déluge des données et de dévoiler des réalités invisibles [Gray et al, 2012]. Dans les travaux de sociologie du journalisme, l'enquête par les données est pensée comme une transformation profonde du rapport des journalistes à leurs sources, offrant l'opportunité d'une distanciation à l'égard de relations considérées comme asymétriques [Parasie & Dagiral, 2013]. En Russie, plus qu'ailleurs, le recours aux données s'inscrit dans ces perspectives et porte des espoirs de lutte contre la censure, la désinformation, le secret et la corruption [Yablokov, 2018]. Le cas russe enrichit ainsi l'étude de «l'économie politique des données» engagée dans d'autres contextes [Loveluck, 2016].

Les réseaux médiatiques des consortiums d'enquête

Les pratiques du journalisme de données sont diverses, allant du traitement des mégadonnées (*big data*) à l'analyse des données ouvertes en passant par l'observation des nombreuses traces numériques laissées par la navigation en ligne. Leur ambition commune est d'éclairer les «violations de l'ordre moral» [Parasie & Dagiral, 2013]. Le développement du *data journalism* est une pratique globale [Bigot, 2017] qui permet aux journalistes de diverses nationalités de s'insérer dans des collectifs internationaux et de contribuer à l'avancement de leurs enquêtes. Le traitement des grandes masses de données est généralement assuré par des collectifs d'acteurs comme *l'International Fact Checking Network* (IFCN) basé en Floride, le *Global Investigative Journalism Network* basé au Maryland, l'*International Consortium of Investigative Journalists* (ICIJ) ou le réseau danois SCOOP qui se sont développés au cours des années 2010. Dans le monde occidental, des liens se sont noués entre les mondes informatique et journalistique. Aux États-Unis puis au Royaume-Uni, des programmeurs ont intégré les rédactions de grands journaux ou d'organisations indépendantes produisant de l'information [Gray et al, 2012]. Les journalistes russes s'insèrent dans ces collectifs d'enquête, contribuant notamment aux investigations internationales impliquant des protagonistes russes et nécessitant de recourir à des données dans cette langue. Au printemps 2016, le journal indépendant *Novaïa Gazeta* participe à l'enquête sur les Panama Papers. Les 11 millions de documents rassemblés sont traités par reconnaissance optique des caractères (OCR) et sont transformés en immense base de données par l'ICIJ. *Novaïa Gazeta* participe à la publication des documents liés à la partie russe.

Lorsqu'il s'inspire des méthodes d'*open source investigation* (OSINT), le journalisme d'investigation par les données numériques est à la recherche de révélations et de scandales. Lors de l'affaire Skripal, en Grande-Bretagne, le média russe *The Insider* enquête avec l'équipe *Bellingcat* pour dévoiler les noms des membres des services de renseignement russes impliqués dans la tentative d'assassinat. Créé en 2013 par le journaliste indépendant Roman Dobrokhotov, le site travaille à partir des données publiques ou fuitées, grâce à l'aide de contributeurs indépendants et bénévoles. Les journalistes s'appuient sur des logiciels, images et banques de données en libre accès – Google Earth et YouTube, notamment. *Bellingcat* (de l'expression « *to bell the cat* », « mettre un grelot au cou du chat »), s'appuie sur le travail de journalistes citoyens, pour la plupart autodidactes, dont le travail permet, au-delà de l'information du public, de réunir des preuves pour des poursuites pénales[4]. Grâce à ces coopérations, les sites d'investigation russes bénéficient d'une forte reconnaissance internationale, couronnée par l'obtention de prix. Le site *The Insider* a notamment été décoré du prix « Innovation » du Conseil de l'Europe (2018), du *European Press Prize* (2019) pour l'investigation sur les auteurs de l'empoisonnement de Sergueï Skripal à Salisbury[5], ainsi que du *Free Media Award* (2019).

La passion numérique du journalisme d'investigation en Russie

L'engouement pour le journalisme de données en Russie est proportionnel à la fermeture de l'espace public russe, qui rend l'accès aux informateurs et sources physiques de plus en plus difficile. À l'heure du numérique, « Le pire des moments pour les médias et les libertés politiques en Russie post-soviétique pourrait-il également être le meilleur moment pour le reportage d'investigation ? » s'interroge Sheila Coronel, du *Global Investigative Journalism Network* dès 2013[6]. La journaliste Elizaveta Ossetinskaia, fondatrice du média en ligne *The Bell*, pense, elle aussi, que l'investigation n'a jamais été aussi dynamique et sa qualité aussi bonne[7]. De nouveaux projets médiatiques apparaissent dans le contexte russe [Rostova, 2019]. Ils considèrent les données comme un facteur d' « objectivité mécanique », permettant de rompre définitivement avec les suspicions de subjectivité de

4 *Bellingcat, les combattants de la liberté,* de Hans Pool (PB, 2018, 90 min). www.bellingcatfilm.com (consulté le 13 février 2023).

5 Prix de l'investigation : « Les suspects de l'empoisonnement de Salisbury démasqués : investigation en quatre parties », par Christo Grozev, Roman Dobrokhotov et Daniel Romein (« Bellingcat », Grande-Bretagne). https://www.lemonde.fr/actualite-medias/article/2019/05/23/l-european-press-prize-pour-the-guardian-bellingcat-et-le-projet-forbidden-stories_5466208_3236.html

6 Sheila Coronel. Muckraking in Putin's Russia. 18 avril 2013. https://gijn.org/2013/04/18/muckraking-in-putins-russia/ (consulté le 13 février 2023).

7 *Ibid.*

l'enquêteur. De nombreux journalistes russes se forment à l'enquête par les données dans les médias « indépendants » depuis le milieu des années 2010.

Le recours aux données est ainsi pratiqué par les journalistes de RBK, de *Meduza*, de *Novaïa Gazeta*, du service russe de la BBC ainsi que des sites d'investigation comme *The Insider, Mediazona*, *Proekt* ou *IStories*. D'après une data-journaliste interrogée, « Ce sont plutôt les nouveaux médias qui adoptent le journalisme de données et élaborent de nouveaux formats. Les grosses rédactions comme *Vedomosti* ou *Kommersant* le pratiquent peu »[8]. En 2019, le site *Novaïa Gazeta* crée une section spécifique de data-journalisme au sein de sa rédaction[9]. Les journalistes codent, rassemblent les données et les visualisent. Ils relèvent de la section plus large des grandes investigations. Comme l'explique une journaliste, « Nous avons souvent affaire à des données lors des investigations, cela permet de réaliser des enquêtes de meilleure qualité ». Sur la raison de l'ouverture de cette section, Alessia Marokhovskaïa (qui rejoint ensuite le média d'investigation *IStories* fondé en 2020) explique : « Les médias occidentaux ont compris depuis longtemps qu'il existe de nombreuses histoires dans les données (…) mais pour cela il faut des gens spécialisés, des data-journalistes[10] ».

Le site *Proekt*, lancé en 2018 par Roman Badanine, après son licenciement successif pour raisons politiques de la rédaction en chef de plusieurs médias d'information, s'inscrit dans cette même dynamique. Le site se définit comme un « média indépendant, réunissant des journalistes d'investigation et des reporters. Nous faisons ce que nous savons faire : trouver ce qui est caché et important et vous le raconter. Nous estimons que c'est indispensable car, en Russie, il n'existe quasiment plus de médias qui touchent aux thèmes compliqués et dangereux »[11]. La rédaction est composée d'une dizaine de journalistes qui publient un article d'investigation chaque semaine. Comme l'explique Roman Badanine en 2018, *Proekt* est fondé sur des investigations basées sur les « *big data* » (*bolchie dannye*)[12]. Les enquêtes et les investigations menées à partir des données numériques reposent sur une méthodologie qui favorise une restitution chiffrée et objectivée de la vérité. De nombreux articles présentent ainsi des données agrégées, compilées et mises en visibilité par des procédés infographiques.

8 Entretien de l'auteur avec une journaliste, en ligne, 8 décembre 2020.

9 La section est composée de trois journalistes : Irina Dolinina, Artem Chennikov et Alessia Marokhovskaia sous la direction d'Andrei Zaïaakine.

10 https://jrnlst.ru/data-journalism-novaya

11 https://www.proekt.media/about/ (consulté le 13 février 2023).

12 https://vc.ru/media/42523-eks-glavred-dozhdya-roman-badanin-zapustit-izdanie-proekt-s-rassledovaniyami-na-osnove-bolshih-dannyh (consulté le 13 février 2023).

Dans le cas russe, l'enquête et l'investigation par les données ne constituent pas le monopole des journalistes mais représentent aussi une opportunité pour les militants d'opposition. Le plus connu d'entre eux, A. Navalny, a construit sa notoriété sur la dénonciation de la corruption de l'élite du pays grâce à des enquêtes en ligne. Son exemple est spécifique au contexte russe. En effet, son mouvement est un hybride assez inédit entre un mouvement politique de type partisan, une association militante de lutte contre la corruption et un média d'investigation. Il constitue à ce titre une forme de résistance originale en contexte d'autoritarisme numérique. Cette composition multiple permet à la Fondation de mener des enquêtes retentissantes en Russie même, puis de poursuivre ses activités à distance après l'exil de ses principaux militants. Depuis l'étranger, ils continuent à travailler sur des enjeux transnationaux, notamment dans les enquêtes sur le blanchiment d'argent sale d'Est en Ouest en mobilisant des registres et bases de données dans plusieurs pays y compris la France. La Fondation de lutte contre la corruption (FBK) d'A. Navalny a pour particularité de maîtriser l'ensemble de la chaîne de dévoilement, depuis la recherche des données jusqu'à leur mise en visibilité. Elle réalise, grâce à la compilation de sources numériques, de virulentes enquêtes à charge contre les responsables du pays dans une veine populiste [Glazunova, 2020], et notamment contre le premier ministre D. Medvedev en 2017[13].

Les médias qui pratiquent l'investigation en ligne obtiennent des succès d'audience significatifs, si l'on en croit les métriques de la société Medialogia qui mettent en visibilité la notoriété relative des différentes rédactions. Entre janvier et juin 2021, les sites Navalny.com, Theins.com, Zona.media, *Novaïa Gazeta* ou *Proekt* apparaissent régulièrement parmi les sources les plus citées sur les réseaux sociaux russes. Le site *IStories* obtient un succès d'estime avec ses enquêtes sur la corruption dans les cercles du pouvoir mais aussi ses données sur les inégalités sociales et environnementales. En juillet 2021, Roman Dobrokhotov (*The Insider*) et Roman Badanine (*Proekt*) apparaissent dans le top 10 des journalistes les plus cités en Russie[14].

Le journalisme de données, une utopie technique ?

En Russie, dans un contexte de manipulation politique du champ médiatique et de renforcement des contrôles sur les médias, cet intérêt pour le journalisme numérique s'appuie sur des apprentissages en statistique, codage, infographie et analyse de sources quantitatives. D'après un journaliste du média Znak.com, « le

13 https://dimon.navalny.com/ Pour une présentation des méthodes d'enquête en ligne de FBK, voir ici : https://www.bellingcat.com/resources/case-studies/2015/08/19/yachtspotting/ (consulté le 13 février 2023).

14 Voir le site : https://www.mlg.ru/ratings/ (consulté le 13 février 2023).

travail avec les données transforme presque le journalisme en science exacte»[15]. Ces appuis techniques permettent aux journalistes de renouer avec les espoirs des débuts d'Internet [Flichy, 2012 ; Loveluck, 2015] marqués par une confiance dans les vertus du numérique, mais posent la question de leur réflexivité face aux données, souvent prises pour argent comptant, qu'ils manipulent [Lowrey et al, 2019].

Le développement des formations en data-journalisme

Au cours des années 2010, le journalisme de données s'institutionnalise progressivement grâce au développement de programmes d'enseignement, de formation, de récompenses ou de communautés en ligne [Bounegru & Gray, 2021]. En Russie, il bénéficie de l'organisation d'un cursus universitaire (un master de *data journalism* est créé à l'Université d'État - Haut Collège d'Économie de Moscou en 2016)[16], du développement de formations aux méthodes d'investigation en ligne au croisement de la programmation et du journalisme ainsi que de l'apparition de journalistes spécialisés dans les rédactions. En mars 2016, le premier hackathon sur le journalisme de données se déroule à Moscou à l'initiative du Comité des initiatives civiques d'A. Koudrine et du Haut collège d'économie. En complément, la chaîne Telegram intitulée « *Data Jurnalistika* (DDJ Russian) » constitue un espace d'échange des savoirs et de réflexivités sur les données depuis août 2019. Elle est administrée par Anastasia Valeeva qui invite ses membres « à discuter des problèmes actuels du data journalisme en langue russe, à partager des matériaux, des conseils et à créer des équipes »[17]. En janvier 2020, la journaliste Ioulia Apoukhtina s'interroge sur cette chaîne :

> « Qu'est-ce que la qualité en data journalisme ? L'exigence d'une fiabilité statistique, les modalités de fabrication et les questions de publication des liens et des ensembles de données (*dataset*). Les exigences scientifiques doivent-elles s'appliquer au journalisme d'investigation et à quel degré ? Où se termine l'illustration par les statistiques et où commence la recherche ? »[18].

La méthode d'enquête devient parfois partie intégrante de l'article comme en témoignent les encadrés méthodologiques qui accompagnent les enquêtes sur les

15 Dmitrij Kolezev. Mozhno kupit' labuteny dlia vsekh zhitelej Nishnego Tagila. Znak.com, 2 mars 2016. https://www.znak.com/2016-03-02/v_moskve_proshel_pervyy_hakaton_po_data_zhurnalistike (consulté le 13 février 2023).

16 https://www.hse.ru/ma/datajourn/ (consulté le 13 février 2023).

17 Anastasia (administrateur), data journaliste basée au Kyrgyzstan, post du 14 août 2019. La chaîne compte 375 membres en janvier 2021.

18 Iûlâ Apuhtina, post sur la chaîne Telegram DDJ Russian, 9 janvier 2020.

sites de *The Insider*, *Proekt* ou FBK. Le site *IStories* propose même une rubrique «atelier» pour s'initier à l'analyse des données sous Excel, à la visualisation et la cartographie sous Datawrapper et à la programmation sous Python[19]. La lecture de ces encadrés techniques et les entretiens avec les journalistes montrent la diversité des données mobilisées, ce qui n'est guère spécifique au contexte russe et proche des observations réalisées sur le terrain nord-américain [Parasie, 2013]. Le travail sur les données à proprement parler est fondé sur l'apprentissage du code (pour moissonner et nettoyer les données, construire des bases ou concevoir des visualisations). Comme l'explique Alessia Marokhovskaïa : «Le journalisme de données est du journalisme, mais on n'y parle pas avec des gens mais avec des données (…) et pour cela il faut connaître leur langage. Habituellement, c'est la langue de programmation Python». En février 2020, Egor Skovoroda, journaliste pour *Mediazona*, suit une formation intitulée «Python pour l'analyse des données» et reconnaît que «Le code pour les nuls» est devenu son livre de chevet, tout en se souvenant que, quelques années auparavant, il se moquait des formations au tableur Excel[20]. Il explique : «Python pour les journalistes d'investigation est comme un nouvel anglais, ne pas le connaître est tout simplement honteux». L'une des journalistes, qui publie des articles pour *Proekt*, a une formation de développeur en informatique et sait coder en Java et Python. Elle explique aussi que sa double expérience en journalisme économique et en programmation lui permet de travailler avec les grandes masses de données[21].

Outre les données statistiques, les journalistes russes élargissent leurs sources et s'intéressent à l'ensemble des traces numériques disponibles en ligne : «L'activité OSINT est utilisée par les enquêteurs mais aussi les journalistes, les professionnels de l'informatique et des affaires de sécurité mondiale, le secteur bancaire, afin de détecter les fraudes potentielles, escroqueries, phishing ou le blanchiment d'argent»[22]. Les journalistes russes bénéficient des outils d'analyse numérique désormais disponibles pour recourir à ces pratiques. En avril 2020, Andreï Zakharov, alors correspondant de la BBC, anime un séminaire en ligne intitulé «Comment enquêter sur la Covid19 sans quitter sa maison : la méthode OSINT (*Open Source Intelligence*)». A. Zakharov est connu pour son enquête sur les bourses aux crypto-monnaies de la Fondation FSB (qui a perdu 450 millions de dollars sur la plateforme d'échange WEX) ainsi que pour ses publications sur les usines à troll d'E. Prigojine. Comme il l'explique,

19 https://istories.media/workshops/ (consulté le 24 août 2021).

20 https://zeh.media/praktika/obrazovaniye/9648173-ne-znayu-kak-eto-prigoditsya-mne-v-zhurnalistike-no-moy-mozg-popytka-pouchit-python-uzhe-rasshevelil (consulté le 13 février 2023).

21 Entretien de l'auteur avec une journaliste, en ligne, 8 décembre 2020.

22 https://www.psbedu.paris/fr/actus/open-source-intelligence-technique-renseignement-service-intelligence-economique; voir aussi https://nothing2hide.org/fr/2019-09-18-guide-osint-2019/ (consulté le 13 février 2023).

> «Les investigations sont nécessaires dans les médias sérieux car elles apportent une réputation en Russie et dans le monde entier. (…) Il faut du temps pour réaliser de bonnes investigations. Il faut générer des hypothèses, essayer de les vérifier, accepter des échecs, chercher ailleurs (…). C'est vrai que c'est dur moralement. (…) il faut, en plus, perfectionner sans cesse son utilisation des instruments.»[23].

Le travail sur les données revêt enfin une dimension esthétique : «Nous nous battons pour que nos contenus soient beaux (…) et compréhensibles»[24]. Le recours aux données s'accompagne de mises en forme infographiques permettant de visualiser les statistiques obtenues [*Interfaces numériques*, 2020]. Les journalistes réalisent des investissements de forme et inventent des instruments de visualisation pour montrer ce qui était invisible.

Les opportunités des sources ouvertes, achetées ou fuitées

Le travail d'enquête par les données interroge les sources disponibles. Les plus directement accessibles sont les données ouvertes (*open data*), mises à disposition par les administrations dans le sillage des recommandations de la rencontre de Sebastopol (Californie) en 2007, lorsque les activistes numériques demandent la «libération» des données publiques dès leur production et dans leur intégralité. Le terme d'*Open Government Data* émerge, accompagné par l'ouverture de portails de publication des données publiques. La Russie n'est pas à l'écart de ce mouvement et lance, dans les années 2010, une politique d'*open data* dans une logique de développement économique (et non de contre-expertise au sein de la société civile). En 2011, le portail open.gov.ru recense les réalisations en matière de données ouvertes. En 2013, la ville de Moscou lance la plateforme de données ouvertes data.mos.ru. Des projets similaires se développent dans diverses régions du pays. En 2014, le site data.gov.ru est ouvert. Des volumes massifs de données sont publiés, à l'exemple de la base Rosreestr (le registre des droits de propriété).

Ces données ouvertes constituent des sources privilégiées pour les journalistes qui enquêtent sur les marchés publics, les infractions juridiques, les inégalités sociales, la protection médicale… Des militants et des entrepreneurs défendent l'ouverture des données publiques en Russie et mettent en place des initiatives de valorisation de leurs contenus. Dans une note institutionnelle française intitulée «Russie : de la Glasnost' à l'*Open Government*. Les progrès réalisés en matière de transparence», V. Ma-Dupont affirme que la Russie s'engage résolument dans la révolution de

23 Andrej Zaharov. Webinaire organisé le 2 décembre 2020 par le site Spektr.

24 https://radioportal.ru/news/chto-takoe-data-zhurnalistika-i-chem-ona-mozhet-pomoch-lyuboy-redakcii (consulté le 13 février 2023).

l'open data, accueillant le sommet pour les données ouvertes en décembre 2015[25]. Cette ouverture se situe dans le prolongement de l'action de D. Medvedev à la tête de l'État russe entre 2008 et 2012. Des arguments économiques (attrait des investisseurs et génération de nouveaux flux financiers) viennent en appui de cette politique.

Cette ouverture est prise au sérieux par les médias qui récoltent et analysent les données ainsi rendues disponibles. Comme l'explique Elizaveta Ossetinskaïa, fondatrice du projet *The Bell*, « Nous avons maintenant beaucoup de bases de données. Nous avons des informations sur les appels d'offres publics. On peut trouver beaucoup d'informations sur les structures des compagnies privées »[26]. Pour une journaliste interrogée, « À partir de 2014, les organes du pouvoir ont commencé à publier activement de nombreuses données. Sous quelle forme ? Le facteur déterminant a été l'ouverture du système des marchés publics où l'on trouve presque toutes les données concernant les dépenses du budget public (…) Naturellement, on a commencé à travailler avec ces données sur les contrats publics »[27]. Toutes les enquêtes fondées sur les données ouvertes ne sont pas des enquêtes à charge contre le pouvoir mais leur analyse permet de documenter les questions sociales comme le montre le projet « Qui paye les retraites ? » du studio de développement des données de *RIA-Novosti*, le projet Merkator sur l'âge des logements à Moscou, ou le projet Demoscope sur les accidents de la route.

Si les données publiques constituent des sources journalistiques respectables, les données volées, achetées ou fuitées nourrissent les investigations les plus explosives. Les données fuitées (*leaked*) qui circulent dans l'espace numérique russe viennent mettre en lumière l'activité de hackers qui parviennent à publier des sources cachées. Certains journalistes évoquent la possibilité de recourir à des « fuites » de données ou des achats sur le *darknet*. Dans un pays marqué par l'emprise des services de sécurité et l'obligation de conservation des données personnelles sur le sol russe, l'accès aux informations moissonnées par les entreprises de surveillance constitue l'objet de convoitises. La quantité et la variété des données disponibles sont corrélées à la faible protection des données personnelles, dénoncée par les défenseurs des libertés numériques. Cette défaillance liée à l'absence de règlement sur la gestion des données offre paradoxalement des opportunités pour les journalistes d'investigation qui collectent ainsi des informations diverses sur leurs enquêtés. Comme l'explique

25 https://www.economie.gouv.fr/files/files/directions_services/igpde-editions-publications/revuesGestionPublique/IGPDE_Reactive_Russie_decembre_2015_janvier_2016.pdf (consulté le 13 février 2023).

26 Sheila Coronel. Muckraking in Putin's Russia. 18 avril 2013. https://gijn.org/2013/04/18/muckraking-in-putins-russia/ (consulté le 13 février 2023).

27 Entretien de l'auteur avec une journaliste, en ligne, 8 décembre 2020.

le journaliste A. Zakharov, en décembre 2020, « À Moscou, on se rend compte qu'il y a un système massif de surveillance de la population. On le voit avec l'exemple des données de vidéosurveillance avec reconnaissance faciale. (..) C'est très facile de trouver où une personne réside »[28]. Il cite aussi l'exemple des services wifi du métro qui permettent de tracer le trajet d'un voyageur à travers toute la ville. Il donne les tarifs des données vendues : 1000 roubles pour les données d'un passeport, 15 000 roubles pour la liste des passagers d'un avion[29]. A. Navalny en fait une cause politique en déclarant, en décembre 2020 : « Je remercie la loi Iarovaïa qui a permis aux membres corrompus des unités de maintien de l'ordre de vendre librement les données issues de nos téléphones portables ou les données des compagnies aériennes »[30], données qu'il utilise pour les propres enquêtes de sa Fondation.

Les luttes politiques pour l'interprétation et l'appropriation des données

Le recours aux données nourrit des investigations qui mettent en lumière la corruption des autorités, les malversations des entrepreneurs ou l'incurie des administrations. Ces révélations, qui vont parfois jusqu'au scandale (comme dans le cas des révélations sur les auteurs de l'empoisonnement d'A. Navalny ou sur le palais de V. Poutine et l'opulence de ses proches au début de l'année 2021), suscitent en réponse des contre-mesures qui ne relèvent pas du démenti ou de la contre-expertise mais de registres de justification ou de pratiques de détournement ou d'empêchement de la critique. Lors des scandales d'ampleur fédérale, la réponse publique emprunte aux ontologies du complot international. Dans le cas des enquêtes les plus retentissantes, le pouvoir russe contre-attaque en affirmant que les données « ont été fournies par les services spéciaux occidentaux »[31]. V. Poutine lui-même déclare qu'il s'agit de « la légalisation des sources des services spéciaux américains »[32]. La suspicion sur la provenance des données mobilisées par les journalistes justifie leur enregistrement sur la liste des « agents de l'étranger » pour déconsidérer leur travail et les mettre en accusation. Au-delà de ces arguments complotistes, la lutte politique pour l'appropriation des données s'inscrit aussi dans des dispositifs socio-techniques qui concernent

28 Andrej Zaharov. Webinaire organisé le 2 décembre 2020 par le site Spektr.

29 https://www.youtube.com/watch? v=v6slhNgKCOI (consulté le 13 février 2023).

30 https://www.youtube.com/watch? v=smhi6jts97I&t=2208s (consulté le 13 février 2023).

31 Andrej Zaharov. Kak rassledovanie ob otravlenii Naval'nogo izmenilo žurnalistiku. *IJnet*, 4 janvier 2021. https://ijnet.org/en/node/9468 (consulté le 13 février 2023).

32 Putin nazval dannye po Naval'nomu « legalizaciej materialov » specslužb SŠA. RBK, 17 décembre 2020. https://www.rbc.ru/politics/17/12/2020/5fdb30b19a79477f9d320cff (consulté le 13 février 2023).

les données elles-mêmes, dont l'accès est empêché, restreint ou falsifié. Une fois la guerre en Ukraine engagée, la mise en accusation des journalistes et de leurs données se renforce et devient un enjeu stratégique dans un contexte de mobilisation militaire.

La lutte contre les data-journalistes

En 2020 et 2021, l'épistémologie de l'enquête numérique en Russie réactive des confrontations politiques qui plongent leurs racines dans les épisodes de la guerre froide et la suspicion durable qu'elle nourrit à l'égard des influences étrangères. Alors que l'État russe est soupçonné d'être le principal pourvoyeur de fausses informations dans le monde médiatique occidental des années 2010, il dénonce en retour le complot des journalistes d'investigation enquêtant dans l'espace numérique à ses dépens. Les journalistes russes qui utilisent les données sont pris à partie par les médias d'État et font face à des articles à charge visant à les discréditer[33]. Leurs coopérations internationales sont vues comme des ingérences étrangères. Les tentatives de scandalisation autour des malversations d'État sont accusées d'être le fait d'« agents étrangers » (en vertu de la loi russe de 2012 amendée en 2017) bénéficiant du soutien politique et financier de gouvernements hostiles.

Selon la législation russe, peuvent être déclarés « agents de l'étranger » des médias (depuis 2017) ou des personnes physiques (depuis 2021) qui diffusent des informations au grand public et reçoivent des financements étrangers (quel qu'en soit le montant). Les médias d'investigation par les données tombent très rapidement sous le coup de la loi. Le média *The Insider* est reconnu comme agent de l'étranger par une décision du ministère russe de la Justice du 5 décembre 2017. Le journal pro-pouvoir *Ekspress Gazeta* affirme qu'il est contrôlé par « les services spéciaux de l'Occident »[34]. À l'automne 2019, ce sont les journalistes de *Proekt* qui font face à des menaces, des filatures et une tentative d'intrusion sur leurs comptes après le début d'une enquête sur les mercenaires russes en Afrique et au Moyen-Orient. Les journalistes ont d'abord reçu par e-mail des menaces de rétorsions physiques. Des tentatives pour s'introduire sur leurs comptes sur Facebook, Telegram et sur leur mail sur Google ont été constatées[35]. Au printemps et à l'été 2021, les sites *Meduza*, *Dojd*, *IStories* sont inscrits sur la liste des « agents de l'étranger ». Plusieurs dizaines de journalistes sont aussi inscrits à titre

33 https://russian.rt.com/world/article/593261-hodorkovskii-tsar-rassledovanie (consulté le 13 février 2023).

34 https://www.eg.ru/society/655731-smi-nezavisimyy-the-insider-kontroliruyut-specslujby-zapada-078698/ (consulté le 13 février 2023).

35 https://zona.media/news/2019/10/15/proekt (consulté le 13 février 2023).

individuel sur cette liste dont Roman Badanine et plusieurs membres de l'équipe du média *Proekt*[36]. En juillet 2021, le site *Proekt* est déclaré « média indésirable dans le pays ». Son équipe éditoriale annonce la fin de ses activités. R. Badanine et plusieurs de ses collègues quittent le pays pour assurer leur sécurité. Avec le début de la guerre en Ukraine, la liste des médias et des journalistes empêchés de travailler s'allonge considérablement. Face aux risques qu'ils encourent, la plupart d'entre eux préfèrent s'exiler à l'étranger, d'où ils poursuivent leurs investigations en ligne (voir chapitre 8).

La lutte pour les données numériques

Outre les personnes, les données sont enrôlées dans des luttes politiques. Face au renforcement de la répression, la fiabilité des sources publiques est posée, dans un contexte où la statistique d'État en Russie est traditionnellement soupçonnée de partialité. Les journalistes constatent que l'ensemble des données publiques ne sont pas publiées et certaines sont de médiocre qualité[37]. Ce constat n'est pas spécifique à la Russie mais commun à d'autres espaces où les administrations, comme dans le cas des sources policières par exemple, « conservent la liberté de les arranger comme bon leur semble » [Parasie & Dagiral, 2013]. En 2021, des observateurs estiment que la quantité de données ouvertes augmente en Russie mais que leur qualité décline. O. Kuzmitcheva constate qu'il existe de nombreux exemples de « mauvaises données » présentées dans des versions obsolètes ou sous formes de graphiques sans accès aux sources originales… Sous couvert de données ouvertes, certaines administrations mettent en ligne des données illisibles[38]. La publication des données suscite des tensions au sein même de l'administration russe. Comme l'explique un expert en 2017 : « Dans l'administration, il y a deux tendances : ceux qui veulent passer à la culture numérique et les revanchistes qui veulent fermer les données. L'équilibre des forces est à 50/50 »[39].

Les controverses médiatiques liées aux investigations en ligne suscitent en retour des rétorsions contre les données. Le cas de la base de données Rosreestr en est un exemple éclairant. En 2015, après la publication du film « Tchaika » d'Alekseï

36 Voir le registre officiel des médias remplissant les fonctions d'agent de l'étranger du ministère de la Justice à cette adresse : https://minjust.gov.ru/ru/documents/7755/ (consulté le 22 août 2021).

37 https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2017-10/Valeeva_Open%20data%20and%20investigative%20journalism%20in%20Russia.pdf (consulté le 13 février 2023).

38 https://data.gov.ru/sites/default/files/presentation/prezentaciya_kuzmicheva.pdf (consulté le 13 février 2023).

39 Entretien avec un expert, Moscou, 14 septembre 2017.

Navalny, accusant les fils du procureur général Iouri Tchaïka de corruption, leurs noms sont remplacés par les combinaisons de lettres et de chiffres « LSDU3 » et « YFYAU9 » dans Rosreestr. Selon A. Navalny, il s'agit d'une conséquence directe de son enquête. Depuis cette première polémique, les soupçons de manipulation des données ouvertes se multiplient. En décembre 2020, le site *Meduza* rapporte que les autorités ont cessé de publier les données fiscales de nombreuses entreprises. Les journalistes notent que certaines données, qui par le passé avaient permis des enquêtes sur la corruption, sont manquantes. En janvier 2021, *Meduza* affirme que Rosreestr a caché des données sur les biens immobiliers de l'homme d'affaires Mazaraki, soupçonné de malversations, dans le registre unifié des biens immobiliers de l'État (UGRN). Rosreestr disposait d'informations classifiées sur les biens immobiliers de la famille Mazaraki.

En décembre 2020, une loi est adoptée qui interdit la publication de données sur les forces de sécurité, les juges et les hauts fonctionnaires, même si leur vie n'est pas en danger (ironiquement appelée « loi sur le droit de LSDU3 »). Le 15 décembre 2021, le Conseil de la Fédération envisage de limiter l'accès à Rosreestr. Pour le journal d'État *Rossijskaïa Gazeta*, la fermeture de l'accès à Rosreestr est justifiée par la nécessité de protéger les « données personnelles » et de lutter contre les criminels qui veulent s'emparer des biens immobiliers. Les journaux indépendants y voient une nouvelle forme de censure. Une journaliste est pessimiste quant à l'avenir des données ouvertes en Russie :

> « Il y a beaucoup d'exemples où l'administration publie des données puis cesse de les transmettre. Parfois, un ministre donne l'ordre de publier des données puis son successeur donne l'ordre inverse. (…) Malheureusement, cela est parfois lié au travail des journalistes, surtout dans les domaines sensibles comme la santé ou l'exécution des peines. Cela m'est arrivé. J'ai publié un article sur le manque de médecins où j'ai comparé les soins en oncologie dans différentes régions. Après cela, la rubrique sur le site du ministère de la santé qui publiait ces données a été bloquée par un mot de passe »[40].

Elle cite le cas d'un collègue travaillant sur les questions pénitentiaires, dont les données ont été bloquées après la publication d'un article. Beaucoup de régions ferment leurs portails de données ouvertes et renoncent à les publier. Les données relatives au niveau de vie sont les plus difficiles à obtenir. Comme l'explique Ivan Begtine, de l'association Infokultura, « Dans notre pays, l'État répond de tout et les indicateurs de qualité de l'enseignement, de la criminalité ou de la santé sont très politisés. Les propriétaires de données ont peur qu'elles

40 Entretien avec une journaliste, en ligne, 8 décembre 2020.

révèlent la médiocrité de leur travail et l'État a peur visiblement de publier ces données »[41].

Les données dans la guerre, la guerre des données

Suite au lancement de l'offensive militaire russe contre l'Ukraine, les spécialistes des données s'inquiètent des conséquences du conflit sur leur accès aux sources numériques. Alors que les rumeurs se développent concernant les chiffres réels de la mobilisation, l'ampleur des pertes militaires ou les effets des sanctions sur l'économie russe, les données officielles deviennent progressivement inaccessibles. Cette dynamique est constatée sur la chaîne Telegram « Données ouvertes RU » (*Otkrytye dannye RU*, environ 2700 membres en novembre 2022)[42]. Ivan Begtine, l'un de ses animateurs, publie le 26 février, deux jours après l'offensive, un « guide pour l'archivage rapide des matériaux numériques ». Il écrit : « Actuellement, alors que se produisent des événements catastrophiques, que des actions militaires se déroulent, de grands volumes de textes, d'images ou de vidéos sont publiés, qui peuvent être inexacts et disparaître quelques heures après leur publication. L'archivage numérique est plus important que jamais ». Le 3 mars, il publie des conseils sur l'archivage, expliquant : « Il semble que, dans les mois à venir, ce sera un défi majeur d'archiver ce qui pourrait très bientôt être détruit, supprimé, désactivé, bloqué. Les plus grands risques se situent au niveau de la fermeture qui se produit lorsqu'une organisation est liquidée. Par exemple, la liquidation de [l'association] Memorial ou maintenant la liquidation de *Ekho Moskvy* [le média *Echos de Moscou*] ».

Différents témoignages confortent l'idée de la disparition des données publiques. Le 4 mars, Max constate que les résultats des votes à la Douma ne sont plus publiés depuis le 22 février. Maksim lui répond : « À la guerre comme à la guerre. Les données sont ouvertes sur ordre ». En mars, Maria constate : « Dans l'enfer de tout cela, j'ai remarqué que de nombreux services avec des données ouvertes ne fonctionnent plus, de nombreux jeux de données sont tout simplement absents des sites web des administrations. Même http://data.gov.ru est en panne depuis un mois ». Elle évoque le risque que l'institution des données ouvertes disparaisse de Russie à l'avenir et que les données soient données « à la demande », à la merci des décisions bureaucratiques. En avril, Ivan Begtine confirme que « le niveau d'ouverture diminue d'année en année. De nombreux portails régionaux de données ouvertes sont fermés, sur la moitié d'entre eux les données ne sont pas actualisées depuis au moins deux ans ». Miroff lui rétorque : « Vous donnez

41 Količestvo otkrytyh dannyh v Rossii rastet, a ih kačestvo – net. *CNews*, 14 juillet 2021. https://www.cnews.ru/news/top/2021-07-14_kolichestvo_otkrytyh_dannyh (consulté le 13 février 2023).

42 https://t.me/opendatarussiachat (consulté le 13 février 2023).

l'impression que le niveau d'ouverture était élevé auparavant. Pour les régions, l'ouverture des données a toujours été un devoir vide de sens imposé par la mode fédérale ». À l'épreuve de la guerre, les journalistes et citoyens font l'expérience de la dégradation et de la disparition des données ouvertes. Cette dynamique met en lumière la fragilité des sources dans le monde numérique russe sous contrôle autoritaire.

Conclusion

Dans la Russie des années 2010, le *data journalism* se développe, s'appuyant sur les données publiques, achetées, fuitées ou volées pour mener des enquêtes, sur des thèmes allant de la corruption aux inégalités sociales en passant par les questions de santé et d'environnement. Ce fort engouement traduit une conception quantitative et objective de l'enquête, en cohérence avec les méthodes des consortiums transnationaux du journalisme d'investigation. Cette objectivation de l'investigation est alimentée par l'ouverture et la massification des données disponibles. Les enquêtes, qui font parfois scandale, suscitent une réponse des institutions sécuritaires qui répriment les journalistes et placent les données au cœur de conflits d'appropriation entre les enquêteurs et les administrations publiques. Suite à des révélations embarrassantes, des données disparaissent ou sont travesties. Elles sont enrôlées dans des luttes d'usage et d'interprétation, dont témoignent de nombreux journalistes qui voient se refermer des données ouvertes et s'interrogent sur la qualité de celles publiées. Leur confiance dans les chiffres est ébranlée, ce qui remet en cause la conception objective et positive du recours aux données pour faire place à une réflexion sur leur construction. En Russie comme ailleurs, la donnée ouverte est prise dans les dispositifs politiques, culturels ou économiques qui la construisent. O. Dovbysh [2021] rappelle que le journalisme de données repose sur des données dont la production est cadrée par des relations de pouvoir. Avec la guerre, l'enjeu stratégique de l'accès aux données numériques est plus manifeste encore, suscitant des conflits d'appropriation et d'interprétation à usage militaire. Ces tensions montrent les enjeux politiques liés aux données et nourrissent la réflexion sur les conditions de production des savoirs dans le monde actuel. Elles conduisent les enquêteurs à dénaturaliser l'usage des données et à rompre avec l'« imaginaire cybernétique » [Supiot, 2015] pour développer de nouvelles réflexivités numériques et politiques à l'heure de l'affrontement militaire.

Références bibliographiques

[Alloing, 2016] Alloing, Camille, « La sousveillance. Vers un renseignement ordinaire. » *Hermès*, n° 76, p. 68-73.

[Anderson, 2018] Anderson, Christopher William, *Apostles of Certainty. Data Journalism and the Politics of Doubt*, Oxford University Press.

[Ausserhofer, 2020] Ausserhofer, Julian, et al., « The datafication of data journalism scholarship: Focal points, methods, and research propositions for the investigation of data-intensive newswork, » *Journalism,* vol. 21, n° 7, p. 950-973.

[Begtin, 2013] Begtin, Ivan, « Gotovy li my k žurnalistike dannyh ? » (Sommes-nous prêts pour le journalisme de données ?), *Polit.ru*.

[Bigot, 2017] Bigot, Laurent, « Le fact-checking ou la réinvention d'une pratique de vérification. » *Communication langages,* 2, p. 131-156.

[Bounegru & Gray, 2021] Bounegru, Liliana, Gray, Jonathan (dir.), *The Data Journalism Handbook : Towards a Critical Data Practice*, Amsterdam, Amsterdam University Press.

[Boullier,2015] Boullier, Dominique, « Les sciences sociales face aux traces du big data. » *Revue française de science politique,* vol. 65, n° 5, p. 805-828.

[Carson, 2019] Carson, Andrea, « New Frontiers: Big Data, Leaks, and Large-Scale Investigative Journalism, » in *Investigative Journalism, Democracy and the Digital Age*. Routledge, p. 171-193.

[Chupin & Daucé, 2016] Chupin, Ivan, & Daucé, Françoise, « Par-delà la contrainte politique ? La banalité des bifurcations dans les carrières journalistiques en Russie contemporaine, » *Réseaux*, n° 199, p. 131-154.

[Chupin & Daucé, 2017] Chupin, Ivan & Daucé, Françoise, « Termination of Journalists' Employment in Russia: Political Conflicts and Ordinary Negotiation Procedures in Newsrooms », *Laboratorium*, vol. 9, n° 2, p. 39-58.

[Coddington, 2015] Coddington, Mark, « Clarifying journalism's quantitative turn: a typology for evaluating data journalism, computational journalism, and computer-assisted reporting, » *Digital journalism,* vol. 3, n° 3, p. 331-348.

[Dagiral & Parasie, 2017] Dagiral, Éric, & Parasie, Sylvain, « La « science des données » à la conquête des mondes sociaux: ce que le « Big Data » doit aux épistémologies locales, » in *Big data et traçabilité numérique: Les sciences sociales face à la quantification massive des individus,* Paris, Collège de France, p. 85-104.

[Daucé, 2019] Daucé, Françoise, « Épreuves professionnelles et engagement collectif dans la presse en ligne à Moscou (2012-2019) », *Le Mouvement social* n° 269, p. 101-116.

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

[Dovbysh, 2021] Dovbysh, Olga, « Trust and reliability of data in authoritarian regime: Practices of data journalism in Russian newsrooms ». Conférence « Automation and data-driven journalism beyond the Western World », 5-6 mai.

[Flichy, 2012] Flichy, Patrice, *L'Imaginaire d'Internet*,Paris, La Découverte.

[Giry, 2017] Giry, Julien (dir.), « Les théories du complot à l'heure du numérique », *Quaderni*, n° 94.

[Glazunova, 2020] Glazunova, Sofia, « Four Populisms » of Alexey Navalny : An Analysis of Russian Non-Systemic Opposition Discourse on YouTube », *Media and Communication*, vol. 8, n° 4.

[Gray et al, 2012] Gray, Jonathan, Chambers, Lucy, & Bounegru, Liliana, *The Data Journalism Handbook: How Journalists Can Use Data to Improve the News*, O'Reilly Media, Inc.

[*Hérodote*, 2022] « OSINT. Enquêtes et terrains numériques », *Hérodote*, vol. 186, n° 3.

[*Interfaces numériques*, 2020] « Entre data journalisme et pratique infographique », *Interfaces numériques*, vol. 9, n°3.

[Lapoix, 2014] « Le data journalisme : entre retour du journalisme d'investigation et fétichisation de la donnée. Entretien avec Sylvain Lapoix », *Mouvements*, vol. 79, n° 3, p. 74-80.

[Koltsova, 2006] Koltsova, Olessia, *News Media and Power in Russia*, Routledge.

[Lemieux,1992] Lemieux, Cyril, « Les journalistes, une morale d'exception? » *Politix,* vol. 5, n° 19, p.7-30.

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

[Loveluck, 2016] Loveluck, Benjamin, « Vers une économie politique des données : le pouvoir à l'aune des *data* », in Bourcier, Danièle, & De Filippi, Primavera, *Open Data & Big Data. Nouveaux défis pour la vie privée*, Paris, mare & martin, p. 245-262.

[Lowrey et al, 2019] Lowrey, Wilson, Broussard, Ryan, & Sherrill, Lindsey A., « Data journalism and black-boxed data sets, » *Newspaper Research Journal*, vol. 40, n° 1, p. 69-82.

[Mann et al, 2002] Mann. Steven, Nolan, Jason & Wellman, Barry, « Sousveillance : Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments », *Surveillance & Society*, vol. 1, n° 3, p. 331-355.

[Milan & Van der Velden, 2016] Milan, Stefania, & Van der Velden, Lonneke, « The alternative epistemologies of data activism, » *Digital Culture & Society,* vol. 2, n° 2, p. 57-74.

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

[Parasie & Dagiral, 2013] Parasie, Sylvain & Dagiral, Éric, « Des journalistes enfin libérés de leurs sources? Promesse et réalité du « journalisme de données », *Sur le journalisme, About journalism, Sobre jornalismo,* vol. 2, n° 1, p. 52-63.

[Parasie & Dagiral, 2013] Parasie, Sylvain, & Dagiral, Eric, « Data-driven Journalism and the Public Good: 'Computer-assisted Reporters' and 'Programmer-Journalists' in Chicago, » *New Media and Society* vol. 15, n° 6, p. 853-871.

[Parasie, 2013] Parasie, Sylvain, « Des machines à scandale : Éléments pour une sociologie morale des bases de données », *Réseaux*, n° 178-179, p. 127-161.

[Rostova, 2019] Rostova, Natalia, « Saving their Profession : Russian Journalists and Their New Media », in *The Russia File*, Wilson Center.

[Roudakova, 2017] Roudakova, Natalia. *Losing Pravda: Ethics and the press in post-truth Russia*, Cambridge University Press.

[Shilina & Shilina, 2019] Shilina, Alexandra, & Shilina, Marina, « Towards Data Journalism in Russia? », in Mutsvairo B., Bebawi S., Borges-Rey E. (dir.) *Data Journalism in the Global South*, Cham, Palgrave Macmillan.

[Stalph & Borges-Rey, 2018] Stalph, Florian & Borges-Rey, Eddy, « Data journalism sustainability: An outlook on the future of data-driven reporting, » *Digital Journalism* vol. 6, n° 8, p. 1078-1089.

[Supiot, 2015] Supiot, Alain, *La Gouvernance par les nombres. Cours au Collège de France (2012-2014)*, Paris, Fayard.

[Valeeva, 2017] Valeeva, Anastasia, *Open Data in a Closed Political System : Open Data Investigative Journalism in Russia.* Thomson Reuters Foundation.

[Vauchez, 2019] Vauchez, Ysé, « Les mythes professionnels des fact-checkeurs. » *Politiques de communication* 1: 21-44.

[Yablokov, 2018] Yablokov, Ilya. *Fortress Russia: Conspiracy theories in the post-Soviet world.* John Wiley & Sons.

[Young et al, 2018] Young, Mary Lynn, Hermida, Alfred, & Fulda, Johanna, « What makes for great data journalism? A content analysis of data journalism awards finalists 2012–2015, » *Journalism Practice* vol. 12, n° 1, p. 115-135.

Chapitre 6

Les droits d'auteur et les livres en ligne : contrôle des contenus, transgressions, espaces de liberté

Bella Ostromooukhova

Le 9 octobre 2015, le tribunal municipal de Moscou a ordonné le blocage permanent de rutracker.org, la plateforme russe la plus populaire de partage de contenus, suite à une plainte pour non-respect du droit d'auteur déposée par la maison d'édition Eksmo, l'un des majors de l'industrie du livre russe. Cette action a été rendue possible par l'entrée en vigueur, la même année, d'une version amendée de la loi 364-FZ, dite « loi antipirate », permettant le blocage définitif de plateformes ne respectant pas les droits d'auteur. L'association *Roskomsvoboda*, émulation du Parti pirate russe [Daucé, 2022], a alors lancé une campagne qu'elle a nommée « la bataille pour le Runet » où elle déclarait que ce blocage (ainsi que la dizaine d'autres qui l'ont précédé) était anticonstitutionnel et qu'il bafouait certains droits fondamentaux comme la liberté de la presse et d'opinion[1].

La question des libertés – y compris sur le plan numérique – se trouve ainsi articulée aux problématiques de définition et de protection des droits d'auteur en ligne. L'accessibilité ou non de certains contenus est en effet conditionnée par l'autorisation de l'ayant droit (que celui-ci soit l'auteur, le producteur ou l'éditeur) qui a le pouvoir de rendre payant, voire de restreindre, l'accès à tel ou tel produit culturel. L'espace en ligne se trouve ainsi cloisonné à deux niveaux : d'une part, des individus ou compagnies privées peuvent instaurer des barrières d'accès aux contenus dont les droits leur appartiennent, et, d'autre part, les États définissent les normes nationales en matière de protection de ces droits et se chargent de les faire respecter. Les mesures restrictives – comme le blocage de sites ne respectant pas les limitations imposées– font l'objet de contestation des défenseurs des droits numériques au même titre que d'autres types de censure en ligne car les droits d'auteur peuvent devenir un instrument ou un enjeu de lutte politique ou idéologique. En effet, certains contenus contestataires en ligne sont

1 https://roskomsvoboda.org/13913 (consulté le 15 décembre 2022).

censurés sous prétexte d'infraction au *copyright*[2]. Depuis l'invasion de l'Ukraine par la Russie, la question du respect des droits d'auteur est cependant revisitée. La vente des droits pour des produits culturels entre la Russie et l'étranger est entravée par les sanctions et le retrait des grands acteurs des industries culturelles du marché russe, induisant l'incitation au non-respect du droit d'auteur de la part des autorités[3] et le retour en force des pratiques de contournement, officiellement en recul depuis une décennie[4].

Les normes en matière de droit d'auteur sont définies et amendées au niveau national, en rapport avec les accords internationaux qui fixent un cadre commun[5], en laissant toutefois une certaine marge de manœuvre pour chaque pays [Martin-Prat, 2014 ; Zasurskij, 2016, p.16-48]. Ceux-ci composent ainsi, chacun à sa façon, entre un modèle français du droit d'auteur, centré sur le droit moral du créateur de l'œuvre, et le modèle anglo-saxon centré sur les droits patrimoniaux de ceux qui assument la responsabilité économique de sa production et de sa diffusion [Benamou & Farchy, 2009]. Ces deux modèles ont toutefois tendance à se rapprocher et à converger au cours du XX^{e} siècle [Baudel, 1998, p.52-57].

L'arrivée d'Internet a bousculé ces normes et a nécessité leur redéfinition. Conçu comme une plateforme de libre circulation de contenus par certains et comme un espace de nouveaux possibles économiques par d'autres, le cyber espace est devenu l'enjeu de luttes entre acteurs économiques, étatiques et associatifs. « Autour de la propriété intellectuelle se joue la bataille de nouvelles formes d'appropriation privée de connaissances et des frontières mouvantes entretenues avec le domaine à la libre disposition du public » [Benhamou & Farchy, 2009,

2 Par exemple, le 23 juillet 2022, « Saint Marienbourg », le dessin animé de l'animateur célèbre Oleg Kuvaev qui représente la vie des Pétersbourgeois lors d'une invasion imaginaire de la Russie par la Chine dans le but de rendre les Russes sensibles à l'horreur vécue par la population civile ukrainienne, est bloqué par YouTube suite à une prétendue utilisation frauduleuse de photographie portant atteinte aux droits de son auteur. L'infraction est ici un prétexte pour retirer un dessin animé condamnant la guerre en Ukraine.

3 Dmitri Medvedev a ainsi appelé, le 31 janvier 2023, à répondre aux nouvelles sanctions de l'Occident en légalisant l'utilisation d'objets de propriété intellectuelle occidentale sans payer de droits. https://www.vedomosti.ru/politics/news/2023/01/31/961116-medvedev-predlozhil-polzovatsya (consulté le 31 janvier 2022).

4 *Roskomnadzor* note que le nombre de plaintes pour usages frauduleux d'objets de propriété intellectuelle a augmenté de 20% en 2022. https://www.vedomosti.ru/technology/news/2023/01/23/960100-rkn-otmetil-rost (consulté le 23 janvier 2022).

5 La convention de Berne pour la protection des œuvres littéraires et artistiques a été adoptée en 1886 et signée par dix pays. Le nombre de signataires allait augmentant mais restait restreint, les États-Unis et l'URSS, par exemple, n'y ayant pas souscrit. La convention de Genève, dite également « La Convention universelle sur le droit d'auteur », élaborée sous l'égide de l'Unesco et signée en 1952, avait pour vocation de garantir le respect de la convention de Berne dans les pays qui n'avaient pas signé cette dernière.

p.114]. Alors que les GAFAM et les industries culturelles tendent à s'imposer sur le marché de la production et de la diffusion des contenus culturels en ligne [Waldfogel, 2018], leur action est diversement contestée et contournée. Outre les acteurs qui se mobilisent contre les répressions des fraudes ou cherchent à étendre le domaine public, nombreux sont ceux qui diffusent et consomment les contenus culturels en dépit des interdits commerciaux. Ces personnes relèvent d'un ensemble plus large généralement désigné par le nom de « hackers », qui prend sa source dans l'univers de la *computer science* américaine des années 1960 et s'est ensuite diversifié, englobant une multitude de pratiques, de sphères d'action et de domaines culturels, impliquant diverses grammaires politiques [Turner, 2006], de l'anarchisme et autonomisme au libertarianisme [Maxigas, 2012], parfois en conjuguant plusieurs d'entre elles [Coleman, 2012]. Le point commun aux différents hackers réside dans leur « répertoire d'action en ligne » [Van Laer and Aelst, 2010] : quel que soit l'objet du « hacking », ils enfreignent une barrière, technique ou symbolique, pour accéder à un contenu caché aux yeux du commun des mortels, souvent en « réaction à un certain mode d'échanges commerciaux, et aux pratiques de contrôle qui en découlent » [Bacot and Canonne, 2019, p.10].

Ce chapitre[6] montre comment l'État, les industries culturelles et les « *hackers* » cherchent à s'approprier le Runet autour d'un objet précis, le livre[7]. Loin d'être aussi lucrative et aussi massivement consommée que le cinéma ou la musique, cette branche est néanmoins très bien intégrée dans le marché mondial et investie par un fort capital symbolique par les autorités russes qui souhaitent redorer le blason du cliché soviétique de « la nation des grands lecteurs » [Ostromooukhova, 2019]. Dans un premier temps, nous allons esquisser la mise en place, en Russie, de l'appareil législatif des droits d'auteur depuis les années 1990 et la formation d'un marché légal des textes au format numérique, dans un contexte de libéralisation et d'ouverture du marché des biens culturels, puis d'instauration d'un contrôle étatique de plus en plus strict. Dans un second temps, nous montrerons comment ces contraintes sont déjouées par un type d'acteur, les « bibliothèques

6 Ce chapitre est une version mise à jour d'un article paru sur le même sujet [Ostromooukhova, 2021].

7 L'étude est basée sur une enquête qualitative qui comprend des entretiens semi-directifs, conduits à Moscou en février-mars et juin 2019, avec différents acteurs : avocats qui ont participé à l'élaboration de la législation « antipirate » et d'autres qui défendent les bibliothèques de l'ombre, membres d'ONG impliquées dans la négociation des limites de la légalité (Roskomsvoboda, Wikimedia.ru et Association des cyber éditeurs) et un représentant d'AAPI. Les entretiens avec les administrateurs de lib.ru (juin 2019) et Librusec (juillet 2020), complétés par une étude des discussions sur les forums de bibliothèques et les blogs personnels, menée en 2019-2023, permettent de mettre en évidence les stratégies de contournement et leur signification pour ces acteurs.

de l'ombre[8]» spécialisées dans les textes de fiction, qui s'évertuent à diffuser des livres au détriment des restrictions. Nous montrerons l'évolution des techniques de survie à travers quelques études de cas emblématiques : lib.ru, également appelé «bibliothèque de Moshkow», créée dès avant la chute de l'URSS et dont la popularité a atteint son apogée à la fin des années 1990 ; Librusec[9], apparu en 2007, dont l'âge d'or se situe au milieu des années 2010 ; Flibusta[10], créée par quelques membres désillusionnés de la communauté Librusec en 2009 ; et Maxima library[11], qui reprend, en 2013, les bases de Librusec et Flibusta et essaie de se développer comme une plateforme «légale» avant d'être reléguée dans l'«ombre» deux ans plus tard.

Mise en place des contraintes liées au respect des droits d'auteur en ligne : logiques, acteurs, conflits

L'industrie du livre en Russie, dans l'acception occidentale de ce terme, apparaît après la chute de l'Union soviétique et l'introduction de l'économie du marché, de même que le droit d'auteur russe se redéfinit afin que cette nouvelle branche, tout comme les autres industries culturelles, puisse s'insérer dans le contexte économique mondial. L'arrivée massive d'Internet ouvre de nouvelles perspectives, permettant à la fois la libre circulation des textes et la formation du marché du livre numérique.

L'héritage soviétique

Avant 1917, le système d'édition russe était aligné sur les normes internationales, mis à part l'existence d'une «liberté de traduction» qui permettait la publication en russe d'ouvrages étrangers sans payer de droits. La révolution bolchévique entraîne un changement radical, qui conduit l'URSS à élaborer son propre système de production de livres et un droit d'auteur particulier. Dans la doctrine marxiste-léniniste, toute œuvre culturelle devait être accessible à l'ensemble de la population afin de contribuer à l'éducation des masses laborieuses. Le droit

8 Le terme «pirate», fréquemment utilisé dans le langage courant, possède de multiples connotations qui sont souvent instrumentalisées par les acteurs. Stigmatisés par certains ayant droits ou leurs défenseurs qui mettent en avant l'aspect hors la loi voire «terroriste» de leurs actions, les «pirates» se désignent souvent volontiers comme tels, en raison de l'idée de liberté et de puissance attachée à cette notion [Keucheyan, 2008]. Afin de me distancier de ces significations supplémentaires, j'appellerai notre objet d'étude, à l'instar de Joe Karaganis [2018], les «bibliothèques de l'ombre», en utilisant le mot «pirate» ou «piratage» uniquement lorsqu'il est utilisé par les acteurs eux-mêmes.

9 https://librusec.pro/ (consulté le 31 janvier 2022).

10 http://flibusta.is/ (consulté le 31 janvier 2022).

11 http://maxima-library.org/ (consulté le 31 janvier 2022).

moral, qui existait dès l'instant qu'une œuvre était créée, demeurait inaliénable et appartenait à l'auteur, mais pour une durée limitée et bien plus courte que dans les pays ayant souscrit à la convention de Berne pour la protection des œuvres littéraires et artistiques (1886) : vingt-cinq ans à partir de la publication ou quinze ans après la mort de l'auteur pour les œuvres posthumes. Les droits patrimoniaux, quant à eux, pouvaient être cédés pour une courte durée aux entreprises d'État qui s'occupaient de la production et de la diffusion des biens culturels. Par ailleurs, il existait une très longue liste d'usages gratuits d'une œuvre qui permettait de la diffuser le plus largement possible. L'Union soviétique avait par ailleurs conservé la « liberté de traduction » des œuvres étrangères de la Russie tsariste. Bien que l'URSS ait adhéré à la Convention universelle des droits d'auteur en 1973, un certain degré de liberté à l'égard des titulaires de droits étrangers avait subsisté, y compris dans les premières années post-soviétiques [Elst, 2005, p. 65-90].

Étroitement contrôlée par la censure, la production culturelle de l'État était concurrencée, dans la période post-stalinienne, par une importante production et diffusion artisanale d'œuvres, le *samizdat*, qui regroupait les personnes qui recopiaient et faisaient circuler de façon clandestine des textes dactylographiés (monographies, anthologies, tracts, périodiques) interdits par la censure soviétique ou rejetés par les maisons d'édition, contournant à la fois les questions de droit d'auteur et de censure [Zaslavskaya, 2015]. Cette pratique n'était pas illégale tant que les œuvres produites et distribuées en dehors des canaux officiels n'étaient pas vendues [Elst, 2005, p.34]. Dans la pratique, cependant, la production et la distribution informelles de textes non censurés étaient considérées comme des activités criminelles contribuant à la diffusion de contenus politiquement nuisibles, et les personnes impliquées étaient sévèrement réprimées. Néanmoins, un marché noir des biens culturels (incluant le *Samizdat, le Tamizdat*[12] ou la production culturelle officielle détournée de ses canaux de diffusion habituels) a proliféré dans les années 1970-1980 : ce type d'activité commerciale était interdit par la loi mais toléré par l'État soviétique comme une façon de parer aux lacunes de l'économie planifiée [Thiesse & Schmatko, 1999, p.77].

L'après 1991 : aligner le droit d'auteur russe sur les normes internationales pour s'insérer dans le marché mondial

Après la chute de l'Union soviétique, la production culturelle russe se privatise, se polarise et entreprend de s'insérer dans la production mondiale en nouant des partenariats avec les grandes compagnies étrangères. L'afflux massif de films, de musiques et de livres étrangers auparavant difficilement accessibles se fait

12 Manuscrits exportés clandestinement et publiés en Occident, puis réintroduits, toujours clandestinement, en URSS.

souvent par des canaux parallèles, au détriment du *copyright* [Kiria & Sherstoboeva, 2015 ; Thiesse & Schmatko, 1999], en utilisant des supports physiques mais aussi en investissant les opportunités offertes par l'Internet, dont l'usage se banalise progressivement en Russie au cours des années 1990-2000.

Toutefois, afin de rassurer les partenaires étrangers et rendre le marché russe attractif, la législation russe du droit d'auteur est progressivement alignée sur les normes mondiales. La loi n° 5351-1 sur la propriété intellectuelle et les droits voisins, adoptée en 1993, porte la durée de la protection à cinquante ans après la mort de l'auteur, ce qui était préconisé par la Convention de Berne à laquelle la Russie adhère en 1995. La loi a également exclu les cas de libre utilisation prévus par la législation soviétique, a reconnu des droits voisins auparavant inexistants et permis l'apparition d'organisations responsables de la gestion collective des droits de propriété intellectuelle (DPI).

Dès les années 1990, le gouvernement russe entame des négociations pour adhérer à l'Organisation mondiale du commerce (OMC) qui n'aboutissent qu'en 2012. Dans la perspective de cette adhésion, des entreprises américaines, telles que Microsoft, la *Motion Picture Association of America* (MPAA) et la *Recording Industry Association of America* (RIAA), exigent de la Russie un engagement plus ferme en matière de protection des DPI. Pour répondre à ces attentes et donner des garanties à ces partenaires étrangers, la durée du droit d'auteur a été étendue, en 2004, à soixante-dix ans, s'alignant ainsi sur le *Copyright Term Extension Act* américain de 1998 [Alekseeva et al., 2013, p.69]. Au même moment, la loi sur la propriété intellectuelle et les droits connexes a été amendée pour y inclure les utilisations numériques des œuvres [Rassolov, 2016], conformément au *Digital Millennium Copyright Act américain* (DMCA) de 1998. Cependant, cette loi n'a été appliquée que de manière sporadique, notamment en raison de l'absence de mécanisme d'application.

En élaboration depuis les années 1990, la partie IV du Code civil de la Fédération de Russie, dédiée aux droits d'auteur, a été adoptée en 2006. Immédiatement après son entrée en vigueur, le 1er janvier 2008, le président Medvedev a ordonné sa révision. Il s'agissait, en effet, de trouver un compromis entre plusieurs exigences : d'une part, inclure les normes fixées par l'Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce (ADPIC) [Alekseeva et al., 2013, p.62] qui allaient dans le sens d'une forte protection des droits, et d'autre part, répondre aux revendications des professionnels de l'Internet, comme l'Association russe des communications électroniques (RAEK), fondée en 2006, et des associations de défense des libertés sur Internet comme Wikimedia.ru et l'Association des cyber éditeurs, qui aspiraient à créer un mécanisme simplifié d'interaction entre les titulaires de droits et les intermédiaires de l'information,

et de légaliser les licences ouvertes en Russie [Alekseeva et al., 2013, p.72]. Le président Medvedev s'est rangé aux côtés de ces experts qui aspiraient à davantage de souplesse de la législation : en 2008, il a appelé à « limiter la responsabilité des intermédiaires de l'information pour les contenus téléchargés par les utilisateurs » [Zasurskij, 2016, p.54].

« Combattre le piratage » : l'un des volets du contrôle du Runet dans les années 2010

Cependant, la politique de l'État change brusquement en 2012, avec le retour de V. Poutine à la présidence de la Fédération de Russie. Dès le début de son nouveau mandat, celui-ci approuve une série d'initiatives législatives visant à intensifier le contrôle de l'État sur l'Internet national [Soldatov & Borogan, 2016]. La loi fédérale n° 139 de 2012, connue sous le nom de « loi sur les listes noires », qui implique la constitution d'un registre des sites web au contenu « illégal » (c'est-à-dire fournissant des informations sur les drogues, la pédopornographie et le suicide, ou alors relevant de la vague catégorie de l'« extrémisme »), a été parmi les premières, fournissant ainsi un outil de censure des contenus en ligne. Un an plus tard, en 2013, des députés de la Douma soumettent un projet de loi visant à appliquer le même mécanisme aux sites internet qui ne respectent pas les droits d'auteur. Il s'agissait de mettre en place des outils de répression, jusqu'ici absents, contre les infractions faites aux droits d'auteur en ligne. V. Poutine se range alors clairement du côté des ayants droit et la Douma approuve la loi fédérale n°187, également appelée par ses détracteurs la « loi anti-pirate », la « loi contre Internet » ou encore le « SOPA russe ». En effet, elle fait écho aux projets de loi américains de 2011 *Stop Online Piracy Act* (SOPA) et *Protect Intellectual Property Act* (PIPA), qui visaient également à investir l'État du pouvoir de « mettre à contribution les gérants des plateformes en ligne afin de faire respecter les intérêts des industries du copyright » [Nowak, 2016, p.178]. Mais si le tollé soulevé par les lois SOPA et PIPA dans la société américaine fait reculer les législateurs aux États-Unis [Herman, 2012, p.215-216], le gouvernement russe s'est montré imperméable aux mobilisations contre la loi « anti-pirate », pourtant nombreuses [Zasursky, 2016, p.62-63]. Les critiques ont établi un parallèle entre la « loi sur les listes noires » et la « loi anti-piratage », étant donné la similitude des mécanismes de répression qu'elles mettent en place et des acteurs qu'elles impliquent (le tribunal municipal de Moscou, l'agence *Roskomnadzor*). Cela a créé une convergence des luttes autour de ces deux problèmes distincts (blocages de sites en raison de leur contenu indésirable ou pour le non-respect du droit d'auteur). Les actions de protestation conduites par les acteurs de l'Internet russe tels que Wikimedia.ru ou Yandex ont été nombreuses et similaires à celles des plateformes américaines mobilisées contre SOPA [Alekseeva et al., 2013, p.81-85], la pétition lancée par l'organisation

de défense des droits numériques *Roskomsvoboda* créée en 2012 [Daucé, 2022] a recueilli 100 000 signatures [*Antipiratskij zakon*, 2017, p. 47], RAEK a produit des rapports sur les dommages que cette loi allait causer à l'industrie de l'Internet et aux ayants droit eux-mêmes.

Malgré cette mobilisation de divers acteurs, la loi a été adoptée et s'est ensuite renforcée au fil des ans, s'étendant à un plus grand nombre de contenus et englobant de nouveaux acteurs. Sa première version, qui ne s'appliquait qu'aux contenus audiovisuels, établissait la marche à suivre juridique et désignait les « intermédiaires informationnels » (administrateurs de sites, hébergeurs et FAI) comme responsables de la légalité des contenus. Les amendements entrés en vigueur le 1er mai 2015 ont étendu la protection du droit d'auteur à tous les produits culturels au format numérique, en dehors de la photographie. L'accord à l'amiable entre les ayants droit et les « intermédiaires informationnels », fréquemment pratiqué auparavant, a été rendu plus difficile. Les sanctions ont également été renforcées. Notamment, le tribunal municipal de Moscou a obtenu le droit de bloquer définitivement et irrévocablement des sites en cas d'infractions multiples.

Les blocages qui ont suivi, dont celui de *Rutracker*, ont induit de nombreuses tactiques de contournement, que les amendements subséquents de la législation ont cherché à contrer. Ainsi, les amendements entrés en vigueur le 1er octobre 2017 permettaient à *Roskomnadzor* de bloquer les « miroirs » créés par les sites de l'ombre. L'étape suivante consistait à bannir les plateformes ne respectant pas les droits d'auteur des résultats de moteurs de recherche et des réseaux sociaux. Les chaînes de télévision appartenant à Gazprom Media ont intenté, en 2018, un procès au moteur de recherche Yandex suite à la présence de liens vers des contenus illicites sur le service Yandex.video. Ce procès s'est soldé par la signature, le 1er novembre 2018, d'un mémorandum par les majors de l'industrie internet russe (Yandex, Mail.ru et Rambler) qui s'engageaient à supprimer les liens vers les contenus audiovisuels illégaux de leurs moteurs de recherche. Une nouvelle version de ce mémorandum, incluant davantage d'acteurs dont VKontakte, et englobant les livres (exclus de sa première version principalement dédiée au contenu audiovisuel), a été signée en janvier 2022, en attendant une nouvelle version de la loi « antipirate ».

Les messageries (notamment Telegram) et les applications mobiles deviennent, à la fin des années 2010, un moyen commode pour diffuser les contenus en contournant le *copyright*. Une nouvelle loi[13], entrée en vigueur en octobre 2020, rend ces applications et leurs agrégateurs App Store et Google Play et Huawei

13 Loi numéro 177-FZ du 08 juin 2020 http://publication.pravo.gov.ru/Document/View/0001202006080030? index=1&rangeSize=1 (consulté le 12 décembre 2022).

AppGallery responsables de la diffusion de contenus illégaux. Ces compagnies étrangères, sans être obligées de se plier aux lois russes, réagissent toutefois assez volontiers aux plaintes. En ce qui concerne Telegram, après la levée du blocage de cette messagerie en 2020, la chaîne collabore assez activement avec les majors de l'industrie du livre russe, en supprimant notamment les canaux visés par des plaintes, sans qu'il n'y ait de dispositif légal particulier l'y obligeant[14].

La lutte contre les contournements du copyright est donc portée par deux types d'acteurs : les industries culturelles étrangères (pour la plupart américaines) qui voudraient endiguer le contournement du DPI par des plateformes russes, et celle des compagnies russes soucieuses de protéger leur production dans le cyber espace national. Les plus grandes parmi ces dernières ont par ailleurs créé une organisation chargée de cette protection, AZAPI[15], au moment où la première version de la loi « antipirate » a été votée. La législation « antipirate », critiquée pour ses failles par certains et pour son caractère liberticide par d'autres, tente de donner des garanties à ces différents acteurs.

Les bibliothèques en ligne : l'art de survivre dans le cadre de la loi et en dehors

Dans cet environnement de plus en plus contraint et verrouillé, à la fois par les acteurs privés et étatiques, la diffusion de livres en format numérique se fait à la fois *via* un marché légal, monopolisé par les grandes entreprises, et à travers de multiples canaux informels dont certains se maintiennent dans le domaine légal et d'autres survivent dans l'illégalité. Ces différents canaux ont toutefois une origine commune, qui remonte à l'économie parallèle soviétique.

La formation du marché légal du livre numérique

Se procurer des textes en dehors des voies officielles faisait en effet partie de l'*habitus* des hommes et des femmes soviétiques de l'époque du socialisme tardif. Les livres jouant un rôle essentiel dans le système de valeurs soviétique, 68% des ménages des grandes villes achetaient des livres au marché noir afin de faire face à la pénurie de littérature à la mode [Stemakh, 2001, p. 146]. Ainsi, Maksim Moshkow, administrateur de lib.ru, l'une des premières bibliothèques en ligne russes, décrit les premiers échanges de textes numérisés entre les collaborateurs

14 https://gipp.ru/overview/ekspertnye-obzory/borba-s-piratami-kak-otstoyat-avtorskie-prava-v-telegram/ (consulté le 12 décembre 2022).

15 *Associaciâ po zašite avtorskih prav v internete* (Association pour la défense des droits d'auteur sur Internet), https://azapi.ru/ (consulté le 12 décembre 2022).

des instituts de recherche dans les années 1980 - début des années 1990, comme un moyen d'étancher sa « soif de lecture » ancrée dans cette pénurie de lectures de la fin de la période socialiste :

> « Nous étions habitués au fait que si un livre était bon, on ne pouvait pas l'acheter dans une librairie, il était forcément épuisé. Et à la bibliothèque, il fallait faire la queue et même là, on ne savait jamais si on pouvait l'emprunter. C'est pourquoi nous avions tous l'habitude de faire la chasse aux livres. Vous vous mettez au défi de trouver un texte précis, vous faites la queue, vous demandez autour de vous… Et puis un jour vous arrivez au travail et vous voyez que le livre qui vous manquait est juste là [sur le disque dur de l'ordinateur]. Et vous n'êtes pas dans une bibliothèque où vous devez le rendre, ni dans un magasin où il n'est jamais disponible, ni chez un spéculateur qui vous le vendrait quatre fois le prix normal… Voici le fichier - vous pouvez simplement le prendre, le copier sur votre ordinateur, et c'est tout »[16].

La numérisation manuelle de textes et son échange entre pairs était donc une pratique ancrée dans les milieux de l'*intelligentsia* technique dès avant la chute de l'URSS, la libéralisation du marché et l'arrivée de l'internet. Elle s'amplifie dans les années 1990, et le développement d'Internet lui donne une nouvelle impulsion. Des bibliothèques en ligne russophones prolifèrent et se diversifient dans les années 1990, sans se préoccuper du droit d'auteur. Ce n'est qu'à la fin des années 1990 que l'on voit apparaître, sur des forums de discussion et dans les médias consacrés à Internet, la conscience de la nécessité de tenir compte de la législation [Bodo, 2018].

Dans les années 2000, alors que les livres au format numérique deviennent progressivement attractifs pour les éditeurs traditionnels, émerge un marché des bibliothèques en ligne, entraînant la nécessité de tracer les frontières entre les acteurs « légaux » et « illégaux ». Ces dernières se définissent à travers une série de procès pour « piratage ». En 2004, *KM online*, une société en ligne spécialisée dans les produits éducatifs multimédia, tente de devenir une bibliothèque en ligne légale et payante et signe un contrat avec les principaux éditeurs russes. Elle intente alors un procès pour « piratage » contre les grandes bibliothèques adelbaran.ru et lit.ru, qui se solde par des amendes mineures pour les responsables des plateformes incriminées, mais qui les labellise désormais comme « illégales ». Ce même sort attend toutefois aussi le plaignant : en juillet 2006, un traducteur intente un procès contre *KM online* pour l'utilisation non autorisée de ses traductions, expulsant ainsi cette bibliothèque, à son tour, de la sphère légale.

16 Entretien avec Maksim Moshkow, le 4 juillet 2019.

Dans ce contexte, a été créée, en 2005, la société Litres, devenue la première grande librairie en ligne spécialisée dans la vente de livres électroniques. Ses fondateurs - des administrateurs de grandes bibliothèques de l'ombre – ont étudié les raisons de l'échec commercial de *MK online* et se sont donné pour but de créer un système plus fonctionnel et efficace. Ils ont en outre valorisé leur savoir-faire technique : l'un des fondateurs de la compagnie, Dmitri Gribov, était à la tête de l'équipe de développeurs du format de livre électronique FictionBook (FB2, ainsi que sa nouvelle version FB3 sortie en 2017[17]). Celui-ci est par la suite devenu le format le plus populaire sur le marché russe, promu par Litres [Haritonov, 2016, p.24]. Les fondateurs ont également mis en place un système de vases communicants entre les bibliothèques « illégales » qu'ils géraient et Litres. Ce dernier signait un contrat avec les écrivains qui lui cédaient les droits exclusifs de vente des livres électroniques, suite à quoi les versions « illégales » de leurs œuvres étaient retirées des bibliothèques de l'ombre qui redirigeaient leurs lecteurs vers Litres. La bibliothèque « légale » était donc largement alimentée par les ressources « illégales », qui continuaient à exister en parallèle. En 2009, les parts majoritaires de Litres ont été rachetées par les majors de l'édition russe AST et Eksmo qui en ont fait leur agent sur le marché du livre électronique.

Bookmate, une autre plateforme dédiée à la lecture en ligne, plus orientée vers le développement international, a été créée à peu près au même moment et s'est développée en parallèle. Fondée par un homme d'affaires britannique vivant en Russie et son partenaire russe, elle appartenait, depuis 2017, à la compagnie Bookmate Limited officiellement enregistrée en Irlande qui avait développé ses services dans de nombreux autres pays d'Europe, d'Asie et d'Amérique latine. Toutefois, suite à l'invasion de l'Ukraine par la Russie, cette compagnie irlandaise s'est retirée du marché russe en juillet 2022 avant d'être déclarée « média agent de l'étranger » en octobre de la même année. La plateforme Bookmate a été rachetée par Yandex, qui va poursuivre son développement à l'intérieur du territoire russe[18][17].

D'autres plateformes étrangères, comme le service *streaming* suédois de livres audio Storytel, qui a été l'acteur le plus important à occuper cette niche en Russie depuis 2017, se sont retirées du marché russe courant 2022. Ils ont ainsi laissé la place aux acteurs russes, et ont permis notamment à Litres et à Bookmate (depuis son rachat par Yandex) de s'agrandir davantage.

17 https://gorky.media/context/strannovatyj-fb3-otchet-federatsii-izdatelej-i-portret-pirata/ (consulté le 24 novembre 2022).

18 https://www.vedomosti.ru/media/articles/2022/06/30/929253-yandeks-pokupaet-bookmate (consulté le 24 janvier 2023).

Le marché du livre électronique a donc été monopolisé en Russie par des grands groupes et continue à l'être dans le contexte actuel, tout en se recentrant sur les majors nationaux depuis février 2022.

Rester dans les limites de la légalité

Face à ce marché, centré sur la production des grandes maisons d'édition russes, des plateformes de libre partage de textes ont continué à se développer, dans l'optique de pallier aux insuffisances de ce système, à savoir donner l'accès à des textes inaccessibles car trop anciens, trop rares ou publiés en dehors des grands circuits.

Certaines de ces plateformes arrivent à se maintenir dans les limites de la légalité, comme c'est le cas de lib.ru. Cette bibliothèque, commencée comme collection privée que son administrateur, Maksim Moshkow, a partagée dès les premiers pas d'Internet en Russie, a pris de l'ampleur dans les années 1990. La croissance exponentielle de la collection était assurée par le fonctionnement collaboratif de la bibliothèque : des enthousiastes numérisaient des livres à l'aide de scanners, les transformaient en fichiers texte grâce au programme FineReader qui s'est répandu en Russie dès 1994 et les envoyaient à Moshkow qui les ajoutait à sa collection après un bref travail de rédaction. Cette centralisation représentait un frein à la croissance : lorsque le flux de messages était devenu trop important, l'administrateur n'avait plus suffisamment de temps pour le gérer et a ralenti les mises à jour.

Attaqué en justice pour « piratage » en 2004[19], Moshkow a dû choisir, pour lib.ru, entre une certaine forme de légalité ou la survie en dehors du cadre légal ; il a opté pour la première solution en scindant sa bibliothèque en deux. Il a créé une nouvelle section qu'il a appelée « *Samizdat* », dédiée aux textes envoyés par leurs auteurs pour une première publication en ligne. Ne la considérant pas comme de la « vraie » littérature, car sa valeur n'avait pas été sanctionnée par un éditeur, Moshkow a accepté qu'elle soit mise en ligne de façon décentralisée. La section Samizdat a donc été équipée d'un programme permettant aux auteurs de télécharger eux-mêmes les textes, de sorte qu'elle puisse s'enrichir sans l'intervention de l'administrateur. Se développant activement depuis sa création, ce site est devenu une pépinière pour les maisons d'édition, qui y cherchent régulièrement de nouveaux talents. Une fois leur texte repéré et publié, il incombe aux auteurs de négocier avec la maison d'édition la présence ou non de leurs œuvres dans la bibliothèque de Moshkow.

19 https://www.ng.ru/telecom/2004-11-02/13_lib.html (consulté le 16 février 2023).

La partie « bibliothèque », qui contient les livres déjà publiés, a été gelée depuis la fin des années 2000 et expurgée des œuvres dont les ayants droits ont exigé le retrait. Outre l'inconvénient du fonctionnement centralisé susmentionné, Moshkow argue d'un changement de paradigme dans la fabrication des fichiers. La communauté qui alimentait la collection de lib.ru valorisait le travail manuel consistant à numériser des livres et à les convertir au format texte. Ce processus était considéré comme une pratique de « hacking » à laquelle était attachée une valeur ajoutée. Depuis que les livres électroniques produits par les maisons d'édition sont devenus monnaie courante, la numérisation de textes est devenue une pratique désuète, la communauté qui s'y consacrait s'est progressivement désintégrée, et le flux d'ouvrages scannés a progressivement diminué.

Ainsi, lib.ru représente aujourd'hui, d'une part, un lieu de stockage muséal pour les classiques libres de droits, et d'autre part un site d'autoédition, avec sa communauté d'auteurs à la recherche d'un public et d'un éditeur, ses règles de fonctionnement internes et son code de conduite envers les maisons d'édition, élaboré au cours des collaborations.

D'autres bibliothèques, plus récentes mais souvent bâties sur les archives de leurs prédécesseurs, et qui continuent à alimenter leurs bases, ont espéré se maintenir dans le domaine légal jusqu'au milieu des années 2010.

Maxima Library, par exemple, a d'abord essayé de montrer patte blanche, tactique qui s'était avérée efficace pour lib.ru. La page d'accueil du site affirme : « Nous sommes une bibliothèque libre pour des gens libres (…) Nous nous efforçons de garantir le libre accès aux œuvres sans enfreindre les droits de quiconque[20] ». Plus tard, les administrateurs annoncent sur le forum de la bibliothèque qu'ils avaient été contraints de retirer certains livres pour offrir un accès gratuit au reste. Néanmoins, malgré ces efforts, en décembre 2016, le site http://maxima-library.org a été bloqué en Russie. Le représentant de la bibliothèque sur le forum librusec.ucoz l'a annoncé de manière amère :

> « À cause de deux livres minables d'un certain Pereliaguin, qui se trouvent sur notre site depuis des lustres, nous sommes "bloqués à la demande des ayants droit". Mais aucun de ces assassins de livres n'a lu ces livres, ce n'est pas l'affaire des ayants droit de lire, leur affaire est d'empêcher les gens de lire (…) La Bibliothèque continue de fonctionner, bien sûr, tout le monde connaît les moyens et les méthodes de contournement (enfin, peut-être à part les membres de *Roskompozor*) »[21].

20 http://maxima-library.org/ (consulté le 16 février 2023).

21 http://librusec.ucoz.de/forum/27-2818-103197-16-1482497381 (consulté le 16 février 2023). Le terme de Roskompozor est formé par déformation de Roskomnadzor, croisé avec le mot « *pozor* » qui veut dire « la honte ».

Cette sortie de la sphère légale est saluée par les autres utilisateurs du forum qui, dans leurs commentaires, renversent le stigmate du blocage : « bienvenue ! », « enfin, vous êtes considérés comme une bibliothèque sérieuse »[22].

Il en va de même pour les autres bibliothèques mentionnées au début de ce chapitre, Librusec et Flibusta. Alors que ces plateformes ont pu maintenir des liens étroits avec le marché officiel jusqu'au début des années 2010, l'application de la « loi anti-piratage » a mis définitivement fin à ces zones grises et radicalise la dichotomie légal vs illégal. La plupart des bibliothèques de l'ombre, bloquées par *Roskomnadzor* avant la fin de l'année 2016, se sont consolidées autour de l'image d'un *underground* culturel et ont dû s'approprier, voire produire, des outils de résistance numérique.

Tactiques de survie dans l'illégalité

Les stratégies de survie développées aujourd'hui par les bibliothèques de l'ombre russes poursuivent trois objectifs principaux. Le premier consiste à assurer la pérennité et la croissance de leur collection, qui dépend à son tour de la vitalité de la communauté que le site fédère. Le second est d'assurer la sécurité personnelle des administrateurs qui endossent la responsabilité légale de la fraude présumée. Enfin, ces sites doivent garantir l'accès à leurs collections sur le territoire de la Fédération de Russie, où ils sont généralement bloqués en vertu de la « loi antipirate ».

Les bibliothèques de l'ombre constituent des communautés qui fédèrent lecteurs et administrateurs [Bodó, 2018]. Contrairement à lib.ru, Librusec, Flibusta et Maxima Library fonctionnent selon le modèle Wiki, où les textes et les notices sur les œuvres et les auteurs sont mis en ligne par les utilisateurs eux-mêmes. L'éventail d'actions accessibles à chaque utilisateur dépend de son ancienneté, de ses compétences (en codage, notamment) et des mérites au sein de la communauté (résolution de problèmes techniques ou un grand nombre de livres mis en ligne ou commentés). Toutefois, chaque membre connecté jouit de la possibilité de télécharger et de modifier le contenu de la bibliothèque. Cela a pu permettre aux administrateurs – très peu nombreux – de se dédouaner en cas de poursuites pénales : ils pouvaient écarter la responsabilité des contenus mis en ligne par les utilisateurs[23]. Cet argument n'est cependant plus valable depuis l'introduction de la notion d'« intermédiaires informationnels » par la législation « antipirate ».

22 *Ibid.*

23 Cf. par exemple, l'interview de l'administrateur de Librusec publié dans Livejournal : https://ya-parazit.livejournal.com/227533.html (consulté le 20 juin 2022).

Cette constitution collaborative des collections assure par ailleurs la possibilité de leur croissance exponentielle. Ilya Larin, administrateur de Librusec et développeur de formation, a mis le code source de sa bibliothèque en accès libre sur son site[24]. Cette pratique de partage du code est profondément ancrée dans la culture hacker dans laquelle la liberté d'expression et le partage du code sont intrinsèquement liés [Coleman, 2012, p.9]. L'entretien que l'auteure a mené avec Larin montre que ce partage du code et celui des textes constituent pour lui des garanties de la survie de l'écosystème :

> « Ils (Flibusta) ont emprunté le code source de mon site, ont copié mes archives. Beaucoup de bibliothèques ont utilisé le code source de Librusec. Depuis, elles ont évolué dans des directions différentes. Une pollinisation croisée se produit constamment : certains utilisateurs sont sur plusieurs bibliothèques à la fois, et quand un nouveau livre paraît, ils le téléchargent sur plusieurs sites à la fois. Il s'agit aujourd'hui d'une communauté assez dense, ce qui la rend plus pérenne. Si demain Flibusta disparaît, eh bien, il ne se passera rien »[25].

Cette « pollinisation croisée » garantit la pérennité des collections en multipliant les supports et les moyens de diffusion, grâce aux membres de ces communautés qui mettent à disposition leurs savoir-faire particuliers ou leur accès à des ressources spécifiques. Par exemple, tout utilisateur peut télécharger l'intégralité de la bibliothèque accompagnée d'un programme qui transforme l'archive en une base de données, rendant ainsi la navigation plus commode. Une fois la base de données complète installée sur l'ordinateur, l'utilisateur peut, mensuellement ou annuellement, télécharger ses mises à jour. Ainsi, la collection de la bibliothèque est répliquée de nombreuses fois et conservée non seulement en ligne, mais aussi hors ligne. Si la bibliothèque virtuelle venait à être supprimée du serveur, elle pourrait donc être restaurée à tout moment à partir des copies conservées par les utilisateurs, ce qui rend sa disparition totale impossible. Or, le moyen le plus pratique pour télécharger un gros volume de données, comme la bibliothèque ou ses mises à jour, est de recourir aux *torrents*. Les commentaires sur les principaux agrégateurs de *torrents* montrent que les distributions de mises à jour des bibliothèques sont l'œuvre d'un petit nombre de bénévoles. D'autres utilisateurs prennent ensuite le relais et distribuent les bases téléchargées par leurs propres moyens. Certaines bibliothèques de l'ombre ont leurs propres *torrents*, créés par les membres de la communauté.

Le serveur qui héberge la collection est également d'une grande importance pour la sécurité de la bibliothèque. La législation du pays où il est situé doit être suffisamment tolérante à l'égard des infractions au droit d'auteur. Sur les forums,

24 https://github.com/larin/librusec (consulté le 02 juillet 2022).

25 Entretien avec Ilya Larin, le 14 juillet 2020.

les administrateurs échangent des commentaires sur les « bons » et les « mauvais » emplacements. Larin affirme qu'il y a un équilibre à trouver entre les différents types de censure pratiquée par les législations nationales. Hébergé aux Pays-Bas, un pays perçu par Larin comme tolérant envers les sites pirates, Librusec y a été accusé de « pédopornographie » à cause d'un manuel soviétique d'éducation sexuelle représentant des enfants dénudés. Son administrateur a donc dû déplacer l'hébergement vers un autre pays[26]. Les différences dans les législations nationales sont ainsi instrumentalisées pour échapper aux contraintes.

Une sécurité supplémentaire est assurée par le choix de l'hébergeur. Certains, plus coûteux, se déclarent imperméables aux requêtes extérieures. Ils constituent ainsi un rempart contre les éventuelles plaintes des ayants droit qu'un hébergeur ordinaire satisferait sans entrer dans les détails.

Une autre tâche des administrateurs de bibliothèques est d'assurer leur sécurité personnelle. En effet, la législation « antipirate » les rend pénalement responsables du contenu illégal des sites qu'ils entretiennent. Deux tactiques existent : d'une part, l'éloignement géographique qui garantit l'immunité ; d'autre part, l'anonymat le plus strict qui ne permet pas d'établir un lien entre la personne physique et son double virtuel.

Larin, qui vit en Équateur depuis le début des années 2000, est un exemple illustrant la première tactique. Son lieu de résidence éloigné lui permet de ne pas cacher son identité, qu'il utilise notamment sur les réseaux sociaux (Livejournal, Facebook) et dans les interviews publiques. Lors de l'entretien, il souligne l'inefficacité des décisions de justice dans son pays de résidence :

- Litres a intenté un procès contre moi, ici en Équateur. Je crois même qu'ils l'ont gagné, mais cela n'a eu aucune répercussion sur moi. La spécificité de l'Amérique latine, c'est que lorsqu'un « gringo » en poursuit un autre, personne ne se sent vraiment concerné.
- Peuvent-ils exiger que vous payiez une amende ?
- Ils peuvent l'exiger, oui. Mais ils ne peuvent pas me forcer à la payer. De plus, le tribunal a statué que le domaine Librusec me soit retiré, ce qui était supposé tuer la bibliothèque. Cela fait deux ans maintenant. Cependant, le domaine fonctionne toujours, je renouvelle la licence chaque année. Voilà, c'est l'Équateur[27].

Le terme « gringo », qui désigne les étrangers en Amérique latine, souligne le statut de Larin qui lui permet de se percevoir – et d'être perçu – décalé par rapport aux

26 *Ibid.*

27 *Ibid.*

préoccupations locales de son pays de résidence. Cependant, il se sent également éloigné du contexte russe :

> « (Les gens de Litres), je ne les ai jamais vus en vrai ; ils habitent quelque part dans la lointaine ville de Moscou, sur un autre continent, ils s'y occupent de leur petit business. Eh bien, tant mieux pour eux »[28].

Sa posture de personne libre de toute contrainte géographique le rend imperméable à d'éventuelles poursuites. On peut noter la différence avec le fondateur de WikiLeaks, Julian Assange, qui voyait lui aussi en l'Équateur – ou du moins dans son ambassade londonienne – un lieu d'asile lui permettant d'échapper à l'extradition vers les États-Unis où l'attendait un jugement pour divulgation de documents classés confidentiels par le gouvernement américain. La stature politique de ce personnage, devenu un symbole de l'opposition à l'État américain, l'a rendu dépendant d'un jeu diplomatique entre les puissances. L'asile qui lui a été accordé durant sept ans a été le résultat d'une prise de position anti-impérialiste de Rafael Correa, président de l'Équateur, en 2012. Assange a été remis à la police britannique par son successeur, Lenin Moreno, soucieux de se démarquer de son prédécesseur. Larin, quant à lui, n'est aucunement une figure publique. Il souligne le choix totalement apolitique de son lieu de résidence, effectué en 2000, soit bien avant la création de Librusec, « en raison de son climat agréable », et prend soin de n'être associé à aucune cause locale ou internationale.

Son exemple est cité par les administrateurs d'autres bibliothèques comme la raison pour laquelle ils ne peuvent se permettre de révéler leur identité, ne jouissant pas de la même immunité géographique. Par exemple, l'un des principaux administrateurs de Flibusta, qui se fait appeler Stiver, vivant supposément en Allemagne, relate sur le forum de la bibliothèque, en novembre 2014, sa confrontation avec les forces de l'ordre locales, sans nommer le pays où cela se déroule :

> « Comme certains d'entre vous le savent, je fais l'objet d'une enquête depuis environ deux ans. La même maison d'édition bien connue en Russie a déposé une plainte contre moi, m'accusant de toutes sortes de péchés, allant de la diffusion illégale de textes à la gestion d'un syndicat international du crime et à l'enrichissement y afférant, bien entendu.
>
> Les policiers ont recueilli les informations sur moi, ont fouillé mon logement et mon bureau et ont saisi mon ordinateur portable. Puis ils ont commencé à examiner ce qu'ils (…) ont récolté. Résultat pour le moment : affaire classée.

28 *Ibid.*

> L'enquête n'a pas trouvé et ne s'attend pas à trouver d'irrégularités au-delà de quelques détails négligeables. (…)
>
> La tentative d'incriminer (avec des arguments absolument hilarants), en plus de ma personne, toute la bibliothèque, a également échoué. L'enquête a spécifiquement indiqué que le projet est à but non lucratif et ne génère pas de revenus »[29].

Cette nouvelle apparemment positive a suscité des réactions mitigées de la part des membres du forum. La plupart d'entre eux ont exprimé leur joie, espérant que cela créerait un précédent qui permettrait aux bibliothèques de l'ombre de sortir de l'illégalité. Certains utilisateurs taquinaient Stiver, l'invitant à révéler son identité, puisqu'elle était déjà connue de la police. Cependant, les utilisateurs se sont finalement accordés sur l'utilité pour tout le monde de rester anonymes afin d'éviter les ennuis, notamment au vu des précédents de responsables de bibliothèques de l'ombre arrêtés, comme celui des fondateurs de Pirate Bay en 2010, déjà débattu auparavant sur le forum.

L'enquête sur Stiver n'a pas créé de précédent en Russie : la résolution d'un tribunal allemand n'a changé ni le rapport des autorités russes envers la bibliothèque ni sa perception par les majors de l'industrie russe. Cependant, elle a renforcé le besoin des membres de la communauté de rester anonymes. La section « réglementation » du site indique clairement l'importance cruciale de l'anonymat, en précisant que « les actions susceptibles de porter atteinte à la sécurité ou aux droits personnels des utilisateurs sont interdites. En particulier, dévoiler l'identité de quelqu'un est interdit[30] ». Lorsque j'ai demandé un entretien à un autre administrateur de Flibusta, celui-ci a catégoriquement refusé tout moyen de communication qui pourrait permettre de découvrir son identité ou son lieu de résidence, me renvoyant au procès que Stiver avait subi.

Enfin, la troisième façon de garantir la pérennité des bibliothèques est d'en assurer l'accès à tous les utilisateurs. Des tentatives d'empêcher les blocages de sites ont été entreprises, notamment, par *Roskomsvoboda* lors de la « bataille pour le Runet » en novembre 2015. Le tribunal s'étant prononcé pour le blocage éternel de Rutracker, les avocats de *Roskomsvoboda* ont lancé une campagne pour lever ces mesures restrictives, en arguant que la restriction de l'accès à l'ensemble du site pour protéger quelques titres du catalogue d'Eksmo violait le droit des millions d'utilisateurs d'accéder au contenu du site et celui des milliers d'auteurs qui y distribuent leurs propres œuvres[31]. Un site web a été créé pour recueillir des

29 https://flibusta.is/node/261839 (consulté le 6 janvier 2023).

30 http://flibusta.is/node/4023 (consulté le 06 janvier 2023).

31 https://roskomsvoboda.org/13690/ (consulté le 06 janvier 2023).

fonds et des signatures[32], et une plainte signée par sept mille personnes a été déposée au tribunal. Cette tentative de couper court aux blocages en créant un précédent judiciaire n'a pas porté ses fruits : la plainte a été rejetée à deux reprises et n'a pas eu d'incidence sur la suite de la procédure.

Les blocages deviennent monnaie courante à partir de 2015. Il est désormais vital, pour les bibliothèques de l'ombre, de chercher des moyens de rester visibles pour le grand public vivant en Russie. Le premier consiste à multiplier les « miroirs » sûrs, en cherchant le domaine adéquat. Les experts de *Roskomsvoboda* proposent, par exemple, le domaine .lib, régi par EmerCoin, considéré invulnérable grâce à sa structure : « Le réseau DNS d'EmerCoin est entièrement décentralisé et ne comporte aucun site susceptible d'être bloqué sur demande des autorités ou permettant de faire pression sur ses propriétaires[33] », comme cela peut arriver pour des domaines gérés par l'ICANN[34].

Les réseaux qui garantissent l'anonymat, comme Tor et l'« *Invisible Internet Project* » (i2p), permettent également d'échapper aux contraintes nationales, ce qui conduit les bibliothèques de l'ombre à y installer leurs « miroirs »[35].

Un autre moyen d'augmenter sa visibilité consiste à apprendre aux utilisateurs les astuces pour contourner les blocages. Les sites et les forums des bibliothèques de l'ombre affichent toutes des listes de moyens techniques permettant d'échapper aux contraintes créées par les fournisseurs d'accès Internet russes à la demande de *Roskomnadzor*. Cette diffusion des savoir-faire semble omniprésente et circule par de nombreux autres canaux : listes de diffusion, messages sur les réseaux sociaux, tutoriels YouTube. Les solutions proposées comprennent le changement de serveur DNS, l'utilisation du mode turbo du navigateur (Opera, Chrome et Yandex), des plug-ins spéciaux pour les navigateurs, des services VPN, du navigateur Tor et d'anonymiseurs. Les membres de la communauté familiers avec ces savoir-faire expliquent aux utilisateurs moins initiés le fonctionnement de chaque méthode, ses avantages et ses inconvénients (qui se résument souvent à l'équilibre entre la vitesse d'exécution et la simplicité d'utilisation). Ils testent les VPN et les anonymiseurs pour ensuite partager leurs observations avec les autres utilisateurs. Cette maîtrise des outils de contournement fait aujourd'hui partie des compétences partagées par des personnes fréquentant les bibliothèques de l'ombre, et les rapproche d'usagers souhaitant accéder à d'autres types de contenus bloqués, qui se sont multipliés depuis l'instauration de la censure de

32 https://zarunet.org/ (consulté le 06 janvier 2023).

33 https://roskomsvoboda.org/12118/ (consulté le 16 février 2023).

34 *Internet Corporation for Assigned Names and Numbers*, organisation à but non lucratif basée à Los Angeles.

35 https://roskomsvoboda.org/28612/ (consulté le 24 novembre 2022).

guerre en mars 2022, qu'il s'agisse des sites de médias indépendants ou encore des réseaux sociaux appartenant à la compagnie Méta.

Outre les *torrents* déjà mentionnés, les usagers et administrateurs de bibliothèques rivalisent de créativité pour organiser la diffusion des mises à jour des collections. Là encore, la prolifération des moyens et des supports est de mise. Par exemple, Librusec.ucoz, un forum commun à plusieurs bibliothèques parallèles et qui sert de refuge en cas d'inaccessibilité du forum interne, dispose d'une section intitulée «Notre Tortuga[36]». L'un des administrateurs du forum y place les liens vers les mises à jour des bases de données Librusec et Flibusta via des sites de partage de fichiers gratuits.

Parallèlement à cette plateforme, les communautés utilisent également les réseaux sociaux et les messageries. Par exemple, un bot sur le réseau social russe VKontakte a permis, pendant un temps, de faire une recherche rapide dans les bibliothèques de l'ombre et de faciliter leur accès en cas de panne ou de blocage. Cependant, en juin 2019, VKontakte et la maison d'édition Eksmo ont conclu un accord selon lequel le réseau social doit vérifier le statut légal de tous les livres téléchargés par ses utilisateurs. Cela n'a toutefois pas entraîné la disparition du bot : en septembre, il a été transféré en un lieu plus sûr[37].

Après le durcissement de l'attitude de VKontakte à l'égard des contenus illégaux, certaines bibliothèques de l'ombre ont commencé à utiliser Telegram, devenu très populaire en Russie malgré – et même en raison de – son blocage entre 2018 et 2020, et réputé être tolérant à l'égard des contenus illégaux grâce aux opinions libertariennes de son propriétaire, Pavel Dourov. De nombreuses chaînes distribuaient des livres numériques et audio[38], et des bots ont été écrits à cet effet. Cependant, en août 2020, ces bots auraient cessé de fonctionner, supposément à la suite d'un accord entre Telegram et les autorités russes. En annonçant la nouvelle sur le forum de Flibusta, les utilisateurs ont immédiatement proposé une solution technique pour contourner cette nouvelle barrière :

- Le bot Flibusta a été bloqué non seulement sur iOS, mais aussi sur Android.
- Comment faire pour que le bot fonctionne à nouveau ? C'est simple – vous devez suivre les étapes suivantes :
    1. Créez un groupe ;
    2. Ajoutez-y un bot en cliquant sur le lien suivant (…)[39].

36 http://flibusta.is/node/474924 (consulté le 24 novembre 2022).

37 https://github.com/FlyInk13/FlibustaBot (consulté le 24 novembre 2022).

38 https://gipp.ru/overview/ekspertnye-obzory/borba-s-piratami-kak-otstoyat-avtorskie-prava-v-telegram/ (consulté le 16 février 2023).

39 http://flibusta.is/node/474924 (consulté le 24 novembre 2022).

Ajouté à un groupe, le bot n'est plus considéré comme tel par le système et peut continuer à être utilisé. Les usagers tournent ainsi à leur avantage des lacunes internes du système de messagerie pour contourner les blocages.

La survie des bibliothèques et des communautés qui les font vivre est donc conditionnée par la multiplication des supports et des lieux où elles sont conservées, par la réactivité des membres de ces communautés face aux obstacles qui se présentent ainsi que par leur capacité à trouver des solutions créatives et à les diffuser le plus largement possible. Les communautés s'appuient sur les savoir-faire techniques de leurs membres afin que ces bibliothèques demeurent pérennes. La subsistance des canaux de communication semble essentielle dans ce processus, d'où leur multiplication et parfois leur redondance.

Ce phénomène n'est certainement pas propre à la Russie et s'inscrit dans une dynamique plus large. Selon Keucheyan et Tessier, dans le monde numérique actuel, les « hackers » ou les « pirates » ne seraient pas des révolutionnaires ; l'idée d'une « révolution » n'est pas prometteuse car elle serait « systématiquement suivie d'une contre-révolution qui entraîne des conditions d'existence similaires – ou pires – que celles qui précédaient la révolution en question ». Ainsi, les hackers ne cherchent pas la confrontation. Au contraire, ils profitent des « interstices, des zones inoccupées par l'État » et une fois repérés, « ils disparaissent, se dispersent pour se reformer à un autre endroit » [Keucheyan & Tessier, 2008, p.457]. Mais si, selon les auteurs, ces détournements symboliques ne peuvent avoir lieu que dans un pays démocratique, nous avons montré qu'ils trouvent également leur place dans un contexte autoritaire. Les ONG russes luttant pour le libre accès, comme l'Association des éditeurs Internet, Wikimedia.ru ou *Roskomsvoboda*, font partie de réseaux internationaux et endossent des luttes politiques mondialisées. Les bibliothèques de l'ombre, elles, se tiennent à l'écart de ces causes et promeuvent une conception d'une liberté ancrée dans la maîtrise d'outils techniques et de pratiques culturelles qui ne sont pas censurées par une autorité extérieure à leur communauté.

Conclusion

Après la chute de l'URSS, les industries culturelles et l'État russes ont longuement œuvré à faire respecter, sur le Runet, les normes internationales du droit d'auteur afin de rassurer les partenaires commerciaux étrangers et permettre le déploiement des acteurs nationaux. La lutte contre le « piratage », menée par leurs efforts joints, en a été l'une des conséquences directes. Or, depuis l'invasion de l'Ukraine, les collaborations avec les majeurs occidentaux ont été rompues, alors que le public russe est habitué à consommer des produits culturels mondialement distribués. L'État s'évertue dès lors à trouver des moyens de légaliser des formes de contournement du copyright, tout en ménageant les industries nationales. Un projet de loi permettant d'utiliser des produits culturels des « pays inamicaux » sans l'accord des ayants-droits étrangers a été déposé en août 2022, mais a été vivement critiqué par les représentants des industries qui craignent de perdre leur crédibilité sur le marché mondial[40]. Ces derniers cherchent leurs propres moyens de fournir au public russe le contenu convoité. Par exemple, Eksmo annonce la publication de best-sellers mondiaux sous forme de « *summaries* », des résumés du livre sans citations directes. Ces pratiques sont dénoncées comme des manifestations de « piratage » légalisé par de nombreux acteurs, y compris les défenseurs des droits numériques qui s'étaient auparavant mobilisés contre la législation « anti-pirate »[41].

Ce renversement de situation n'entraîne toutefois pas de changement en ce qui concerne les bibliothèques de l'ombre, toujours considérées comme représentant un danger potentiel pour les industries culturelles nationales, voire un *underground* culturel incontrôlé.

Les luttes pour un Internet libre de toute censure et celles pour un accès libre et équitable aux écrits se chevauchent à plusieurs égards. Les défenseurs des droits numériques se mobilisent pour les deux causes, les englobant sous la même étiquette d'« Internet libre ». En dehors de la Russie, les répressions ont conduit les administrateurs des bibliothèques de l'ombre à une politisation progressive. Après avoir commencé comme des « joyeux lurons partageant gaiement ce qui était vendu » par d'autres, ils se sont retrouvés dans le même combat que des « victimes de persécution et de censure politique », ce qui leur a conféré un motif de rébellion [Bodó, 2015, p. 7]. Les communautés autour des bibliothèques de l'ombre russes, quant à elles, se tiennent généralement à l'écart des protestations publiques menées en leur nom par les organisations de défense des libertés numériques, se centrant davantage sur les aspects techniques de contournement

40 https://www.vedomosti.ru/business/articles/2022/10/14/945479-kinoseti-i-prodyuseri-poprosili-mishustina (consulté le 16 février 2023).

41 https://roskomsvoboda.org/post/prinuditelnoe-licenzirovanie/ (consulté le 16 février 2023).

des contraintes et de formation des utilisateurs. Par exemple, les quelques posts explicitement « politiques » sur les mobilisations anti-copyright dans le monde ne provoquent guère de réactions, contrairement aux posts sur les questions techniques qui sont largement discutés.

Toutefois, leur statut de hors-la-loi les libérant de la nécessité de respecter les restrictions imposées par la législation russe, ces plateformes se positionnent en tant qu'un espace de liberté dans un contexte de plus en plus contraint. Certaines communautés s'en saisissent pour exprimer une position politique claire, passible de répressions si elle figurait sur un site non bloqué. Ainsi, la Maxima Library arbore, mis en exergue sur sa page d'accueil, le slogan « Liberté à l'Ukraine ! Non à la guerre ! Mort aux fascistes poutiniens » en ukrainien, en russe et en anglais après février 2022.

D'autres affirment leur indépendance vis-à-vis du contexte répressif russe. Ainsi, sur le forum de Flibusta, un utilisateur s'interroge pour savoir si des rapports sexuels dans certaines œuvres de science-fiction peuvent être considérés comme de la « propagande des rapports LGBT[42] ». « Vous êtes ici sur un site bloqué dont l'administrateur se contrefiche des lois de la Fédération de Russie. Ne vous prenez pas la tête, cela ne concerne que ces malheureux auteurs qui essaient de vendre leurs écrits pour des roubles », lui répond un autre membre de la communauté[43].

D'autres encore, comme Librusec, restent concentrés sur les discussions purement littéraires et techniques. Toutefois, quel que soit leur degré de politisation affiché, ces communautés promeuvent l'idée de « liberté absolue » attachée à l'imaginaire pirate. Par leur simple existence, elles contestent l'entreprise de construction d'un Runet souverain où ne circuleraient que des œuvres produites et diffusées par l'industrie du livre russe sur laquelle l'État tente d'affirmer son emprise.

Références bibliographiques

[Alekseeva et al., 2013] Alekseeva, Anastasija et al. (dir.), *Transformaciâ Avtorskogo Prava v Internete. Zarubežnye tendencii, biznes-modeli, rekomendacii dlâ Rossii* (*Transformation du droit d'auteur face à l'Internet. Les tendances étrangères, les modèles de buseness, les recommendations pour la Russie*), Moscou, Associaciâ internet-izdatelej,», 384.

[*Antipiratskij zakon*, 2017] « Antipiratskij zakon, pravoprimenenie, tendencii i sistemnye problemy za period 08.2013-06.2017 » (« Lois antipirate : application, tendances

42 En durcissant les textes adoptés depuis les années 2010, une loi interdisant « la propagande LGBT » dans l'espace public est entrée en vigueur en décembre 2022, dans un contexte de « guerre de valeurs » menée par la Russie contre les pays occidentaux.

43 http://flibusta.is/node/588957 (consulté le 16 février 2023).

et problèmes systémiques, 08.2013-06.2017»), rapport publié par *Roskomsvoboda*, https://antipiracy.changecopyright.ru/, consulté le 12 décembre 2022.

[Bacot & Canonne, 2019] Bacot, Baptiste & Canonne, Clément, «Musique et hacking: de l'éthique aux pratiques», *Volume !* vol. 16, n° 1, p. 7-14.

[Baudel, 1998] Baudel, Jules-Marc, «Le droit d'auteur français et le copyright américain: les enjeux», *Revue française d'études américaines* vol. 78, p. 48-59.

[Benamou & Farchy, 2009] Benamou, Françoise & Farchy, Joëlle, *Droit d'auteur et copyright*, Paris, La Découverte.

[Bodó, 2015] Bodó, Balázs, «The common paths of piracy and samizdat», in Parisi, Valentins (dir.), *Samizdat*, Budapest, CEU Institute for Advanced Study, p. 19-34.

[Bodo, 2018] Bodó, Balázs, «The genesis of the Library Genesis: the birth of a global scholarly shadow library», in Karaganis, Joe (dir.), *Shadow Libraries*, Cambridge, MA, The MIT Press, p. 25-51.

[Coleman, 2012] Coleman, Gabriella, *Coding Freedom: The Ethics and Aesthetics of Hacking,* Princeton, Oxford, Princeton University Press.

[Daucé, 2022] Daucé, Françoise, «Pirater l'autoritarisme», *Terminal*, n° 134-135.

[Elst, 2005] Elst, Michiel, *Copyright, Freedom of Speech, and Cultural Policy in the Russian Federation*, Law in Eastern Europe, Leiden, Brill.

[Haritonov, 2016] Haritonov, Vladimir, *Elektronnoe knigoizdanie v Rossii. Problema dostupa i gosudarstvennoe regulirovanie (L'édition électronique en Russie. Les problèmes d'accès et la régulation d'État),* Moscou, Associacija internet-izdatelej, 182.

[Herman, 2012] Herman, Bill, «A political history of DRM and related copyright debates, 1987-2012», *Yale Journal of Law and Technology* vol. 14, n° 1, p.162-225.

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

[Kiria & Sherstoboeva, 2015] Kiriya, Ilya & Sherstoboeva, Elena, «Russian Media Piracy in the Context of Censoring Practices», *International Journal of Communication* vol. 9, p. 839-851.

[Martin-Prat, 2014] Martin-Prat, Maria, «The future of copyright in Europe», *The Columbia Journal of Law & The Arts* vol. 38, n° 1, p.29-47.

[Nowak, 2016, p.178] Nowak, Jakub, «The good, the bad, and the commons: a critical review of popular discourse on piracy and power, during anti-ACTA protests», *Journal of Computer-Mediated Communication* vol. 21, n° 2, p.177-194.

[Ostromooukhova, 2021] Ostromooukhova, Bella, «Free libraries for the free people: how mass-literature «shadow» libraries circumvent digital barriers and redefine legality in contemporary Russia», *First Monday* vol. 26, n° 5.

[Ostromooukhova, 2019] Ostromooukhova, Bella, « Négocier le contrôle, promouvoir la lecture. Éditeurs indépendants face à l'État dans la Russie des années 2010 », *Bibliodiversity*, juin 2019.

[Rassolov, 2016] Rassolov, Il'ja, *Pravo i kibernetičeskoe prostranstvo (Law and cyberspace),* Moscou, Moskovskoe bjuro po pravam čeloveka.

[Soldatov & Borogan, 2016] Soldatov, Andrej & Borogan, Irina, *Bitva za Runet. Kak vlast' manipuliruet informaciej i sledit za každym iz nas (Bataille pour le Runet. Comment les autorités manipulent les informations et surveillent chacun d'entre nous)*, Moscou, Al'pina,.

[Stelmakh, 2001] Stelmakh, Valeria, « Reading in the context of censorship in the Soviet Union », *Libraries & Culture* vol. 36, n° 1, p. 143-51.

[Thiesse & Schmatko, 1999] Thiesse, Anne-Marie & Chmatko, Natalia, « Les nouveaux éditeurs russes », *Actes de la recherche en sciences sociales*, n° 126-127, p. 75-89.

[Turner, 2006] Turner, Fred, *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Eise of Digital Utopianism*, Chicago, University of Chicago Press.

[Van Laer & Aelst, 2010] Van Laer, Jeroen & Van Aelst, Peter, « Internet and social movement action repertoires: opportunities and limitations », *Information, Communication & Society* vol. 13, n° 8, p. 1146-1171.

[Waldfogel, 2018] Waldfogel, Joel, *Digital Renaissance: What Data and Economics Tell Us about the Future of Popular Culture,* Princeton and Oxford: Princeton University Press.

[Zaslavskaya, 2015] Zaslavskaya, Olga, « Samizdat. Between Practices and Representations », *Lecture series at Open Society Archives*, Budapest, February-June 2013, IAS Publications no. 1. Budapest, Central European University, Institute of Advanced Study, p. 87-99.

[Zasurskij, 2016] Zasurskij, Ivan, *Novaâ Model' Regulirovaniâ Avtorskih Prav. Obŝ estvennoe Dostojanie i Koncepcija Obŝego Blaga (Un nouveau modèle de régulation des droits d'auteur. Le domaine public et la conception du bien commun),* Moscou, Associaciâ internet-izdatelej.

Chapitre 7

Mobilisations et contestations sur les blogs et réseaux sociaux

Perrine Poupin

En Russie, le monde militant et la pratique revendicative ont été reconfigurés par le numérique. Les transformations sont telles que la réflexion sur Internet et les réseaux numériques sociaux s'impose désormais comme un passage obligé pour étudier ces activités [Desroches, 2011]. Comme d'autres secteurs du monde social, les mobilisations collectives ont été envahies de manière croissante par des supports technologiques informatisés notamment portables et mobiles, jusque dans les régions les plus reculées du pays. Les protestataires sont passés des mails, des listes de diffusion et des blogs (LiveJournal) à des dispositifs du Web 2.0 (sites de réseaux sociaux, médias sociaux comme YouTube), les premiers étant cependant encore utilisés par une partie des personnes. Les usagers et les types d'usages sont diversifiés : Facebook, Twitter, Telegram sont les principaux moyens de communication des militants politiques et des populations urbaines et diplômées, le réseau russe VKontakte reste le média principal des habitants et des citoyens ordinaires.

En plus de coordonner des actions revendicatives, les technologies numériques permettent aux collectifs d'informer au quotidien, de diffuser des contre-expertises, de faire pression sur des dirigeants, de discuter et de mener des enquêtes. Des initiatives sont spécifiquement dédiées à l'activité informationnelle de type généraliste ou spécifique (corruption des élites, écologie, libertés en ligne, etc.). Certaines d'entre elles sont désormais basées en Europe à la suite de l'exil de leurs fondateurs. Des associations juridiques accompagnent également les personnes victimes de répressions liées à Internet. Enfin, le contexte pandémique et le confinement ont par exemple été l'occasion d'initiatives solidaires et de manifestations virtuelles sur Internet, à partir d'inscriptions portées sur des cartes de grandes villes proposées par des applications GPS. Le chapitre s'intéresse à l'articulation entre action collective et nouvelles technologies dans les mobilisations collectives de la dernière décennie en Russie, après une mise en contexte historique. Il rend compte de l'actualisation de l'action collective dans le contexte russe, où Internet a peu à peu cessé d'être la zone de liberté qu'il semblait

être jusqu'au début des années 2010. Il montre ce que sont devenus ces espaces dans le cadre de la guerre en cours, où les réseaux sociaux (VKontakte, mais aussi Telegram et YouTube) constituent aussi des vecteurs de propagande pro-Kremlin, en Russie, en Europe et sur les territoires occupés par la Russie en Ukraine.

Le développement d'un Internet à but revendicatif et l'attrait du média-activisme. Fin des années 1990-début des années 2000

Le marketing politique a fait son apparition en Russie lors de la campagne présidentielle de 1996, à une époque où les médias russes sont passés sous contrôle de groupes oligarchiques qui les ont instrumentalisés comme outils de guerre médiatiques. Ce marketing politique fait aujourd'hui partie du paysage politique russe [Rakhmanova, 2012]. Les nouveaux dispositifs de communication fascinaient les militants et les artistes engagés des grands centres urbains, qui avaient l'impression que le « PR » (les relations publiques) politique et la « *polittekhnologia* » (la technologie politique) étaient des instruments essentiels de l'action politique et des outils qu'il fallait étudier [Kireev, 2006, p. 17]. Dans cette perspective, des militants initièrent une forme de « médiactivisme » (le terme apparaît à la fin des années 1990 et au début des années 2000 en Russie) en se donnant comme mission de produire, de manière horizontale, un type d'information sur des bases militantes, visant à proposer un autre cadrage des réalités politiques et sociales[1].

Lors de la campagne pour les élections parlementaires de décembre 1999, le groupe *Radek*, composé d'artistes et de militants moscovites, organisa une mise en scène spectaculaire, axée sur le succès médiatique. Cette action faisait suite à une série d'interventions urbaines artistiques, regroupées *a posteriori* sous le nom d'« actionnisme moscovite », à forte teneur politique et plutôt destinées jusqu'alors à la communauté des pairs. Les actions se sont ensuite adressées à un public plus large et ont tablé sur un modèle de « spectateur anonyme », qui aurait incarné la condition commune des individus en Russie de l'époque. Selon ces artistes, le chaos, la dépression et la violence des années 1990 avaient détruit le public démocratique et actif de la perestroïka. Il fallait, pour eux, s'adresser à un autre public, celui des médias de masse. Le 7 décembre 1999, le groupe *Radek* brandit sur le mausolée de Lénine, aux pieds des murs du Kremlin, une banderole avec ces mots : « Contre tous ![2] ». L'action fut retransmise par plusieurs chaînes de télévision, avec une liberté de ton possible à l'époque, leurs journalistes ayant été invités sur les lieux par les artistes.

1 Sur la notion de média-activisme, voir [Cardon & Granjon, 2013].

2 Selon la Constitution russe, il était légalement possible jusqu'en 2006 de voter « contre tous les candidats », et dans le cas où la majorité des votes allait à cette mention, les élections devaient être reconduites, avec de nouveaux candidats. Cela n'arriva jamais.

Les participants de ce type d'action rêvaient qu'en préparant une action claire, inattendue, brillante et en la montrant à la télévision, ils pouvaient changer les mentalités. Les actions spectaculaires sont en effet vues par leurs initiateurs comme seules capables d'attirer un public découragé par la politique ordinaire [Cossart & Taïeb, 2011, p. 146]. La campagne fut un succès, mais sans lendemain. Ces performances de rue ont ouvert la voie à toute une série d'actions à forte dimension spectaculaire, ponctuelles, rapides et ne nécessitant pas d'engagement sur la durée. Ce type d'actions a été mené dans les années 1990 par les activistes écologistes et libertaires de *Khraniteli Radougui* (Les gardiens de l'arc-en-ciel) et le Parti national-bolchévique russe (NBP) d'Édouard Limonov, et dans les années 2000 et 2010, par les groupes *Voïna* (2007-), *Pussy Riot* (2011-) et les militants antifascistes. Ces groupes furent poursuivis après 2012. Leurs membres ont connu la prison et l'exil. Le registre de l'action spectaculaire, médiatique, malgré ces répressions et le peu de résultats, est resté très populaire et fait encore figure de référence aujourd'hui chez les militants politiques, les intellectuels et les artistes engagés.

Le médiactivisme en Russie s'est ensuite diversifié et s'est approprié des innovations technologiques qui ont conditionné par la suite la production et la diffusion des informations militantes. Il prit un tournant vidéo au début des années 2000 et adopta les dispositifs numériques de communication, perçus comme des outils d'émancipation et des catalyseurs de changements sociaux. La multiplication de caméras-vidéo légères à des prix abordables et d'appareils mobiles de type smartphone et tablette a permis à de nombreux activistes de photographier et de filmer les rassemblements de rue et les activités revendicatives. Les militants se mirent à diffuser les images sur Internet afin de rendre compte des événements revendicatifs d'une autre manière que les médias officiels, qui couvraient peu, mal ou pas du tout ces actions. Différents usages peuvent être recensés [Poupin, 2013]. Dans le public des pairs, les récits et les images permettent de revivre des expériences passées, dont certaines très vives. Concernant le public plus large, Internet permet aux militants et aux artistes engagés de transmettre et de visualiser les preuves par l'image de la possibilité de protester et d'être courageux : les activistes pensent ainsi convaincre, recruter de nouvelles personnes et inciter le public à passer à l'action. Dans cette perspective, l'image chargée d'émotions est perçue à la fois comme le support et le message, et elle est censée être performative. Elle est vue comme un catalyseur direct de l'évolution du public [Bloomfield & Doolin, 2012], passant du public passif à public actif. Cette vision est restée dominante dans le monde militant jusqu'à aujourd'hui.

En plus de montrer les rassemblements de rue, Internet et les outils de communication numériques ont été appropriés par les groupes militants pour diffuser des informations, critiquer l'action gouvernementale, mener

des campagnes publiques, débattre, créer des réseaux, recruter, se socialiser et organiser des rassemblements. Les groupes utilisèrent à partir de la moitié des années 1990 le courrier électronique [O'Lear, 1999], puis au début des années 2000 les blogs (LiveJournal, lancé en 2000 en cyrillique) [Poberezhskaya, 2018], et ensuite les sites Internet et les plateformes numériques (par ordre de popularité, YouTube lancé en Russie en 2007, VKontakte en 2006, Facebook en 2008 et Twitter en 2007). Telegram fut lancé plus tard, en 2013, par les frères Nikolaï et Pavel Dourov, fondateurs de VKontakte, après que le gouvernement russe eut pris le contrôle de VKontakte. LiveJournal, Facebook, Twitter et Telegram sont surtout utilisés par les cercles restreints de l'opposition politique et des populations urbaines et diplômées. VKontakte n'a jamais cessé d'être le réseau social le plus populaire en nombre d'utilisateurs en Russie. Ces différences d'usages traduisent une fracture politique et sociale dans le pays. Ceci dit, il existe des usages mixtes et complémentaires entre différents outils numériques, en fonction des contenus et des contacts. Nous distinguons dans la suite du propos deux grandes catégories d'usagers, l'opposition politique et les citoyens non-militants.

Promesses d'Internet comme espace public chez l'opposition politique. Années 2000 et 2010

Avec le développement d'Internet dans les années 2000, les militants politiques montrèrent une grande appétence pour les médias numériques, considérés comme des outils puissants d'information, de communication et d'organisation. Au même moment, le régime de Poutine reprenait le contrôle sur les médias mainstream. Internet représentait pour une population urbaine et diplômée qui ne faisait pas confiance aux médias traditionnels une révolution de l'information par rapport à la période soviétique et aux années 1990 [Trakhtenberg, 2004 ; Nenachev, 2010]. La liberté de ton sur Internet a été très grande jusqu'aux manifestations contre la falsification des élections en 2011-2012, qui ont réuni plusieurs centaines de milliers de personnes dans les rues et qui ont marqué un tournant dans les rapports du pouvoir à Internet. Auparavant, les mécanismes de contrôle existaient, mais ils étaient ciblés et subtils. Pour les militants et certains analystes, Internet constituait en Russie un refuge pour s'exprimer et débattre librement, voire un véritable espace public autonome [Nocetti, 2012]. Internet était le lieu de nouvelles formes d'expression et de contestation qui travaillaient la Russie connectée, plutôt insensible au militantisme traditionnel. Il permettait un engagement ludique et distancié et représentait un facteur d'émancipation de la classe moyenne urbaine. Pour d'autres analystes, cette liberté d'informer et de débattre sur Internet était un leurre, une « émigration virtuelle » d'une partie des intellectuels [Tchernyshev, 2008] ou, pour reprendre une expression russe, une « *soupape d'évacuation de la*

vapeur sociale», tolérée par les autorités qui y voyaient une manière de surveiller les critiques et les contestations, de les contenir en ligne et si besoin de réprimer les auteurs. Ces critiques d'Internet en tant que lieu d'expression alternatif sont apparues dès le début des années 2000, lors de l'avènement au pouvoir de Poutine. Dans les mêmes années, la télévision restait la principale source d'information pour la majorité de la population, y compris dans la capitale.

Depuis les élections législatives de 2003, et des amendements incessants à la loi électorale par Poutine qui ont permis un filtrage des candidats, les partis d'opposition libéraux-démocrates (par exemple *Iabloko* et *Pravoïe Delo*) ont été expulsés de l'arène parlementaire. L'opposition s'est recomposée et a réinvesti la rue, qui est devenue pour elle un nouvel espace de représentation[3]. Dans ces conditions, la protestation de rue est perçue comme la seule expression possible pour les *outsiders* politiques sur la scène publique [Lipsky, 1968]. Les usages d'Internet de l'opposition ont suivi ces modifications des rapports de force entre acteurs politiques. Certains d'entre eux ont développé sur Internet des activités informationnelles de type généraliste et spécifique (corruption des élites, mouvements des droits de l'homme et associations juridiques de défense des libertés en ligne, etc.). Ils ont créé des blogs, puis des pages personnelles et des sites. Certains de ces groupes sont désormais basés en Europe à la suite de l'exil de leurs fondateurs, persécutés en raison de leurs activités revendicatives, notamment après le tournant des années 2011-2012 (voir chapitre 8). D'autres acteurs politiques de l'opposition se sont engagés dans l'organisation de séries de rassemblements de rue pour un changement de système politique (« Marche des dissidents », 2005-2008) et le droit de la liberté de réunion (« Stratégie-31 », 2009-2015), durement dispersés par le pouvoir. Des blogueurs de LiveJournal, qui joua un rôle pionnier dans l'Internet revendicatif en Russie dans les années 2000 [Etling et al., 2010], ont pu raconter ces événements, en témoins directs sur leurs pages personnelles. En 2017, quelques dizaines de milliers de personnes descendirent dans la rue, répondant au slogan d'Alekseï Navalny: « Il n'est pas votre Dimon » (un diminutif argotique de Dmitri), après la diffusion sur YouTube d'un documentaire traitant des affaires de corruption liées au Président du gouvernement de la Fédération de Russie Dmitri Medvedev (33 millions de vues en quelques jours). En août 2019, environ 50 000 participants se rassemblèrent à Moscou après le rejet de la candidature d'une soixantaine de candidats indépendants aux élections locales et pour demander des élections libres.

Dans ces années 2010, avec le développement des réseaux sociaux numériques dans les centres urbains et la numérisation d'une partie de la vie sociale, les

3 Le leader démocrate Ilya Iachine l'explique en 2005 dans son ouvrage *Ulitchny protest* [La protestation de rue] (https://www.yabloko.ru/Publ/Book/Yashin/protest_004.html, consulté le 17 février 2023).

frontières entre espaces publics et privés se sont déplacées. Les sociabilités revendicatives ont évolué. Les groupes militants ont dès lors occupé à la fois des espaces géographiques physiques et ouverts (rassemblements de rue), des lieux fermés (pour les réunions et conférences) et des espaces publics numériques [Baker, 2011]. Ces évolutions de la digitalisation des activités revendicatives étaient perçues comme des améliorations majeures par les militants en Russie. Ces derniers appelaient explicitement de leurs vœux la convergence entre la rue et le cyberspace, et même parfois le remplacement de la première (faisant l'objet de plus en plus de mesures répressives) par la seconde.

Internet et les outils numériques offraient à ceux qui luttaient de nouvelles « opportunités médiatiques » [Gamson, 1998, p. 63] : les militants pouvaient composer des récits alternatifs aux récits officiels et aux opinions communément admises. Les récits et les images qui circulaient sur Internet construisaient des communautés imaginées et des identités publiques d'opposition au régime. Tout rassemblement de rue donnait lieu à la réalisation de films et de photographies, publiés et diffusés sur Internet. Ces formes visuelles sont des embrayeurs puissants de conversations privées et publiques [Gunthert, 2013 ; 2014]. Selon les dires des militants, sans ces images, l'action n'existait pas. Les militants plaçaient de grands espoirs dans Internet, y compris pour recruter de nouveaux membres. Les groupes misaient davantage sur les relais médiatiques que sur les rencontres physiques dans les rassemblements. Le succès des actions se mesurait à la quantité des réactions engendrées sur Internet [Gromov, 2008, p. 27] et notamment dans les médias numériques. Cette stratégie médiatique est typique des années 2000 et 2010.

Le développement des médias numériques n'a pas mis en cause la dépendance des militants envers les médias professionnels. Cette situation n'est pas typique de la Russie [Neveu, 2010 ; Lysenko & Desouza, 2010]. Au contraire, de nombreux militants ont embrassé dans les centres urbains une carrière de journaliste et ont mis le travail médiatique au cœur des activités revendicatives en Russie. Les discours militants ont été nourris de stratégies de captation de l'attention médiatique. Les collectifs ont organisé des rassemblements et des campagnes publiques dans des formes « médiatiquement acceptables », c'est-à-dire qui devaient être conformes aux canons démocrates-libéraux russes qui régissent l'action revendicative – approche légaliste qui utilise les canaux admis de la contestation comme les meetings, les pétitions et les lettres, ainsi qu'une critique des pratiques plus radicales d'action (actions non autorisées par les autorités, grèves, occupations de sites, sabotages y compris en temps de guerre comme actuellement). La stratégie médiatique crée des tensions et des pressions éprouvantes sur les personnes et les mises en commun à l'intérieur des groupes. Elle a un impact sur l'action revendicative et les récits sur l'action. Selon cette

perspective, les militants s'adaptent aux besoins des médias plus qu'ils n'élaborent une stratégie propre [Rucht, 2004]. Les médias traitent comme des cas individuels ce qui pourrait être problématisé en enjeux collectifs [Neveu, 1999]. Ils ont tendance à héroïser certains militants au sein de la foule [Gitlin, 1980, p. 146-179]. La « certification médiatique des leaders » [Neveu, 1999, p. 249] renforce les chefs dans leurs organisations. Elle valide la forme organisationnelle traditionnelle dans les milieux de l'opposition politique russe, qui excluent les profanes des processus de décision. Le but premier de cette stratégie est d'occuper au maximum les scènes des meetings et l'espace médiatique afin, selon une formule que les militants répètent à l'envi, d'« *imposer à la société* [leur] *agenda* » [*povestka*][4]. Cette stratégie implique un désinvestissement à l'égard d'un travail militant de terrain [Neveu, 2010, p. 250], par manque de temps et d'intérêt et en raison des risques encourus. Dans cette logique, les collectifs cherchent peu à ouvrir des espaces de discussion et de politisation dans les rassemblements ou les réunions alors que ces activités sont pourtant capables de façonner un imaginaire et des conduites politiques ainsi que de favoriser l'innovation tactique [Sobieraj, 2011].

La dématérialisation des discussions a eu un autre impact sur les activités revendicatives. Elle a donné lieu à une nouvelle forme de socialisation propre à Internet, qui n'a pas aidé les militants en Russie à établir une langue publique, qui puisse sortir les situations de communication des deux formats qui prévalaient en URSS, à savoir les « discussions de cuisine » entre proches et la langue formelle et officielle rigide. L'art de parler et de s'écouter en public n'est pas un exercice reconnu dans les activités politiques ou revendicatives. Le sociologue Boris Gladarev [2013] utilise la métaphore de « surdité publique » pour qualifier le défaut de capacités de parler en public dans des discussions publiques. Internet constitue, en Russie comme dans d'autres pays autoritaires, un espace d'interactions complexes entre divers types d'internautes, journalistes et autorités [Arsène, 2011]. De plus, les différentes plateformes sont agrégées entre elles et les points de vue exprimés sont plutôt homogènes. Les personnes sont idéologiquement proches et certaines appartiennent aux mêmes réseaux d'interconnaissance hors ligne. Ces plateformes excellent dans la diffusion restreinte au sein de petits cercles de personnes qui savent où trouver l'information (« *narrowcasting* »), mais jouent un rôle en général mineur dans la large diffusion (« *broadcasting* ») et la transformation des opinions [Sobieraj, 2011, p. 175]. En Russie, les médias de l'espace public oppositionnel constituent, selon des analystes, des sortes de « ghettos informationnels » à la fois isolés et isolants [Kiriya, 2012], potentiellement renforcés par les logiques algorithmiques [Pariser, 2011]. Il est difficile en réalité d'évaluer concrètement

4 La notion de « mise en agenda » fut importée des États-Unis et entra massivement dans la langue ordinaire des journalistes, qui par dizaines de milliers ont assisté depuis 1991 à des stages aux États-Unis et des séminaires d'ONG en Russie, comme l'organisation *Interviews* (liquidée en 2007 par Vladimir Poutine) qui assura des formations professionnelles gratuites [Matvejchev, 2010, p. 10].

l'efficacité de la participation et des mobilisations en ligne et les effets d'Internet sur l'engagement explicite hors ligne car la nature des publics civiques concernés est peu aisée à identifier [Arsène, 2011, p. 896].

En Russie, les activités revendicatives font face à un environnement hostile et imprévisible. Elles sont menées la plupart du temps dans le régime de l'urgence. Les militants sont peu nombreux, ils se sentent isolés et marginalisés. Dans les années 2000 et 2010, les rassemblements réunissaient en moyenne quelques centaines de participants, y compris à Moscou ou Saint-Pétersbourg, qui comptent respectivement 12,7 et 5,4 millions d'habitants. Les pratiques protestataires sont risquées et obtiennent rarement gain de cause. Les rassemblements sont régulièrement dispersés par les forces de l'ordre. Dans ce contexte, Internet offre la possibilité de communiquer, sans le risque de l'épreuve des relations concrètes. Les croyances liées aux capacités de « changer la société » par Internet ont redéfini les priorités de la scène revendicative des années 2000-2010. La stratégie médiatique nourrit autant de croyances que d'incertitudes chez les militants. Selon une causalité circulaire, l'absence de militants et de base sociale invite au choix de la stratégie médiatique. Ce processus creuse le fossé entre les militants politiques et le reste de la population, entre les militants chevronnés et les militants moins investis, qui quittent les collectifs rapidement. La stratégie médiatique fonctionne comme cause et conséquence de l'érosion du militantisme.

En outre, la mise en visibilité des pratiques militantes sur Internet comporte des risques : elle peut attirer l'attention du pouvoir et conduire à des surveillances rapprochées ainsi qu'à des répressions policières et judiciaires. Les militants ont découvert ces aspects en Russie dans les années 2010. Les informations et les traces numériques laissées sur les plateformes web par les militants de l'opposition et des militants progressistes (antiracistes, LGBT, antifascistes, etc.) ont également été utilisées par leurs ennemis politiques, membres des mouvements d'extrême-droite ou pro-Kremlin. Les mouvements d'extrême-droite se sont appropriés Internet et les outils numériques à la fin des années 1990, comme les autres groupes militants, dans des buts de propagande et d'organisation [Kuzmin, 2008]. Depuis les années 2000, ils utilisent des techniques de manipulation et de désinformation pour diffuser des discours de haine et de stigmatisation sur des sites, des bibliothèques en ligne, des blogs, puis des réseaux sociaux numériques. Internet constitue une ressource également pour ces groupes, pour préparer leurs actions de rue : LiveJournal leur a permis de coordonner la « Marche russe », une manifestation annuelle des mouvances nationalistes, qui se déroule depuis 2005 dans les grandes villes de Russie. Le Mouvement contre l'immigration illégale – qui jouait dans les années 2000 un rôle clé d'intermédiaire entre partis politiques, députés et mouvances d'extrême-droite – a organisé à l'aide de LiveJournal en 2006 des émeutes contre des personnes originaires du Caucase, en particulier

des Tchétchènes, à Kondopoga, une petite ville industrielle de Carélie. Dans les années 2000 et 2010, des blogueurs d'extrême-droite identifiaient des militants (notamment antifascistes) dans les manifestations de rue à l'aide de matériaux en ligne, les dénonçaient à la justice (via des politiciens ultranationalistes proches du pouvoir) et publiaient des listes d'« ennemis du peuple » avec noms, photographies, adresses et numéros de téléphone sur Internet. Une douzaine de militants antifascistes, dont les noms circulaient en ligne, ont été assassinés dans ces années 2000, sans que l'on sache si ces assassinats ont été la conséquence directe des identifications en ligne et des dénonciations.

Les mouvements de jeunesse pro-Kremlin sont aussi très actifs sur Internet depuis les années 2000. Des sommes considérables auraient été employées par le gouvernement pour rémunérer des blogueurs pro-gouvernementaux afin qu'ils délégitiment les opposants en inondant leurs blogs et sites de vidéos de photomontages et de commentaires diffamatoires, ou bien en organisant des cyberattaques [Stukal et al., 2022]. Avec l'apparition des blogs, des médias en ligne et des réseaux sociaux numériques, des pratiques ont émergé telles que le « *trolling* », qui est une forme de provocation visant à détourner une conversation de son sujet initial pour l'amener sur un terrain instable en employant des arguments improductifs et haineux. Ces pratiques provoquent la colère et déstabilisent les autres internautes. Une autre pratique est le « *flooding* », où quelques utilisateurs génèrent un nombre important de messages afin de « noyer » celui de leurs adversaires. La production massive d'images négatives sur les opposants au pouvoir par les acteurs pro-gouvernementaux sur Internet disqualifie Internet comme outil de discussion et de revendication politique, au profit d'usages marqués par une prédominance du divertissement et de la communication privée[5].

L'Internet de l'opposition connut un moment de culmination lors des grandes manifestations de 2011-2012. Le blog LiveJournal et les réseaux sociaux numériques Facebook et Twitter jouèrent un rôle clef dans la diffusion de contenus offrant les preuves en images des fraudes électorales [Radchenko et al., 2012 ; Reuter & Szakonyi, 2015 ; White & McAllister, 2014]. Le gouvernement déclara de son côté que ces preuves étaient des « *fakes* ». Au même moment, des mouvements de jeunesse pro-gouvernementaux organisèrent des rassemblements sur les places centrales de Moscou pour empêcher la tenue des manifestations de l'opposition. Des attaques par déni de service furent également menées sur des sites et des plateformes numériques de l'opposition (LiveJournal, Twitter, Facebook). De nombreuses rumeurs furent répandues dans ces réseaux sur la dangerosité de se rendre aux manifestations. Les internautes réagirent à ces attaques et menaces en ligne par des énoncés humoristiques et des appels à

5 Arsène constate la même chose pour la Chine [2011, p. 897].

manifester. Les médias sociaux numériques, y compris VKontakte, facilitèrent l'organisation, la communication et la coordination des rassemblements et renforcèrent la participation [Enikolopov et al., 2020], notamment en ayant recours à des hashtags. Après les grandes manifestations de 2011-2012, le pouvoir plaça Internet de plus en plus sous un régime de surveillance et de répressions.

Mobilisations locales, controverses et réseaux sociaux numériques. Fin des années 2000-années 2010

En Russie, l'accès domestique à Internet a considérablement augmenté au cours des vingt dernières années[6]. Internet n'est actuellement plus une technologie propre à quelques militants experts ou à la population diplômée des mégalopoles. Il est désormais utilisé par un grand nombre d'individus. Les réseaux sociaux sont devenus au fil des années l'une des principales sources d'information en Russie [Toepfl, 2013][7]. Ils sont aujourd'hui des vecteurs efficaces pour les lanceurs d'alerte qui veulent révéler des informations à un public large.

Au cours des années 2000, des mobilisations collectives locales et plus ou moins reliées entre elles, portées par des ONG ou des collectifs d'habitants, ont utilisé Internet dans différents domaines en Russie, parmi lesquels : la sauvegarde du patrimoine urbain[8] ; la défense du logement et du droit à la ville [Clément, Miriasova & Demidov, 2010], les conflits environnementaux et d'aménagement[9],

6 De 2 % en 2000 à 50 % en 2011, et à 80 % en 2019 pour la population de plus de 16 ans (https://www.tadviser.ru/index.php/Статья:Интернет-доступ_%28рынок_России%29, consulté le 17 février 2023).

7 Selon une enquête menée en août 2020 par le Centre Levada, plus d'un tiers des Russes s'informent sur les réseaux sociaux (https://www.levada.ru/2020/09/28/ggh/, consulté le 17 février 2023).

8 Contre la construction de la tour Gazprom, qui aurait été le nouveau plus grand bâtiment d'Europe, à Saint-Pétersbourg en 2009, en utilisant un site Internet, LiveJournal et VKontakte.

9 Défense de parcs urbains menacés de disparition au profit de parkings ou de projets immobiliers ; protection du lac Baïkal contre des pollutions chimiques ; défense de la forêt de Khimki, en banlieue de Moscou, contre un projet d'autoroute en 2007-2011 (selon l'observation des médias Public.ru, elle constitua le thème de la blogosphère le plus repris par les médias en 2010 et en 2011 : http://www.public.ru/blogsmi et http://www.public.ru/blogsmi2011, consultés le 17 février 2023) ; opposition au projet des Jeux Olympiques de Sotchi qui occasionna de nombreuses expropriations illégales en 2014 ; mobilisation contre un projet de méga-décharge nationale à Shies en région d'Arkhangelsk en 2018-2020).

les transports[10], la critique de l'arbitraire étatique[11], la lutte contre la réforme des retraites (2018), le syndicalisme, la défense des secteurs publics de la recherche, de l'éducation, de la culture, de l'aide sociale et de la santé, l'observation des élections et la documentation des fraudes comme le bourrage des urnes (2011-2012), etc.

Certains groupes utilisent exclusivement une seule plateforme (site, LiveJournal), d'autres plusieurs. De nouveaux outils numériques ont vu le jour dans les années 2000 : des sites ont été créés pour des pétitions liées à une mobilisation particulière, puis des sites de pétition en ligne (comme Change.org et Avaaz.org) sont apparus. Les utilisations varient également en fonction des types d'activités au sein des groupes. À la fin des années 2010, dans les mobilisations massives comme la lutte contre un projet national de méga-décharge à Shies, dans la région d'Arkhangelsk (2018-2020), les militants utilisèrent VKontakte pour la construction de la communauté et la communication. Ils se servirent également des chaînes publiques de Telegram pour diffuser des informations (le public était moindre que sur VKontakte) [Poupin, 2021a, 2021b]. VKontakte a aussi été largement utilisé lors des « émeutes des déchets » en Russie [Wu & Martus, 2020]. Pour la coordination pratique des actions, les activistes utilisent de préférence les messageries, comme WhatsApp, Viber et Telegram, plutôt que les tchats VKontakte, car elles sont perçues comme plus sûres vis-à-vis des services de police russes. Ces messageries représentent des « espaces de coulisses » dans la mobilisation [Treré, 2019].

Dès la première moitié des années 2000, Internet (LiveJournal, puis VKontakte) a constitué une source d'information instantanée et alternative aux médias officiels lors de situations d'urgence, notamment au moment d'attentats terroristes, de catastrophes naturelles [Asmolov, 2020] ou industrielles [Golbraich, 2011]. À la fin des années 2000, Internet se répand en dehors des grands centres urbains et des capitales, dans les petites et moyennes villes et dans les espaces ruraux, dans les régions les plus périphériques du pays. Internet donne à voir des régions, des territoires peu connus et des mobilisations d'habitants touchant l'environnement ou le quotidien, auparavant marginalisées et invisibilisées par les médias. Les plus fortes augmentations du nombre d'utilisateurs du Web des années 2010 et du début des années 2020 ont eu lieu dans les petites villes et les zones rurales du pays. Comme dans beaucoup de pays, la diffusion d'Internet dans certaines régions a été grandement facilitée par la réduction du coût d'accès et la propagation rapide des technologies de communication mobile.

10 Mobilisation contre les taxes douanières sur les voitures importées à Vladivostok en 2018 et contre les taxes sur les transports à Kaliningrad en 2009-2010.

11 Mouvement des Seaux bleus contre les infractions au code de la route commises par les véhicules officiels.

Sur Internet, des communautés virtuelles se créent autour de problèmes locaux communs ou de situations d'urgence. Elles réunissent des individus qui cherchent à apporter des réponses pratiques à des problèmes immédiats [Zvereva, 2012]. Face à la faiblesse et à la lenteur de la réponse gouvernementale pour régler les problèmes, des associations de volontaires se sont développées en utilisant les réseaux sociaux numériques, par exemple en 2010 autour de la lutte contre les incendies de forêt et du soutien aux victimes [Bertrand, 2017], dans le cadre du sauvetage des populations face aux crues soudaines à Krymsk dans la région de Krasnodar en 2012 [Roesen & Zvereva, 2014], pour régler des problèmes quotidiens de voirie et de gestion des espaces communs résidentiels, etc. Des activistes ont créé des applications pour documenter ce types de problèmes dans différentes sphères (élections, éducation, écologie, transport, santé publique, etc.) et les faire remonter aux autorités [Ermoshina, 2014]. De cette manière, Internet a encouragé et organisé l'action hors ligne, qui s'inscrit dans un système de débrouille mis en place dans l'urgence. Certains groupes se sont pérennisés et se sont réactivés lors d'autres catastrophes du même type. Ce fut le cas d'une bonne partie des groupes de lutte citoyenne contre les incendies de forêts.

Les questions sociétales sont marquées par des dynamiques complexes de politisation et de dépolitisation, variant selon les contextes, les dossiers et les époques. L'apparition de mobilisations et de controverses sont des moments particuliers de mise en public de problèmes et de politisation d'enjeux sociaux [Chateauraynaud, 2010]. Or, ces moments constituent des séquences limitées dans le temps. Un dossier comme la réforme des retraites, le traitement des déchets, une catastrophe industrielle devient problématique et controversé dans certaines conditions et pour une période donnée, avant d'être redéfini et de retourner dans une sorte d'«oubli» quand la routine administrative et sociale se réinstalle [Hird et al., 2014]. Lorsqu'elles sont au centre de l'attention publique et médiatique, les questions sont des «problèmes publics» [Gusfield, 2009], pour lesquels les citoyens mobilisés attendent des autorités qu'elles leur rendent des comptes, informent et décrivent ces problèmes de manière transparente[12]. Dans ces processus de visibilisation des dossiers, Internet a profondément modifié les régimes de visibilité des actions, des événements, des individus ainsi que des experts et des contre-experts. Il a bouleversé les univers de l'information et des savoirs. Internet fournit aussi en Russie de nombreux appuis critiques aux personnes qui y cherchent des informations. Il a profondément modifié les modes d'existence publique des problèmes ainsi que la portée et la circulation des arguments [Bureau et al., 2003]: il a créé de nouveaux publics, transformé les modalités d'apparition en public et la façon pour les acteurs collectifs de porter les causes, se faire entendre et lutter pour la visibilité. Il a offert un autre type de médiation que les médiations institutionnelles, télévisuelles, journalistiques

12 Ces actions sont résumées dans la notion d'"accountability' introduite par Harold Garfinkel.

traditionnelles. Internet sert à informer et à s'informer au quotidien, faire le point sur des questions controversées, mener et diffuser des contre-expertises et des enquêtes citoyennes, interpeller les pouvoirs, discuter, comparer et mettre en perspective des résultats des mobilisations. Ces processus sont visibles dans les nombreux groupes dédiés aux domaines de lutte et problèmes cités plus haut, sur VKontakte et Facebook.

Les luttes environnementales présentent des aspects intéressants concernant le lien entre mobilisations et outils numériques. Elles furent les premières actions de protestation d'ampleur tolérées par le pouvoir soviétique, durant la perestroïka. Elles donnèrent lieu à un mouvement écologiste d'envergure de 1986 à 1991 [Coumel & Elie, 2014 ; Raviot, 2001]. Après la chute du régime soviétique, ces mouvements perdirent en intensité [Coumel & Elie, 2014 ; Henry, 2010], une partie des militants écologistes furent cooptés par les organes du pouvoir eltsinien [Yanitskii, 1999]. D'autres animèrent des organisations non gouvernementales qui subsistèrent grâce à des financements occidentaux notamment. Ces dernières choisirent la voie de la modération et de l'expertise technicienne, sans assise sociale [Ziegler & Lyon, 2002]. Pendant la perestroïka, les thématiques environnementales étaient traitées, et parfois de manière critique, par les médias de masse. Elles furent exclues à partir des années 2000 de l'agenda médiatique, les médias mainstream devenant loyaux au gouvernement. Face à cette situation, les militants écologistes se tournèrent les premiers vers les médias numériques sociaux. Dans les années 2000, les organisations environnementales (comme Greenpeace, WWF, Bellona, la « Veille environnementale dans le Nord Caucase », « Sauvons [la réserve naturelle de] l'Utrish ! ») mobilisèrent très tôt les outils numériques (sites, VKontakte, LiveJournal, Facebook, Twitter) [Golbraich, 2012].

Depuis le début des années 2010, les questions environnementales et sanitaires ont pris de l'ampleur dans les médias, les réseaux sociaux numériques et les préoccupations du public[13]. Le phénomène est mondial, Tanguy Lepesant [2018] décrit des dynamiques similaires à Taïwan : après avoir connu un engouement fort dans le contexte démocratique de la fin des années 1980, les questions environnementales ont été délaissées dans les années 1990 et 2000, puis ont effectué un retour en force dans les années 2010. Cette évolution est concomitante de la montée d'Internet et des réseaux sociaux numériques. Parallèlement, les conflits environnementaux se sont multipliés dans les régions russes ce qui laisse penser que l'écologie porte en elle un des plus forts potentiels de mobilisation dans le pays, les destructions de l'environnement proche et les conditions

13 Un sondage réalisé en janvier 2020 par le Centre de recherche indépendant Levada a révélé que 48 % des Russes considéraient alors la pollution de l'environnement comme l'une des menaces principales pour l'humanité, devant le terrorisme (42 %) ou les guerres (37 %) (https://www.levada.ru/ 2020/01/23/problemy-okruzhayushhej-sredy/, consulté le 17 février 2023).

sanitaires mobilisant davantage que les questions politiques ou les droits humains. Les problèmes environnementaux les plus abordés sur des réseaux numériques de proximité comme VKontakte sont la destruction des espaces verts dans les villes, l'abattage des forêts et les projets d'aménagements menaçant les milieux naturels et la vie locale [Golbraich, 2019]. Les groupes les plus importants rassemblent plusieurs dizaines de milliers de membres.

Les groupes environnementaux sont de différents types, généralistes ou liés à un conflit spécifique. Les luttes spécifiques utilisent surtout VKontakte et YouTube. Les internautes actifs des pages dédiées aux luttes locales sortent de l'espace numérique et s'engagent dans des rassemblements et des actions hors ligne. Les groupes des luttes spécifiques sont assez disparates et plus ou moins liés entre eux. Vladimir Golbraich [2018] a montré pour la ville de Saint-Pétersbourg que les pages VKontakte de groupes locaux, spécifiques, étaient très peu connectées entre elles et à des groupes généralistes. Mais, pour certaines mobilisations massives et inédites, comme celle de la lutte contre le projet de méga-décharge à Shies, dans la région d'Arkhangelsk, le thème a circulé en dehors des groupes dédiés [Golbraich, 2021 ; Poupin, 2021a, 2021b].

Jusqu'à ces dernières années, ces initiatives et mobilisations intéressaient peu l'opposition politique, qui portait principalement des revendications d'un changement du système et dénonçait la corruption et les répressions politiques, au détriment des questions sociales et environnementales [Wood, 2018]. De leur côté, les mobilisations sociales et environnementales locales se tiennent en général loin des partis politiques, y compris des mouvements de l'opposition libérale. Les habitants mobilisés estiment que la politique est un domaine à part, dangereux, corrompu, vil, dont il ne faut pas s'approcher. Les mouvements et partis d'opposition avaient traditionnellement investi les réseaux sociaux plutôt occidentaux (Facebook, Twitter, Telegram). À partir de 2013, le cas du célèbre opposant nationaliste et libéral, Alekseï Navalny, a constitué une exception à la règle : son équipe de communication professionnelle de la Fondation anti-corruption (FBK) a mis en œuvre une stratégie transmédia visant à mobiliser l'opinion publique sur des sites Internet, des mails, LiveJournal, Twitter, Odnoklassniki, Instagram, VKontakte, Facebook, YouTube, Telegram, etc. [Gambarato & Medvedev, 2015]. Ses reportages prennent souvent (sans les citer) des matériaux publiés par des militants, des fonctionnaires et des journalistes locaux, qui habitent près des sites incriminés dans les régions : ce fut le cas par exemple de la lutte de Shies ou de la catastrophe de Norilsk (en mai 2020).

Pandémie de la Covid-19, mesures sanitaires et mobilisations revendicatives. 2020-2021

La pandémie liée à la Covid-19 a été un désastre sanitaire en Russie. Face à la crainte d'avoir à gérer un mécontentement de masse dirigé contre le président Poutine, le gouvernement a choisi de déléguer aux autorités régionales le soin de prendre, après les élections législatives de septembre 2020, des mesures contraignantes. Le résultat fut une réponse épidémique chaotique, faite de mesures très différentes dans des régions aux situations sanitaires comparables et de passes sanitaires parfois valables seulement à un niveau local. Les mesures sanitaires très strictes et non coordonnées entre elles suscitèrent des mécontentements et la méfiance vis-à-vis du pouvoir qui jusqu'alors ne s'était pas beaucoup préoccupé de la santé des personnes (le système de santé est extrêmement détérioré, notamment dans les régions). Pendant la pandémie, des masses de personnes sont passées en télétravail, à l'enseignement à distance et ont dû s'adapter à la numérisation de nombreux services de l'État. La pandémie a amené à une utilisation plus massive d'Internet et des réseaux sociaux numériques. Comme dans d'autres pays, ces réseaux ont participé à la circulation d'informations trompeuses et de discours de polarisation, de haine et de stigmatisation.

La crise sanitaire et sociale liée à la pandémie de la Covid-19 a également initié une vague de volontariat, qui s'est exercé dans ou avec les réseaux sociaux numériques. Différents mouvements d'aide ont été initiés pour approvisionner les personnes vulnérables en produits de première nécessité, soutenir les établissements et les personnels de santé et fournir une assistance juridique aux patients et leurs familles. Les utilisateurs de Yandex.Maps utilisèrent par exemple des hashtags pour mettre en lien bénévoles et personnes dans le besoin dans les quartiers des villes.

En 2020, dans le cadre des mesures restrictives mises en place, des rassemblements virtuels ont été menés dans plusieurs villes de Russie, dont Rostov-sur-le-Don, Krasnoïarsk, Nijni-Novgorod et Moscou. Les internautes plaçaient un point près d'un bâtiment qui abrite le gouvernement local ou fédéral sur une carte de l'application Yandex.Map, accompagné de commentaires comme « À bas les laissez-passer ! » La société Yandex a « dispersé » ces rassemblements en effaçant les messages jugés inappropriés. En février 2020, un rassemblement en ligne fut organisé contre la vaste révision constitutionnelle autorisant Vladimir Poutine à se maintenir au Kremlin jusqu'en 2036.

Parallèlement, et malgré le contexte pandémique, des manifestations massives de plusieurs dizaines de milliers de personnes ont eu lieu dans la rue, comme à Khabarovsk, la plus grande ville de l'Extrême-Orient russe, de juillet 2020

à septembre 2021, contre l'arrestation politique de Sergueï Fourgal, le gouverneur de la région. Les réseaux sociaux numériques VKontakte, Odnoklassniki et Twitter ont donné à voir et organiser ces événements [Brodovskaya et al., 2021]. Navalny fut arrêté en janvier 2021 à son retour de Berlin, où il avait passé plusieurs mois en convalescence après avoir survécu à un empoisonnement. Son équipe a riposté en lançant de nombreux appels à manifester sur les réseaux sociaux numériques, y compris la plateforme populaire de partage de vidéos TikTok (très utilisée par les lycéens, et où le hashtag #svobodunaval'nomu [#LibérezNavalny] a été partagé plus de 90 millions de fois en quelques jours), et a diffusé sur YouTube une enquête sur l'immense propriété de Poutine sur les rives de la mer Noire (visionnée plus de 60 millions de fois). Dans le contexte de la pandémie, le gouvernement interdisait, comme dans d'autres pays, les manifestations. Malgré cela, environ 15 000 personnes se rassemblèrent à Moscou et plusieurs milliers dans une centaine de villes du pays. Ces rassemblements furent durement dispersés.

Guerre de la Russie en Ukraine, 2022. Une conclusion

Comme nous l'avons dit précédemment, une majorité de citoyens ont accès à Internet en Russie. Les sources d'informations non-officielles, critiques et pertinentes sur un certain nombre de sujets sont disponibles, mais relativement peu utilisées. Les internautes doivent choisir qui croire : ces sources alternatives ou les sources officielles. Cette tâche est difficile car en général les choix sont peu réfléchis, les informations officielles, dominantes sont considérées exactes et fiables sans vérification des sources. La majorité de l'opinion en Russie semble avoir adhéré à l'interprétation officielle des événements qui se sont déroulés en Ukraine, en hiver-printemps 2014 (Maïdan, annexion de la Crimée puis occupation russe des territoires du Donbass) et depuis le 24 février 2022 (guerre actuelle). Ces événements ont été accompagnés d'un flot de discours et d'activités en ligne de la part de mouvements nationalistes russes. Les groupes anti-Maïdan présents sur VKontakte, financés par des fonds gouvernementaux russes, instrumentalisent la nostalgie envers le passé soviétique, cultivée par le régime de Poutine, pour décrire les manifestants ukrainiens et le gouvernement provisoire issu de la révolution de Maïdan comme des « fascistes » et des « nazis » [Kozachenko, 2019]. La thématique militariste s'est imposée à l'agenda politique et médiatique et a réussi à rester au centre de l'attention publique maintenant depuis février 2022. La télévision demeure en Russie le média principal et dominant pour la majorité de la

population[14]. Les médias dominants officiels proposent des versions numériques, qui sont des sources d'information très visitées et citées par les internautes. Les réseaux sociaux numériques constituent de cette manière des relais de la propagande étatique. Une minorité de la population, et ce n'est pas une spécificité de la Russie, connaît les règles du jeu de la désinformation.

Une petite partie de la population s'est exprimée contre la guerre à la fin du mois de février 2022, pendant un mois. La Douma d'État russe a rapidement adopté une loi sur le « discrédit de l'armée » en mars (article 20.3.3), qui concerne également Internet : les posts, les commentaires et les « likes » en ligne. Les amendements ont porté sur le Code des infractions administratives ainsi que sur le Code pénal russe. Entre fin février et fin novembre 2022, 19 428 personnes (dont la grande majorité le premier mois de la guerre) ont été arrêtées dans des rassemblements anti-guerre, un peu plus de 5 000 amendes (d'une moyenne de 400 euros) ont été dressées et environ 350 procédures judiciaires ont été engagées pour fausses informations et discrédit de l'armée[15]. La pratique montre cependant que les juges se rangent souvent du côté des citoyens accusés en vertu de cet article. Des cagnottes ont été ouvertes pour aider à payer ces amendes. Dans ce contexte de guerre et de censure des médias, l'application de messagerie Telegram a connu une montée en puissance. Elle est aujourd'hui une source d'information majeure pour les uns et un vecteur de propagande pour les autres. Internet permet ainsi la diffusion colossale de fausses informations et de propagande tout en offrant des plateformes de diffusion, de contre-vérification plus fortes qu'avant.

Nous avons ainsi vu dans ce chapitre qu'Internet sert autant à l'échange d'informations, aux discussions politiques et à l'organisation d'activités revendicatives qu'à la surveillance, à la communication et aux répressions étatiques ou venant d'organisations nationalistes, pro-gouvernementales. Le cas russe offre un intérêt pour la question des effets de l'activisme en ligne sur les activités protestataires hors ligne. D'un côté, Internet permet de rendre visibles des mobilisations et des problèmes publics qui émergent sur un territoire immense. Mais le militantisme reste en Russie une activité à très haut risque, qui demande une préparation aux situations de face-à-face, ce à quoi ne prépare pas Internet.

---

14 Selon une étude publiée par le centre indépendant Levada, la télévision a été mentionnée comme étant une source d'information par une moyenne de 63% des personnes interrogées en juin en Russie, alors qu'à Moscou, ce chiffre était de 52%. Les médias Internet ont été mentionnés par 32% des répondants en Russie et par 50% des Moscovites. Enfin, 16% des répondants en Russie et 30% des Moscovites ont mentionné Telegram comme source d'information : https://www.levada.ru/2022/07/15/istochniki-informatsii-moskva-i-rossiya/ (consulté le 17 février 2023).

15 Données de fin novembre 2022, rassemblées par le mouvement OVD-Info, né en 2011, qui répertorie les arrestations politiques dans toute la Russie et propose une aide juridique aux personnes interpellées : https://data.ovdinfo.org/svodka-antivoennyy-repressiy-devyat-mesyacev-voyny (consulté le 17 février 2023).

Nous avons vu aussi que la désinformation concerne tous les sujets politiques et sociaux en Russie, et en particulier les mobilisations revendicatives, le contexte de crise épidémique et la guerre. La désinformation a comme conséquence de créer des conflits et des divisions entre les individus ainsi que d'accentuer la polarisation sociale. Il est difficile de dire ce qui va émerger de cela. Les temps sont incertains et le sol est plus que mouvant en Russie.

Références bibliographiques

[Asmolov, 2020] Asmolov, Gregory, « Runet in crisis situations » in Davydov, Sergey (dir.), *Internet in Russia. A Study of the Runet and Its Impact on Social Life*, Cham, Springer, p. 231-250

[Arsène, 2011] Arsène, Séverine, « De l'autocensure aux mobilisations. Prendre la parole en ligne en contexte autoritaire », *Revue française de science politique* vol. 61, n° 5, p. 893-915.

[Baker, 2011] Baker, Stéphanie-Alice, « The mediated crowd : new social media and new forms of rioting », *Sociological research online* vol. 16, n° 4.

[Bloomfield & Doolin, 2012] Bloomfield, Brian & Doolin, Bill, « Symbolic communication in public protest over genetic modification : visual rhetoric, symbolic excess, and social mores », *Science Communication* vol. 20, n° 10, p. 1-26.

[Brodovskaya et al., 2021] Brodovskaia, Elena, Davydova, Maria, Doncov, Aleksandr, Hardikova, Anna, « Bazovye tendencii transformacii massovyh političeskih protestov v RF (2020 - 2021 gg.) » [Tendances fondamentales de la transformation des manifestations politiques de masse en Fédération de Russie (2020-2021)], Actes de l'Université d'État de Tula, 2, p. 45-58.

[Bureau, Chateauraynaud et al., 2003] Bureau, Marie-Christine, Chateauraynaud, Francis, Lejeune, Christophe, Torny, Didier & Trabal, Patrick, « Internet à l'épreuve de la critique », *Programme « Société de l'« information »*, CNRS.

[Cardon & Granjon, 2013] Cardon, Dominique & Granjon, Fabien, *Médiactivistes*, Paris, Presses de Sciences Po.

[Chateauraynaud, 2010] Chateauraynaud, Francis, « Des disputes ordinaires à la violence politique : l'analyse des controverses et la sociologie des conflits » in Bourquin, Laurent, Hamon, Philippe (dir.), *La Politisation : conflits et construction du politique depuis le Moyen Âge*, Rennes, Presses universitaires de Rennes, p. 91-108.

[Clément, Miriasova & Demidov, 2010] Clément, Karine, Miriasova, Olga & Demidov Andreï, *Ot obyvatelej k aktivistam. Zaroždaûiecâ social'nye dviženâ v sovremennoj Rossii* [Des hommes ordinaires aux activistes : mouvements sociaux émergents en Russie contemporaine], Moscou, Tri kvadrata.

[Cossart & Taïeb, 2011] Cossart, Paula & Taïeb, Emmanuel, « Spectacle politique et participation. Entre médiatisation nécessaire et idéal de la citoyenneté », *Sociétés & Représentations* vol. 31, n°1, p. 137-156.

[Coumel & Elie, 2014] Coumel, Laurent & Elie, Marc, « A belated and tragic ecological revolution: nature, disasters, and green activists in the Soviet Union and the Post-Soviet States, 1960s-2010s », *The Soviet and Post-Soviet Review* vol. 40, n° 2, p. 157-165.

[Desroches, 2011] Desroches, Dominic, « La fabrication du climat politique. Analyse de l'espace émotionnel et de la communauté d'émotions », *Implications philosophiques* (http://www.implications-philosophiques.org/semaines-thematiques/passions-dans-lespace-public/la-fabrication-du-climat-politique/).

[Enikolopov et al., 2020] Enikolopov, Ruben, Makarin, Alexey & Petrova, Maria, « Social media and protest participation: evidence from Russia » *Econometrica* vol. 88, n° 4, p. 1479-1514.

[Ermoshina, 2014] Ermoshina, Ksenia, « Democracy as pothole repair: Civic applications and cyber-empowerment in Russia », *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* vol. 8, n° 3.

[Etling et al., 2010] Etling, Bruce, Alexanyan, Karina, Kelly, John, Faris, Robert, Palfrey, John G. & Gasser, Urs, « Public Discourse in the Russian Blogosphere: Mapping RuNet Politics and Mobilization », *Berkman Center Research Publication*, 2010-11.

[Gambarato & Medvedev, 2015] Gambarato, Renira Rampazzo & Medvedev Sergei, « Grassroots political campaign in Russia: Alexey Navalny and transmedia strategies for democratic development », *Promoting social change and democracy through information technology*. *IGI Global*, p. 165-192.

[Gamson, 1998] Gamson, William, « Social movements and cultural change » in Giugni, Marco, McAdam, Doug & Tilly, Charles (dir.), *From Contention to Democracy*, Lanham and Oxford, Rowman & Littlefield Publishers, p. 57-77.

[Gitlin, 1980] Gitlin, Todd, *The Whole World is Watching*, Berkeley, University of California Press.

[Gladarev, 2013] Gladarev, Boris, « Opyty preodolenia « publičnoj nemoty » : analiz obŝ estvennyh diskussi v Rossii načala XXI veka » [Des expériences de dépassement de la « surdité publique » : analyse de discussions publiques en Russie au début du XXI[e] siècle], *La société russe à la recherche d'une langue publique : hier, aujourd'hui, demain* (conférence 15-17 janvier 2013, Saint-Pétersbourg), Saint-Pétersbourg, Éditions de l'Université européenne de Saint-Pétersbourg, p. 13-19.

[Golbraich, 2011] Golbraich, Vladimir, « Počemou proizošel « Sibirskij černobyl' »? Avaria na Saâno-šušenskoj GES v rossiskoj blogosfere » [Pourquoi le « Tchernobyl sibérien » a-t-il eu lieu ? L'accident de la centrale hydroélectrique Sayano-Shushenskaya dans la blogosphère russe], *Télescope : une revue de recherche sociologique et de marketing*, 6, p. 39-45.

[Golbraich, 2012] Golbraich, Vladimir, « Social'nye seti v Internete kak resours dlâ ekologičeskogo dviženâ v Rossii » [Les médias sociaux sur Internet comme ressource pour le mouvement environnemental en Russie] in Božkov, Oleg (dir.), *La sociologie hier, aujourd'hui, demain*, Éditions Eidos, p. 361-375.

[Golbraich, 2018] Golbraich, Vladimir, « Členy ekologičeskih grupp v sotsial'ny'h media : tsifrovoe učastie i interesy » [Les membres des groupes environnementaux sur les médias sociaux : participation numérique et centres d'intérêt], *La sociologie pétersbourgeoise aujourd'hui*, 9, p. 91-119.

[Golbraich, 2019] Golbraich, Vladimir, « Ekologičeskie konflikty v Rossii i cifrovoe setevoe učastie » [Les conflits écologistes en Russie et la participation aux réseaux numériques], *Sociologičeskie issledovaniâ* vol. 6, p. 74-85.

[Golbraich, 2021] Golbraich, Vladimir, « Ekologičeski konflikt v povestke dlâ social'noj seti » [Les conflits environnementaux au programme des médias sociaux], *Sociologie et gouvernement* vol. 7, n° 2, p. 102-115.

[Gromov, 2008] Gromov, Dmitri, « Ulitčny teatr molodežnoj politiki : oppozicionnye dviženia » [Le théâtre de rue de la politique des jeunes : les mouvements d'opposition], *Etnograficheskoe obozrenie*, 1, p. 19-29.

[Gunthert, 2013] Gunthert, André, « La culture du partage ou la revanche des foules » in Le Crosnier, Hervé (dir.), *Culturenum. Jeunesse, culture et éducation dans la vague numérique*, Caen, C & F Editions, p. 163-175.

[Gunthert, 2014] Gunthert, André, « L'image conversationnelle », Études photographiques, n°31.

[Henry, 2010] Henry, Laura, *Red to Green. Environmental Activism in Post-Soviet Russia*, Ithaca, NY, Cornell University Press.

[Kireev, 2006] Kireev, Oleg, *Povarennaâ kniga media-aktivista* [Le livre de recettes du media-activiste], Moscou, Ultra Kultura.

[Kiriya, 2012] Kiriya, Ilia, « Les réseaux sociaux comme outil d'isolation politique en Russie », *Journal of Communication Studies*, vol. 5, n°1(9), p. 193-207.

[Kozachenko, 2019] Kozachenko, Ivan, « Fighting for the Soviet Union 2.0: digital nostalgia and national belonging in the context of the Ukrainian crisis », *Communist and Post-Communist Studies*, vol. 52, n° 1, p. 1-10.

[Kuzmin, 2008] Kuzmin, Alexander, « « Pravy » Internet v Rossii : specifika razvitia i problemy protivodejstvâ » [L'Internet de droite en Russie : spécificités du développement et problèmes de la lutte contre ce phénomène »], POLITEX, vol. 4, n° 3, p. 74-96.

[Lepesant, 2018] Lepesant, Tanguy, « Les questions environnementales, espace de (re) politisation de la jeunesse taïwanaise », *Monde chinois*, n° 56, p. 108-119.

[Lipsky, 1968] Lipsky, Michael, « Protest as a political ressource », *American Political Science Review* vol. 62, n° 4, p. 1144-1158.

[Lysenko & Desouza, 2010] Lysenko, Volodymyr & Desouza Kevin, « Cyberprotest in contemporary Russia : the cases of Ingushetiya.ru and Bakhmina.ru », *Technological Forecasting & Social Change*, 77, p. 1179-1193.

[Matvejchev, 2010] Matvejchev, Oleg, *Povelitel'noe naklonenie istorii* [Inclinaison autoritaire de l'histoire], Moscou, Éksmo.

[Nenachev, 2010] Nenachev, Mikhaïl, *Illiuzii svobody. Rossijskie SMI v epohu peremen (1985-2009)* [L'illusion de la liberté. Les médias russes dans une époque de changement (1985-2009)], Moscou, Logos.

[Neveu, 1999] Neveu, Erik, « Médias, mouvements sociaux, espaces publics », *Réseaux*, vol. 17, n° 98, p. 17-85.

[Neveu, 2010] Neveu, Erik, « Médias et protestation collective » in Agrikoliansky, Eric, Sommier, Isabelle & Fillieule, Olivier (dir.), *Penser les mouvements sociaux*, Paris, La Découverte, p. 245-264.

[Nocetti, 2012] Nocetti, Julien, « Le Web en Russie : de la virtualité à la réalité politique ? », *Russie.Nei.Reports*, 10.

[O'Lear, 1999] O'Lear, Shannon, « Networks of engagement: Electronic communication and grassroots environmental activism in Kaliningrad », *Geografiska Annaler: Series B, Human Geography* vol. 81, n° 3, p. 165-178.

[Pariser, 2011] Pariser, Eli, *The Filter Bubble. What the Internet Is Hiding from You*, New York, Penguin Press.

[Poberezhskaya, 2018] Poberezhskaya, Marianna « Blogging about climate change in Russia: activism, scepticism and conspiracies », *Environmental Communication* vol. 12, n° 7, p. 942-955.

[Poupin, 2013] Poupin, Perrine, « Quand les manifestants s'emparent de la vidéo à Moscou: communiquer ou faire participer ? », *Participations*, n° 7, p. 73-96.

[Poupin, 2021a] Poupin, Perrine, « Shies, d'une opposition à un projet de décharge à un conflit régional contre l'importation de déchets de Moscou dans le Grand Nord (région d'Arkhangelsk) », *EchoGéo*, 56, avril-juin.

[Poupin, 2021b] Poupin, Perrine, « Government responses to online activities of waste protest: the case of VKontakte and the Shies uprising in Far Northern Russia », *First Monday*, vol. 26, n° 5.

[Radchenko et al., 2012] Radchenko, Darya, Pisarevskaya, Dina, & Ksenofontova, Irina, « Logika virtual'nogo protesta : nedelâ posle vyborov-2011 » [La logique de la protestation virtuelle : la semaine suivant les élections de 2011]. *Forum d'anthropologie*, vol. 16, p. 108-126.

[Rakhmanova, 2012] Rakhmanova, Tania, *Au cœur du pouvoir russe. Enquête sur l'empire Poutine*, Paris, La Découverte.

[Raviot, 2001] Raviot, Jean-Robert, « L'écologie et les forces profondes de la perestroïka », *Diogène* vol. 194, n° 2, p. 152-159.

[Reuter & Szakonyi, 2015] Reuter, Ora John & Szakonyi, David, « Online social media and political awareness in authoritarian regimes », *British Journal of Political Science* vol. 45, n° 1, p. 29-51.

[Roesen & Zvereva, 2014] Roesen, Tine & Zvereva, Vera, « Social networks sites on the Runet: Exploring social communication » in Gorham, Michael, Lunde, Ingunn & Paulsen, Martin (dir.), *Digital Russia. The Language, Culture and Politics of New Media Communication*, Abingdon, Routledge, p. 72-87.

[Rucht, 2004] Rucht, Dieter, « The quadruple « A »: media strategies of protests movements since the 1960s » in van de Donk, Wim, Loader, Brian, Nixon, Paul G. & Rucht, Dieter (dir.), *Cyber Protest. New Media, Citizens and Social Movements*, London, Routledge.

[Sobieraj, 2011] Sobieraj, Sarah, *Soundbitten. The Perils of Media-Centered Political Activism*, New York University Press.

[Stukal et al., 2022] Stukal, Denis, Sanovich, Sergey, Bonneau, Richard & Tucker, Joshua A., « Why Botter: How Pro-Government Bots Fight Opposition in Russia », *American Political Science Review* vol. 116, n° 1, p. 843-857.

[Tchernyshev, 2008] Tchernyshev, Yuri, « O vlânij blogosfery na rossijskuiû publičnuiû politiku » [Sur l'impact de la blogosphère sur la politique publique russe], Sciences politiques, 2, p. 99-118.

[Toepfl, 2013] Toepfl, Florian, « Making sense of the news in a hybrid regime: how young Russians decode state TV and an oppositional blog », *Journal of Communication* vol. 63, n° 2, p. 244-265.

[Trakhtenberg, 2004] Trakhtenberg, Anna, « Informatsionnaâ revoliuciâ i informacionnij raskol: čto proishodit v Rossii? » [La révolution de l'information et la fracture informationnelle : Que se passe-t-il en Russie ?], Rapport annuel scientifique de l'institut de philosophie et de droit du Département de l'Oural de l'Académie des Sciences de Russie, 5, p. 329-343.

[Treré, 2019] Treré, Emiliano, *Hybrid Media Activism: Ecologies, Imaginaries, Algorithms*, Abingdon, Routledge.

[Yanitskii, 1999] Yanitskii, Oleg, « Russian Environmental Movements » in Conway, Jill, Keniston, Kenneth, Marx, Leo (dir.), *Earth, Air, Fire, Water: Humanistic Studies of the Environment*, Amherst, University of Massachusetts Press.

[White & McAllister, 2014] White, Stephen & McAllister, Ian, « Did Russia (nearly) have a Facebook revolution in 2011? Social media's challenge to authoritarianism », *Politics* vol. 34, n° 1, p. 72-84.

[Wood, 2018] Wood, Tony, *Russia Without Putin. Money, Power and the Myths of the New Cold War*, Londres et New York, Verso.

[Wu & Martus, 2020] Wu, Fengshi & Martus, Ellie, « Contested environmentalism: The politics of waste in China and Russia », *Environmental Politics* vol. 30, n° 4, p. 493-512.

[Zvereva, 2012] Zvereva, Vera, *Setevye razgovory : kul'turnye kommunikacii v Runete* [Conversations en réseau : la communication culturelle au sein de Runet], University of Bergen.

[Ziegler & Lyon, 2002] Ziegler, Charles & Lyon, Henry, « The Politics of Nuclear Waste in Russia », *Problems of Post-Communism* vol. 49, n° 4, p. 33-42.

Chapitre 8

De l'emprise numérique à la répression physique : perquisitions, prison, exil et guerre

Olga Bronnikova, Françoise Daucé, Ksenia Ermoshina, Benjamin Loveluck

Dans les années 2010, les emprises politiques encadrant l'Internet russe ont longtemps été multiples, distribuées et indirectes (boîtes noires, FAI, algorithmes, gestion des données, règles du copyright, etc.). Elles ont relevé de la régulation et du guidage (*channeling*) des comportements numériques plutôt que de la violence physique. Avec le renforcement progressif de la coercition autoritaire, ces emprises se sont transformées en atteintes directes à la sécurité des personnes et des biens numériques par les structures d'État : perquisitions brutales avec saisie de matériel dans les locaux des médias, des ONG et au domicile des militants ou poursuites pénales pour des publications en ligne. Les lois sur les « agents de l'étranger », sur les « organisations extrémistes » et sur les « organisations indésirables » ont été amendées pour s'appliquer à des militants, journalistes, chercheurs et activistes de plus en plus nombreux. Des affaires criminelles ont été ouvertes contre les plus engagés et publics d'entre eux. La répression s'est renforcée avec l'empoisonnement puis l'emprisonnement de l'opposant A. Navalny et l'interdiction de l'ensemble de son mouvement en 2020. Elle a culminé avec l'invasion à grande échelle de l'Ukraine en février 2022 et l'adoption de la loi dite sur « les fausses informations militaires » qui interdit l'emploi du mot « guerre » (4 mars 2022). Les dispositifs de répression policière et pénale sont mis en place pour empêcher toute mobilisation critique.

Ce durcissement politique articule contraintes hors ligne et en ligne, s'inscrivant ainsi dans des dynamiques larges de « répression numérique » (*digital repression*) documentées dans d'autres contextes [Keremoğlu & Weidmann, 2020 ; Feldstein, 2021 ; Earl et al, 2022]. L'enjeu n'est plus seulement celui de la surveillance ou du contrôle par les outils numériques, il englobe la question de la sécurité physique des personnes. Dans une acception large, selon [Earl et al, 2022], la répression numérique inclut :

- l'usage de techniques de répression traditionnelles contre les protestataires en ligne (arrestations, détentions, amendes, perquisitions…) ;

- l'usage d'outils numériques pour renforcer les dispositifs répressifs traditionnels (surveillance, écoutes, profilage, reconnaissance faciale…) ;
- le développement de stratégies d'information destinées à diminuer la protestation.

Elle a été bien documentée par exemple à partir de l'arrestation de bloggers saoudiens [Pan et al, 2020], de militants azéris [HRW, 2021], d'activistes au Kazakhstan [Anceschi, 2015], en Egypte, Syrie ou Iran [Michaelsen, 2020]. Les militants agissent généralement en ligne et hors ligne, la répression s'exerçant en retour dans ces deux dimensions.

En Russie depuis 2020, et particulièrement suite à l'agression militaire contre l'Ukraine en 2022, le renforcement des menaces aussi bien numériques que traditionnelles, fondées sur l'usage de la force policière et les arrestations physiques des militants et de leurs biens, conduit nombre d'entre eux à devoir choisir l'exil. Depuis l'étranger, les infrastructures et équipements numériques constituent des ressources pour faciliter leur coordination à distance. « L'exil numérique » permet les « appartenances mobiles ici et là-bas » (*mobile belonging here and there*) des personnes connectées à la fois dans leur pays d'accueil et d'origine, à l'exemple des militants iraniens déplacés [Bublatzky, 2022]. Mais, dans le contexte de la guerre, ces liens sont aussi porteurs de risques, notamment pour leurs interlocuteurs restés au pays. Le maintien des communications par-delà la ligne de front peut exposer les acteurs à de nouvelles formes de suspicion. Cette dialectique à double tranchant a été bien documentée dans le cas des activistes syriens et irakiens [Gillespie et al, 2018]. Les déplacements ne mettent pas fin aux menaces sécuritaires pesant sur les exilés politiques, qui se trouvent parfois exposés à des formes de répression transnationale, comme lors des Printemps arabes [Moss, 2016] ou dans les cas des militants iraniens et syriens [Michaelsen, 2020]. Dans cette situation, ils développent de nouveaux rôles autour de projets de sous-veillance, de protection, de formation et d'expertise sur les questions numériques [Porlezza & Arafat, 2022] pour poursuivre leur lutte depuis l'étranger. Engagés contre la guerre en Ukraine, ils mobilisent leurs savoirs militants et techniques pour dénoncer les dérives autoritaires de l'État russe ainsi que les résurgences d'un impérialisme génocidaire.

Ce chapitre analyse les trajectoires des acteurs de l'Internet libre, que nous avons d'abord rencontrés en Russie dans le cadre de notre enquête de terrain pour le projet ResisTIC puis retrouvés à l'étranger après leur exil contraint. Nous avons ainsi documenté les épreuves affrontées par ces militants (notamment ceux des associations Roskomsvoboda, Teplitsa et OZI), par les journalistes indépendants (des principaux médias en ligne critiques) et par les militants associatifs en butte aux répressions du pouvoir russe. Les militants biélorusses, confrontés aux brutales répressions depuis les manifestations de l'été 2020, croisent aussi leur

chemin. Depuis l'étranger, ces acteurs sont dispersés mais connectés [Diminescu, 2005]. Opposés à la guerre en Ukraine et au régime de V. Poutine, ces exilés (qui se qualifient pour certains de *relokanty* ou « relocalisés »[1]) demeurent insérés dans les réseaux et les sociabilités de leur pays, continuant généralement à mener des activités critiques à destination du public russe depuis l'étranger ou imaginant de nouvelles initiatives associatives et médiatiques en direction des publics de la diaspora. Pour ce faire, ils bénéficient du desserrement de la contrainte dans leurs pays d'accueil mais sont pris dans les affrontements géopolitiques de la guerre. L'exil introduit une situation d'asymétrie importante quant aux risques numériques et juridiques encourus entre les relocalisés et ceux qui sont restés [Ermoshina, 2023], ce qui implique notamment la mise en cause de la légitimité des discours des relocalisés par les personnes restées en Russie, notamment, quand les premiers lancent des appels à la contestation depuis les pays « sûrs » où ils sont installés.

Les atteintes à l'intégrité physique et numérique : arrestations, perquisitions et saisies

Tout au long des années 2010, le répertoire répressif de l'État russe se diversifie, créant un faisceau de normes (pénales, judiciaires et techniques) pesant sur les usages numériques (voir chapitre 1). Les contraintes, distribuées et multiples, s'appuient sur les infrastructures techniques (fournisseurs d'accès et de services, plateformes, boîtiers, réseaux, algorithmes) pour discipliner l'espace public. Dès 2012, la loi autorise les premiers blocages de sites sans décision de justice. En 2016, d'après le Google Transparency Report, l'État russe est celui qui adresse le plus grand nombre de demandes de suppression de contenus à Google [Bronnikova & Zaytseva, 2021]. La même année, entrent en vigueur les lois dites « Iarovaïa », obligeant les fournisseurs d'accès Internet à sauvegarder les données de trafic des utilisateurs et fournir aux services gouvernementaux à leur demande, les données personnelles et, le cas échéant, les contenus de leurs messageries électroniques. À partir de 2017, de nombreux opérateurs numériques sont avertis par Roskomnadzor et menacés d'amendes ou de fermetures. En 2018, l'État russe tente de bloquer, sans succès, l'application Telegram.

Progressivement, les personnes physiques elles-mêmes, et pas seulement leurs données ou les contenus produits, sont prises dans le maillage oppressif du pouvoir, menacées d'amendes et de détentions de plus en plus lourdes. Les arrestations,

1 Néologisme forgé lors de la pandémie du Covid-19 pour désigner le déplacement géographique de personnes travaillant à distance. Ce terme, désormais employé par certaines personnes contraintes de quitter la Russie après la guerre, s'ajoute aux autres catégories du déplacement (migrants, exilés, déplacés, expatriés).

perquisitions et autres menaces policières constituent autant de dangers pour les utilisateurs d'Internet. Les poursuites liées à l'administration d'outils de contournement comme Tor («L'affaire Bogatov»)[2], à la publication ou à la re-publication en ligne de contenus critiques ou l'ouverture d'affaires pénales pour des faits supposés d'«extrémisme» ont un effet d'avertissement pour l'ensemble des acteurs critiques de l'Internet russe, s'appuyant sur des pratiques policières et sécuritaires bien documentées en Russie [Le Huérou, 2022], mais aussi sur des formes d'intimidation «par le bas» telles que les dénonciations de «citoyens vigilants» [Favarel-Garrigues, 2018 ; Daucé et al, 2020]. Avec la guerre, tous les opposants à l'agression militaire russe contre l'Ukraine, en ligne et hors ligne, sont directement menacés dans leur intégrité physique, mais aussi dans leur intégrité numérique, ce qui, en raison du caractère omniprésent et intime d'Internet, peut être considéré comme une atteinte aux droits de l'homme [Rochel, 2021].

Les atteintes aux organisations et aux personnes physiques

Pour étouffer toute contestation, le répertoire d'action répressif s'appuie sur des méthodes traditionnelles, communes à tous les États oppresseurs : dénonciations, arrestations, détentions provisoires, ouverture d'affaires criminelles, perquisitions. Tout au long des années 2010, les manifestations et actions de rue s'accompagnent d'arrestations massives suivies de détentions provisoires (de quelques jours à quelques semaines). Les services de sécurité ouvrent des poursuites pénales contre les militants, journalistes et citoyens les plus engagés. Ces procédures s'accompagnent généralement de perquisitions dans leurs bureaux mais aussi à leur domicile.

Les organisations et médias oppositionnels tombent sous le coup de la loi sur les «organisations extrémistes» ou sur «les organisations indésirables» qui mettent en péril leurs membres. À partir de 2020, la législation sur les «agents de l'étranger», qui concernait initialement les associations (2012) et les médias (2017) est élargie

2 Dmitry Bogatov est un développeur, enseignant en mathématiques, militant du logiciel libre, contributeur des projets Debian et GNU, espérantiste. Il a été accusé d'avoir lancé des appels publics à des actes terroristes sur Internet, sur le forum sysadmins.ru. Ces messages ont été identifiés avec l'adresse IP d'un serveur hébergé au domicile de Bogatov, il s'agissait d'un nœud de sortie du réseau Tor maintenu par Bogatov. Le mathématicien a d'abord été placé en détention provisoire le 6 avril 2017, mais une campagne de soutien a été organisée et soutenue par de nombreuses associations russes et internationales comme le Parti Pirate, Roskomsvoboda, Access Now, Electronic Frontier Foundation mais aussi par des projets de logiciels libres comme Debian et Torproject lui-même. L'affaire Bogatov a mobilisé la communauté des développeurs du logiciel libre et des cypherpunks, jusqu'à une série de tweets par Edward Snowden lui-même en juillet 2017. Six mois après son arrestation, Bogatov a été assigné à résidence dans son appartement à Moscou, puis acquitté. Avec sa femme Natalia Fedorova, chercheuse, docteure en biologie, ils ont quitté la Russie et se sont installés aux États-Unis où Bogatov a obtenu le statut de réfugié politique.

aux personnes physiques à titre personnel. De nombreux journalistes et militants associatifs, rencontrés dans le cadre de notre enquête, sont inscrits au registre tenu par le ministère de la Justice à l'exemple de Lev Ponomariov (défenseur des droits de l'homme, n°1 au registre), Daria Apakhonchich (militante féministe, n°5), Elizaveta Maetnaya (journaliste de *Radio Svoboda*, n°13), Sergei Smirnov (rédacteur en chef de *Mediazona*, n°46), Mikhaïl Klimarev (directeur de la Société pour la défense d'Internet, n°112) ou encore Natalia Baranova (militante de la « Serre des technologies sociales », n°113)… La liste est longue et s'allonge de mois en mois. Toutes les personnes concernées, morales et physiques, sont soumises à des contrôles approfondis (de leurs ressources et dépenses notamment) et doivent également publier en ligne un bandeau qui annonce officiellement leur statut d'« agent de l'étranger ».

À partir de 2019, les militants de la Fondation de lutte contre la corruption d'Alekseï Navalny sont particulièrement visés par les poursuites et les perquisitions. Un militant ayant collaboré à l'émission *Navalny Live*, diffusée en ligne sur YouTube, décrit des perquisitions quasi hebdomadaires dans le studio avec la saisie de tout le matériel audio et vidéo pour empêcher la retransmission. L'équipe doit innover en créant deux studios parallèles, pour pouvoir basculer la diffusion de l'un à l'autre. « Parfois les flics ne comprenaient vraiment pas ce qui se passait. Ils bloquaient tout pendant la perquisition et la retransmission continuait. Ça les mettait hors d'eux »[3]. Par ailleurs, ces fouilles et perquisitions s'accompagnent souvent de violences physiques et d'humiliations psychologiques (« Ils nous ont mis au sol, la tête dans le tapis et nous ont laissé comme ça pendant six heures en proférant des menaces de passage à tabac. On ne nous laissait même pas aller aux toilettes »). Bien plus qu'un instrument d'enquête judiciaire ou administrative, la perquisition se présente dans ce contexte comme une méthode éprouvée de harcèlement et d'intimidation. En avril 2021, la Fondation d'A. Navalny est dissoute sur l'ensemble du territoire, après avoir été inscrite sur la liste des « organisations extrémistes et terroristes ».

Les perquisitions concernent aussi les organisations de défense des droits humains et les rédactions des médias d'investigation. En juin 2021, des perquisitions ont lieu au domicile des journalistes du média *Proekt*. Quelques jours plus tard, celui-ci est déclaré « indésirable » en Russie, accusé de menacer l'ordre et la sécurité du pays. Les usagers qui collaborent avec sa rédaction sont passibles de poursuites pénales. En juillet 2021, l'association Komanda 29, engagée dans la défense des prisonniers politiques, est également déclarée indésirable et met fin à l'ensemble de ses activités. Pour protéger ses membres, elle supprime tous ses contenus en ligne ainsi que ses comptes sur les réseaux sociaux. Elle conseille à ses lecteurs de supprimer tous les contenus produits par l'association, ce qui équivaut à la

3 Entretien avec un militant en exil, Varsovie, juin 2022.

disparition de toute trace de son activité. De manière générale, les répressions physiques et numériques de ces dernières années mettent en cause la pérennité des contenus numériques : tant les formateurs en sécurité numérique, que les médias et ONG en danger, préconisent la suppression des données au niveau individuel (nettoyage de la mémoire des ordinateurs et téléphones) et collectif (suppression régulière de l'historique des tchats, voire suppression des sites entiers, comme pour Komanda 29). En réponse, des projets d'archivage indépendants ont été lancés, tels que l'Archive Numérique Nationale[4], alors que l'État russe mène de son côté l'archivage des contenus à des fins notamment judiciaires[5].

Les atteintes aux biens informatiques et aux données numériques

Si les répressions (arrestations et perquisitions), bien documentées par les associations de défense des droits de l'homme depuis 2012[6], mettent en péril l'intégrité physique des personnes, elles menacent aussi leurs équipements et données numériques. Lors des arrestations, ces derniers sont particulièrement vulnérables. La saisie des ordinateurs et des téléphones portables est officiellement illégale mais possible sous la menace de la force. Elle prive les militants de tout outil de communication et met en péril les données liées à leur activité mais aussi les informations personnelles conservées dans leurs appareils. Lors des perquisitions à domicile, les atteintes aux biens numériques sont systématiquement documentées. Les équipements informatiques (ordinateurs, téléphones, disques durs) sont saisis, posant le problème de la sécurité des personnes perquisitionnées ainsi que de leur entourage militant et professionnel.

À partir de 2018, de nombreux témoignages, notamment dans le réseau du mouvement d'A. Navalny, décrivent ces atteintes. Un militant témoigne ainsi : « Lorsqu'ils ont perquisitionné, j'ai juste eu le temps de bloquer l'accès à mon téléphone et à ma chaîne Telegram. Mais je n'ai rien pu faire pour mon Mac qui a été saisi ». Deux ans plus tard, en 2020, il est à nouveau arrêté pour « non respect des organes du pouvoir ». Lors de son séjour d'une semaine en prison, il témoigne : « On a saisi mon téléphone. Je ne pouvais l'utiliser que 15 minutes par jour. Je n'étais pas prêt pour cette situation car toutes mes données étaient sur ma carte sim. Ils ont pris toutes les données de mon compte Microsoft, tous mes contacts sur Skype. Ils ont tout pompé, absolument tout. Quand on oblige quelqu'un à mettre son empreinte digitale pour ouvrir le téléphone, on

4 https://ruarxive.org/ (consulté le 17 février 2023).

5 https://web-arhive.ru/ (consulté le 17 février 2023).

6 Voir les rapports de la Fédération internationale des droits de l'homme (FIDH) sur la Russie (https://www.fidh.org/fr/regions/europe-asie-centrale/russie/14548-russie-2012-2013-l-offensive-contre-les-libertes, consulté le 17 février 2023).

ne peut rien faire»[7]. Une autre militante d'une antenne régionale du mouvement d'A. Navalny rapporte aussi : « Il y a eu des perquisitions en 2019 quand ils ont ouvert les premières affaires pénales, en nous accusant de blanchir de l'argent criminel (…). Les perquisitions ont eu lieu dans les bureaux du mouvement et au domicile des militants. Il y a eu trois vagues : d'abord les coordinateurs du mouvement, puis les bénévoles et enfin leurs parents. Ils ont voulu nous priver de tous nos équipements ». Tous ? « Oui, Les téléphones, les ordinateurs, les clés USB, les appareils photos, absolument tout »[8]. Dans le cas de l'affaire contre Ekaterina Muranova, militante anarchiste de Medvejiegorsk accusée d'apologie du terrorisme, même la tablette de son fils de six ans a été saisie.

Face à ces risques, les acteurs concernés développent des savoir-faire juridiques et techniques pour se former aux nouveaux outils de protection et acquérir les principes de la « sécurité holistique », qui englobe la sécurité physique et juridique des personnes et de leurs données numériques mais aussi leur intégrité psychologique (voir chapitre 4). Les associations de défense des droits humains et numériques, comme OVD-Info ou la Serre des technologies sociales, publient des conseils à destination des personnes arrêtées, pour leur permettre de se défendre. Toutes les associations conseillent de se servir en priorité d'un téléphone quasiment vierge pour les manifestations et actions de rue. Le cas échéant, lors des détentions administratives, elles proposent de bloquer son téléphone avant de le remettre à la police et de demander sa restitution à l'issue de la garde à vue. Légalement, les biens saisis doivent être restitués à l'issue de la procédure d'enquête judiciaire. Cependant, la fiabilité des biens rendus est mise en doute par les militants. Comme l'explique l'un d'eux, « Il ne faut surtout pas utiliser les matériels qui sont restitués par la police car ils sont susceptibles de contenir des programmes malveillants ou de surveillance dangereux pour leurs utilisateurs »[9].

Le déclenchement de la guerre et l'exil sous la contrainte

Pour les plus engagés, les détentions, mais surtout les perquisitions qui les accompagnent, sont généralement comprises comme un avertissement sérieux, les conduisant à envisager leur exil. Dans certains cas, à l'issue de la perquisition, la police restitue le passeport international à son détenteur, ce qui est immédiatement interprété comme une incitation au départ. Les formateurs en sécurité conseillent par ailleurs de garder le passeport international hors domicile. Lorsque le passeport n'est pas restitué, la menace d'arrestation se précise, incitant les personnes concernées à quitter illégalement le territoire par toutes les voies possibles (même

7 Entretien avec un militant en exil, Vilnius, novembre 2021.

8 Entretien avec une militante de la Fondation de lutte contre la corruption, Tbilissi, mai 2022.

9 Entretien avec un militant, Vilnius, novembre 2021.

terrestres, à travers les forêts aux frontières occidentales du pays). Une journaliste en exil à Vilnius évoque ainsi la trajectoire d'un collègue contraint de fuir :

> « Il a passé la frontière ukrainienne à pied, sa famille est restée à Moscou. Il y a eu une perquisition chez lui et on lui a pris ses deux passeports. Cela signifiait un risque de prison. Quand on vous laisse votre passeport après une perquisition, c'est une invitation à fuir »[10].

Avec l'invasion de l'Ukraine en février 2022, l'incitation au départ devient plus explicite encore. Malgré les risques de répression, de nombreux citoyens signent des pétitions en ligne pour dénoncer la guerre (la pétition lancée par le défenseur des droits de l'homme Lev Ponomarev collecte plus d'un million de signatures en quelques jours), les plus intrépides descendent dans la rue, où les forces de l'ordre procèdent à des arrestations massives. L'adoption de la loi sur les « fausses nouvelles militaires » (4 mars 2022) interdit aux journalistes d'employer le terme même de « guerre » et leur impose la publication des sources officielles. Refusant de se soumettre à la censure, de nombreux médias, enregistrés comme « agents de l'étranger » sont définitivement bloqués à la demande de Roskomnadzor. Pour leur couverture de la guerre en Ukraine, les sites de la télévision *Dojd*, de la radio *Echo de Moscou* mais aussi des sites d'information *Meduza*, du service russe de la BBC ou de *Radio Svoboda* sont interdits en Russie. Ces blocages concernent aussi les grandes plateformes internationales. Facebook et Twitter sont bloqués tandis que TikTok suspend ses activités[11]. À ceci il faut ajouter les départs volontaires du marché russe de compagnies technologiques et fournisseurs de services étrangers ainsi que la suspension d'accès aux systèmes de paiement en ligne par Google et Apple pour les utilisateurs russes. L'ensemble de l'écosystème numérique russe, où coexistaient opérateurs internationaux (GAFAM) et nationaux (VKontakte, Yandex), est bouleversé par les restrictions numériques du temps de guerre. Seuls les services de YouTube demeurent accessibles, constituant le principal canal ouvert pour accéder à des contenus médiatiques et culturels alternatifs.

Dans ce contexte, des militants, journalistes et citoyens reçoivent des menaces, directes ou indirectes, des services de sécurité. Parfois incrédules lors des premières alertes, ils évaluent ensuite les risques qu'ils encourent. Un journaliste indépendant de Rostov rencontré à Tbilissi raconte ainsi :

> « Le 24 février, (…) une amie qui connaît quelqu'un au FSB m'a écrit pour me dire que… eh bien, je dois quitter la Russie, parce que sinon je serai probablement bientôt poursuivi pour une affaire pénale. Je lui ai demandé : "ce sont des poursuites pénales contre moi ou contre les journalistes en général ?". Elle m'a dit :

10 Entretien avec une journaliste à Vilnius, novembre 2021.

11 Pour une chronologie de ces blocages, voir https://timeline.resistic.fr/

> "contre toi personnellement". J'ai répondu un truc du genre "*Fuck you*, je ne vais nulle part, je vais rester ici jusqu'au bout" (…) Trois jours plus tard, j'ai plus ou moins repris mes esprits et je me suis dit que je devais vraiment quitter la Russie, car si j'allais en prison maintenant, ce serait totalement inefficace par rapport à ma famille, mon travail… »[12]

Une fois prise la décision du départ, les conditions même du « passage numérique » vers un autre pays constituent une expérience transformative, conduisant à emporter tout ce que l'on peut de sa « vie numérique » tout en dissimulant ce qui pourrait être compromettant [Latonero, 2015]. Les militants et journalistes veillent à supprimer toutes les données présentes sur leurs appareils et à se déconnecter des principaux réseaux sociaux qu'ils utilisent pour ne pas attirer l'attention des services de sécurité. Des guides de bonnes pratiques ainsi que des sites du type wiki se multiplient, qui essaient de synthétiser les expériences de passage de frontières et des pratiques d'auto-défense holistique pendant les voyages à l'étranger. Comme en témoigne le journaliste de Rostov :

> « À l'aéroport, j'ai été interrogé par les hommes du FSB. Ils ont vérifié mon application Telegram. Je m'y attendais et j'avais supprimé toutes les chaînes que je suivais (…). Ils m'ont interrogé sur mes préférences politiques. J'ai répondu que je ne soutiens aucun mouvement car aucun ne me plaît ».

Il poursuit : « Il faut chiffrer le disque de son notebook quand on passe les frontières russe, biélorusse, azérie. Si les autorités le saisissent pendant quarante minutes et qu'il n'est pas crypté, ils peuvent tout pomper »[13].

Au terme de nombreuses années de répression, la protection de leur intégrité physique et numérique est devenue une exigence vitale pour toutes les personnes poursuivies et persécutées pour des raisons politiques en Russie – y compris au moment de basculer vers un départ forcé.

L'exil, la dispersion, le rôle des réseaux numériques depuis l'étranger

Le nombre de citoyens russes en exil augmente constamment au cours de l'année 2022, pour atteindre, selon certaines évaluations, un million de personnes en décembre[14]. Ce nombre de départs est sans précédent pour la Russie post-

12 Entretien avec un journaliste indépendant à Tbilissi, mai 2022.

13 Entretien avec un journaliste exilé en Lituanie, Vilnius, novembre 2021.

14 https://en.wikipedia.org/wiki/Russian_emigration_following_the_2022_invasion_of_Ukraine (consulté le 18 février 2023).

soviétique même s'il est incomparable avec les huit millions d'Ukrainiens ayant dû fuir la guerre dans leur pays. C'est à partir de la répression du mouvement protestataire de 2011-2012 que l'exil politique s'enclenche, selon une temporalité qui s'accélère au fil du renforcement de l'autoritarisme. Le départ des premiers militants politiques et journalistes s'effectue vers les États baltes, l'Allemagne et Israël. Ces premiers départs tracent les routes qui seront diversement empruntées par les exilés suivants.

À partir de février 2022, l'ampleur de l'exil conduit à la diversification des destinations. Une cartographie sommaire permet d'identifier les principaux lieux de refuge (Riga, Vilnius, Tbilissi, Berlin, Tel Aviv, Erevan, Istanbul) qui s'ajoutent aux bases arrières historiques de l'opposition russe (y compris par exemple à Londres avec les équipes de Mikhail Khodorkovsky, à Prague avec *Radio Free Europe*, à Berlin avec la communauté hacker et artistique, etc.). À travers les différentes trajectoires, des destinations privilégiées se dessinent – d'abord pour des questions de régime d'entrée, de résidence et d'obtention de visa simplifiés pour les Russes bien sûr, mais l'exil n'est pas nécessairement le résultat d'une trajectoire programmée, le premier point de chute n'est pas forcément la destination visée, elle peut aussi varier en fonction du profil des acteurs (journalistes, militants, avocats, spécialistes d'Internet appelés *ITichniki,* etc). Les professionnels les plus médiatisés de l'espace public parviennent pour la plupart à obtenir des visas dans les pays de l'Union européenne alors que les autres exilés restent «coincés» dans des pays moins sûrs car toujours dans la sphère d'influence russe ou non-protégés par l'adhésion à l'OTAN. Se dessine également ce que certains exilés appellent une différence de traitement entre l'émigration dite «politique» (pour laquelle il existe des catégories administratives) par opposition à celle qualifiée de «morale»[15].

Les États baltes, avant-postes de l'exil politique

S'agissant des journalistes, la cartographie des médias en exil permet d'identifier des lieux privilégiés d'installation des rédactions qui produisent de l'information à l'intention des publics russophones, en Russie (malgré les blocages des principaux sites) et à l'étranger. Si certains journalistes trouvent refuge en Europe occidentale, la plupart d'entre eux privilégient les pays frontaliers de la Russie, par souci de russophonie, de proximité avec leurs sources et avec leurs lecteurs. Les États baltes (Lettonie et Lituanie) et la Géorgie sont devenus des lieux d'accueil privilégiés. Les rédactions les plus connues, bénéficiant d'une forte notoriété internationale et bien insérées dans les réseaux médiatiques transnationaux, se sont longtemps installées en priorité à Riga. En Géorgie, ce sont les journalistes indépendants,

15 Observation et discussion avec les bénévoles russes des associations d'aide aux réfugiés ukrainiens situées à Tbilissi, septembre 2022.

free lance, souvent issus des médias régionaux qui trouvent un asile provisoire. Une distinction sociale et professionnelle se dessine, en fonction de la notoriété et des ressources de la rédaction d'origine.

L'exil des journalistes russes débute en 2014, suite à l'annexion de la Crimée et à l'adoption de la loi Lougovoï sur le blocage des sites web. Les journalistes les plus exposés, comme l'équipe du média *Grani.ru*, choisissent le départ et s'installent en Europe occidentale, y bénéficiant notamment de l'aide de l'association Reporters sans frontières. Suite au démantèlement du média d'information générale *Lenta.ru*, sa rédactrice en chef, Galina Timchenko, transfère son équipe en Lettonie où elle fonde le site *Meduza.io*. Le gouvernement letton facilite son installation et *Meduza* reconstitue un média en ligne de référence, grâce à son équipe de rédacteurs à Riga et à ses correspondants en Russie.

À partir de 2020 et 2021, le nombre de journalistes russes réfugiés à Riga augmente progressivement, suite aux multiples menaces pesant sur les rédactions. Des journalistes des médias d'investigation *The Insider*, *Proekt* ou *Istories* rejoignent les États baltes. Les autorités lettones favorisent la délivrance de visas humanitaires (visas D) pour créer un «hub» des journalistes russes en exil dans leur capitale. À partir de février 2022, les équipes des médias les plus connus sur la scène internationale, comme celles de la télévision *Dojd* mais aussi du service russe de la BBC, de *Novaïa Gazeta*, de *Radio Svoboda* et celles de certains médias régionaux (*Lyudi Baykala*, *Pskovskaya Gubernia*) s'installent en Lettonie. Ils y bénéficient du soutien matériel et logistique de leur employeur (la BBC a ainsi affrété un bus pour transférer ses journalistes de Moscou à Riga en mars 2022). En décembre 2022, d'après les témoignages disponibles, près de 200 journalistes russes seraient installés en Lettonie. Ils y reconstituent leurs rédactions, dans des lieux mis à disposition par les institutions lettones.

À partir de 2020 également, de nombreux militants russes s'installent à Vilnius, suite à la répression du mouvement d'A. Navalny. Ses partisans y trouvent refuge, avec l'appui des autorités locales. Ils y côtoient les militants du Mouvement de la Russie libre, soutenus par Garry Kasparov, qui y organise chaque année depuis 2014 un forum de l'opposition. Certains journalistes russes ont également choisi de s'installer à Vilnius dès 2014. Une école de journalisme à destination des journalistes russes de province y a ouvert ses portes en 2018. Créée par une ancienne journaliste, elle offre des formations qui sensibilisent les journalistes aux questions de sécurité. Son «école des médias» propose ainsi un module de formation à la sécurité numérique, en partenariat avec l'association française Nothing to Hide. L'objectif de la formation est aussi de créer des réseaux d'information et d'entraide entre journalistes. Avant

la guerre, elle projetait enfin de proposer aux journalistes en état de *burn-out* des « retraites » dans des lieux protégés, avec l'aide de psychologues spécialisés[16].

Tous ces acteurs russes croisent en Lituanie les milliers d'exilés biélorusses qui, suite à la violente répression des manifestations contre les opposants au régime d'A. Loukachenko, à l'été 2020, s'installent à Vilnius, à quelques dizaines de kilomètres de la frontière biélorusse. Ils y constituent une communauté en exil soudée par la présence sur place de S. Tsikhanouskaia, la « présidente » en exil des opposants biélorusses. Pour ces exilés politiques, les États baltes constituent une destination privilégiée à plusieurs titres. En termes géographiques, la proximité des frontières russes et biélorusses limite leur éloignement, voire leur permet d'effectuer de brefs séjours pour visiter leurs proches. L'environnement linguistique local, marqué par la présence d'une forte minorité russophone, facilite leur insertion. Enfin, l'appartenance des États baltes à l'Union européenne et à l'OTAN semble leur apporter des garanties de sécurité. À la croisée de l'ancien espace soviétique et de l'Union européenne, ils font figure d'avant-poste pour les exilés qui y développent aussi des actions de solidarité.

Leur présence croissante suscite cependant des tensions. Le 6 décembre 2022, le Conseil national pour les médias électroniques (NEPLP) de Lettonie retire à la télévision *Dojd* sa licence l'autorisant à émettre sur le câble dans le pays. Cette sanction fait suite aux propos controversés d'un journaliste de la chaîne, Alekseï Korostelev, ayant évoqué en direct la volonté de son média d'« aider les soldats russes envoyés sur le front ». Cette déclaration, comprise comme un soutien à l'armée d'agression russe en Ukraine, suscite immédiatement la réprobation des autorités lettones. Le NEPLP accuse la télévision *Dojd* de « menace à la sécurité nationale et à l'ordre public » et rappelle ses récriminations : utilisation du terme « notre armée » pour évoquer l'armée russe, publication d'une carte de la Russie incluant la Crimée, ambiguïté des propos d'Alekseï Korostelev, interview de *Dojd* avec le maire de Riga jugée trop critique. La sanction du NEPLP est perçue par les journalistes russes comme « le miroir » des sanctions exercées contre les médias par le pouvoir russe. Ils en sont profondément ébranlés : « Nous sommes devenus des ennemis ici et là-bas », s'alarme une journaliste, inscrite en Russie au registre des « agents de l'étranger », arrivée en Lettonie au printemps avec ses enfants. La controverse témoigne de la double exigence qui pèse sur les exilés politiques, pris en tension entre le lien avec leur communauté d'origine et leur insertion dans la société d'accueil. À l'issue de ce conflit, la télévision *Dojd* obtient une licence de diffusion aux Pays-Bas, annonçant sa relocalisation à Amsterdam.

16 Entretien avec une journaliste russe en exil, Vilnius, novembre 2021.

La dispersion des trajectoires après la guerre contre l'Ukraine

Outre les pays baltes, les trajectoires d'exil se diversifient après la guerre. Les acteurs alternatifs ou autonomes, dont l'émigration n'est pas prise en charge par leur employeur et qui ne disposent souvent pas d'un réseau préalable, s'adaptent aux opportunités disponibles. Les uns se dirigent vers les pays d'Asie centrale, les autres vers ceux du Caucase, les troisièmes partent vers la Turquie ou parviennent à gagner l'Union européenne. Dans la précipitation, le départ est souvent guidé par l'achat d'un billet dans l'urgence ou l'accessibilité d'un pays qui ne demande pas de visa.

En Géorgie, de nombreux journalistes arrivent à Tbilissi grâce aux facilités administratives qui leur permettent de s'installer dans le pays sans visa pour des séjours longs. Nombre d'entre eux sont de jeunes journalistes, issus des rédactions de médias russes locaux (de Kazan ou Rostov par exemple) ou exerçant en free lance pour divers médias indépendants. Depuis Tbilissi, ils poursuivent leurs activités à distance, dans une précarité liée à l'absence de contrat salarié avec une rédaction et dans l'incertitude de leur situation dans ce pays. Si la Géorgie est un pays plus indépendant vis-à-vis de la Russie que plusieurs autres États de l'espace postsoviétique, le parti au pouvoir est constamment soupçonné par les acteurs de la société civile d'être accommodant avec Moscou par peur de tendre les relations avec la Russie. La Géorgie a ainsi interdit l'entrée de son territoire à des personnalités médiatiques comme Mikhail Fichman, journaliste politique de *Dojd*, et Mitia Alechkovski, militant et journaliste ayant créé le réseau d'entraide des exilés russes OK Russians (qui s'appelle désormais NODA).

La Géorgie se distingue de plusieurs autres destinations des exilés russes par la vivacité des projets qui s'y déploient. Certains journalistes s'engagent dans les petits médias alternatifs qui se constituent face à la guerre, comme le média en ligne féministe *Verstka* ou le projet *Kholod*, d'autres encore créent des médias locaux, racontant la vie de la diaspora russe en Géorgie et parlant de la Géorgie aux exilés russes, comme *Paper Kartuli* fondé par d'anciens journalistes du média saint-pétersbourgeois *Boumaga*. Dans le domaine de l'aide aux réfugiés ukrainiens, depuis le mois de mars 2022, non moins de cinq associations d'accompagnement des Ukrainiens ont été créées par des ressortissants russes, exilés après le début de la guerre en 2022 ou résidant en Géorgie depuis plus longtemps. Les exilés politiques de longue date offrent parfois leur aide aux nouveaux arrivants, leur proposant un hébergement ou des conseils dans l'urgence pour s'orienter dans la migration. Dans d'autres cas, les nouveaux arrivants, surtout ceux qui ont attendu le début de la mobilisation en Russie pour s'exiler, suscitent des soupçons et critiques de la part de ceux partis immédiatement après le début de l'invasion. Les trajectoires des exilés sont très fluides et mouvantes, le premier pays d'accueil

constituant souvent une étape vers une autre destination. Des journalistes et militants passent ainsi par la Géorgie ou le Kirghizstan avant de rejoindre Riga, Prague, voire Berlin ou Paris. Dans ce vaste mouvement d'exode, l'incertitude sur la localisation des uns et des autres est manifeste, la présence numérique palliant souvent l'indétermination de la localisation physique.

Retrouver son intégrité physique et numérique

L'exil constitue une expérience de précarisation à la fois personnelle et professionnelle, individuelle et familiale, morale et administrative. Face à l'incertitude, la légalisation du statut (l'obtention d'une autorisation de séjour), la recomposition d'un foyer (l'obtention d'un logement), la scolarisation des enfants et l'accès à des ressources financières (l'ouverture d'un compte bancaire) constituent des priorités pour les personnes exilées. Se pose aussi la question de la restauration de leur intégrité numérique.

La grande disparité des trajectoires d'exil, qui se différencient notamment à partir de février 2022, s'accompagne d'un usage intense des ressources en ligne. Ces dernières permettent, d'une part, de conserver le lien entre les personnes dans l'éloignement et, de l'autre, de maintenir une présence dans l'espace public. Dès les premiers départs massifs, des outils de coordination surgissent pour faciliter la communication. Sur Signal ou sur Telegram, des chaînes et des tchats sont créés pour faire circuler l'information et coordonner l'entraide à l'échelle de chaque pays d'exil et à l'échelle internationale. Un exemple important est l'initiative *Kovcheg*[17], qui a mis en place un système de tchats locaux par pays, pour l'échange de savoir-faire et la mutualisation des expériences.

Par ailleurs, l'exil prend également la forme de nouvelles barrières socio-techniques : dans le contexte de la loi sur le « RuNet souverain », de nombreux services importants russes deviennent inaccessibles depuis des adresses IP étrangères (comme Gosuslugi, le site des services publics russes, ou des applications bancaires). Des VPNs dont les serveurs sont localisés en Russie ont été mis en place par des bénévoles (gratuitement) ou par des startups (payant) pour permettre de restaurer les liens numériques avec le pays d'origine. En plus de ces outils numériques, un phénomène qualifié de « VPNs humains » s'est également développé, notamment afin de contourner les blocages de virements bancaires internationaux (avec parfois des schémas très complexes incluant plusieurs intermédiaires humains et technologiques), ou encore via le système d'entraide des « occasions » (*okaziya*) pour se faire livrer des documents, des médicaments ou autres objets de valeur entre la Russie et les pays d'exil.

17 https://kovcheg.live/ (consulté le 18 février 2023).

Une fois à l'abri à l'étranger, les exilés peuvent s'extraire des contraintes imposées par l'appareil oppressif russe et retrouver une intégrité en ligne. Ce processus n'est cependant ni évident, ni uniforme. Certaines personnes, enregistrées comme « agent de l'étranger », se défont des contraintes de ce statut, cessant d'ajouter sur leurs publications l'avertissement infamant imposé par la loi, de déclarer leurs revenus au ministère de la Justice russe, ou de conserver les factures de toutes leurs dépenses quotidiennes. La militante Daria Apakhontchitch, en exil à l'étranger, transforme son rapport au ministère en manifeste anti-guerre qu'elle publie en ligne pour dénoncer les violences du conflit. D'autres, à l'inverse, continuent à se plier aux contraintes de la loi. Le départ ne met pas fin aux injonctions de la législation russe qui pèsent sur eux. De nombreux activistes enregistrés comme « agents de l'étranger » continuent à respecter les obligations liées à ce statut pour permettre leur retour en Russie en cas de nécessité absolue (visite d'un proche malade, par exemple). Des poursuites peuvent aussi être engagées contre des militants se trouvant déjà à l'étranger. À titre d'exemple, M. Klimarev, directeur de la Société de défense d'Internet (OZI), proche du mouvement d'A. Navalny, est inscrit sur la liste des personnes recherchées par le ministère de l'Intérieur russe en novembre 2022 alors qu'il se trouve depuis longtemps hors du pays. À l'étranger, l'inquiétude demeure parmi les exilés, qui craignent la surveillance et les provocations des membres des services spéciaux envoyés par Moscou, notamment dans les pays de l'espace post-soviétique où les Russes peuvent circuler sans visa[18].

Nouvelles mobilisations numériques en exil : comment agir en temps de guerre ?

Depuis l'étranger, les militants, journalistes et citoyens exilés accèdent à un espace numérique non-censuré et aux informations sur les violences militaires et les crimes commis en Ukraine par la Russie. Cette brutalité extrême produit un vaste élan réflexif, à la fois individuel et collectif, qui pose la question des héritages historiques, des responsabilités politiques et des réparations morales à l'égard de l'Ukraine. Dans cette dynamique, le monde numérique participe de ses réflexivités nouvelles en posant le problème de la diffusion des contenus contre la guerre dans la société russe, d'un côté, et de la mobilisation des citoyens exilés, de l'autre.

Les militants pour les libertés numériques sont au cœur de ces deux dynamiques comme le montre l'initiative « Internet sans frontières » portée par les principales associations de promotion de l'Internet libre (OZI, Teplitsa, Roskomsvoboda, eQualit.ie). Elles organisent une série de conférences et de hackathons au printemps 2022 dans les principales villes d'accueil des « exilés » (Tbilissi, Erevan,

18 Entretien avec des journalistes en exil en Géorgie, mai 2022.

Vilnius, Varsovie, Berlin, Paris, Haifa) à destination des *ITichniki*, se démarquant des autres événements par leur caractère technique et appliqué. Durant ces rencontres, elles promeuvent l'usage des outils de contournement de la censure pour permettre la circulation des contenus vers les publics demeurés en Russie. Opposées aux sanctions internationales dans le domaine numérique, elles insistent sur la nécessité de maintenir les liens pour lutter contre la propagande du pouvoir en Russie. Elles mobilisent aussi leurs pairs en émigration pour imaginer de nouvelles initiatives contre la guerre et constituer des solidarités en exil. Ces dynamiques techniques font surgir des questions politiques. Si les uns incriminent la nature du régime russe et attribuent la guerre à l'autoritarisme poutinien, d'autres évoquent plus largement la dimension impériale de l'État russe et développent des arguments décoloniaux pour penser sa défaite, en cohérence avec les positions des citoyens ukrainiens qui se battent pour la défense de leur pays.

Informer contre la guerre

L'accès aux publics restés en Russie est une préoccupation majeure des militants et journalistes en exil qui insistent sur la lutte contre la propagande d'État à l'intérieur du pays. Dès le début de la guerre, en février 2022, ils s'inquiètent des sanctions occidentales qui conduiraient à une déconnexion de l'Internet russe des réseaux numériques internationaux. Pour les militants des associations de défense des libertés numériques comme Roskomsvoboda, OZI ou Teplitsa, le maintien des infrastructures techniques est la condition pour continuer à toucher le public russe critique. Dès mars 2022, Roskomsvoboda publie une déclaration contre les sanctions des compagnies internationales dans le domaine numérique, craignant qu'elles touchent avant tout les simples utilisateurs, qui ont un besoin vital d'une information pluraliste[19]. Des militantes, commes celles du Mouvement féministe anti-guerre (FAS), relaient également cette position :

> « Je passe 24h/24, 7 jours sur 7, à coordonner le mouvement féministe contre la guerre en Russie et en exil. Nous apportons notre aide et soutien logistique, technique et organisationnel. En cas de danger, nous faisons sortir des militantes du pays. Aujourd'hui, notre mission est de sortir les mecs de Russie : les femmes sortent les mecs de Russie – on aura tout vu ! – pour qu'ils n'aillent pas tuer des Ukrainien.nes. Je ne vois pas pourquoi il faut nous empêcher de faire tout ça en rendant plus difficile l'accès à Internet sans lequel nous ne pouvons rien. »[20]

19 https://roskomsvoboda.org/uploads/documents/statement_of_roskomsvoboda_team.pdf (consulté le 17 février 2023).

20 Entretien avec une militante du Mouvement féministe anti-guerre, septembre 2022, Tbilissi.

Au printemps 2022, les conférences « Internet sans frontières » consistent à promouvoir les outils de contournement de la censure en ligne, pour conserver le lien avec les publics restés en Russie. D'après les militants associatifs, 10 à 20 millions d'utilisateurs russes recourent régulièrement à des VPN (*virtual private networks*) pour accéder à des contenus bloqués en Russie. Leur objectif est de faire augmenter significativement ce nombre. La question de la circulation des contenus est déterminante pour les journalistes en exil qui produisent des informations destinées à sensibiliser leurs concitoyens aux ravages de la guerre, cherchant à documenter les crimes commis en Ukraine et à alerter l'opinion publique russe sur les violences criminelles des forces armées. Leur présence à l'étranger leur permet de reprendre leur liberté de parole et d'employer les termes interdits en Russie (notamment le mot « guerre »). Alors qu'ils sont bloqués en Russie, ces médias lancent des campagnes de promotion des outils de contournement des blocages pour faire circuler leurs contenus. Ils élaborent des guides en collaboration avec les associations russes de défense des libertés numériques, contribuant à leur niveau à l'*encapacitation* de leurs lecteurs et participant à la dissémination de savoirs numériques alternatifs. Après avoir été bloqués en Russie, les sites *Meduza*, *Mediazona*, *OVD-info* et *Kholod* invitent leurs lecteurs à les suivre sur différents supports (chaîne Telegram, sites miroirs, liste de diffusion par mail). Certains médias créent leur propre application à télécharger sur les appareils mobiles. Ils conseillent surtout à leurs lecteurs d'utiliser des VPN pour déjouer les blocages en Russie, en les orientant vers les solutions les plus fiables disponibles sur le marché [Bronnikova & Daucé, 2022].

Si les opportunités techniques offertes par les outils numériques leur permettent d'agir à distance, dans le prolongement des savoirs acquis durant la pandémie, les questions de sécurité en ligne demeurent centrales dans les communications avec les personnes restées en Russie. Les journalistes en exil sont préoccupés par la sécurité de leurs sources, afin de continuer à couvrir l'actualité russe. Des dispositifs de sécurisation de leurs communications numériques sont mis en place (recours à des réseaux sociaux sécurisés, chiffrement des données…) pour échanger avec leurs informateurs sur place. Depuis l'étranger, ce rapport aux sources est difficile. Comme l'explique une journaliste de la BBC, productrice vidéo, relocalisée à Riga :

> « Mon travail dépend beaucoup de la possibilité de filmer en Russie. Et cette possibilité s'est fortement dégradée, il est devenu très difficile de travailler. (…) Les gens ne veulent pas parler à distance par liaison vidéo, ils voudraient nous rencontrer en personne. (…) Les gens ont peur qu'on soit des espions mais il arrive parfois qu'ils parlent quand ils ont besoin de nous »[21].

21 Entretien avec une journaliste réfugiée à Riga, 4 décembre 2022.

Pour pallier la difficulté de l'accès aux sources, les médias en exil travaillent avec des journalistes indépendants (*free lance*) ou des connaissances sur place, qui prennent des risques sur le terrain mais ne sont pas sous la responsabilité de la rédaction qui les fait travailler.

Mobiliser sans frontières

Tant pour les militants que pour les journalistes, l'établissement de nouveaux liens avec les personnes dispersées par l'exil est un enjeu majeur pour promouvoir un agenda politique contre le régime russe et contre la guerre. Depuis les pays baltes, le Caucase ou l'Europe de l'Ouest, de nombreuses initiatives numériques s'inventent pour mettre en réseau les citoyens éloignés par la guerre. Des rencontres physiques sont organisées dans les principales villes d'exil, qui s'accompagnent de conférences en ligne pour rassembler les relocalisés. Les rencontres « Internet sans frontières » permettent par exemple de mettre en réseau les exilés dans leurs nouveaux lieux de résidence et entre leurs différents pays d'accueil. La déclaration de ses organisateurs rappelle que « La conférence 'Internet sans frontières' […] porte des ambitions techniques et sociales au service de la diaspora locale, majoritairement russophone. Nous militons pour un accès libre à Internet comme moyen de lutte contre la propagande politique, pour que les citoyens disposent d'informations pluralistes »[22].

Les rencontres s'accompagnent de hackathons, destinés à résoudre des tâches techniques collectivement. À Paris, en novembre 2022, les développeurs sont invités à promouvoir le browser CENO (censorship.no), qui utilise le protocole BitTorrent pour accéder aux informations bloquées, auprès des utilisateurs non spécialistes du numérique. Ils sont aussi sollicités pour populariser AmneziaVPN, un service gratuit de création de VPN personnel multiprotocole sur son propre serveur. À l'occasion de ces ateliers, des liens locaux se tissent entre les développeurs en exil pour recomposer un tissu social propice à l'échange de savoir-faire mais aussi de projets politiques. Les rencontres, qui se déroulent en russe, parviennent à rassembler une centaine de personnes dans chaque ville organisatrice.

Les réseaux des militants des libertés numériques croisent ceux des militants politiques et des défenseurs des droits humains qui organisent des manifestations ou publient des pétitions contre la politique de l'État russe. Lors de la conférence « Internet sans frontières » à Paris, co-organisée par l'équipe ResisTIC, le défenseur des droits de l'homme Lev Ponomarev est présent aux côtés de représentants de l'association Russie-Libertés, de membres de l'organisation Memorial en exil ou

22 https://Internetborders.net/statement-on-war/ (consulté le 21 janvier 2023).

d'un journaliste de la télévision *Dojd* installé à Paris. Dans le public, de jeunes militants, artistes et étudiants originaires de Russie montrent un commun intérêt pour les usages militants du numérique et leurs enjeux dans le contexte de la guerre.

Lutter contre l'autoritarisme politique ou contre la domination coloniale ?

Les militants de l'Internet libre ont longtemps cru aux espoirs démocratiques d'Internet, dénonçant l'autoritarisme croissant du régime politique russe. Avec la guerre, une controverse émerge dans le monde des exilés venus de Russie : faut-il dénoncer l'autoritarisme du pouvoir russe fauteur de guerre ou bien l'impérialisme de la société dans son ensemble ? À la lumière de cette controverse, est-ce que la défense d'un agenda démocratique est suffisante sans critique fondamentale du colonialisme russe ? Les trajectoires des opposants en exil divergent considérablement en fonction de leur vision politique de l'avenir de la Russie. Les initiatives contre la guerre s'accompagnent de prises de positions publiques qui peuvent susciter des tensions. Voulant renouer avec le projet démocratique et libéral, de nombreux « forums pour la Russie libre » proposent des projets de restauration économique ou de réhabilitation de la réputation du pays (avec des initiatives telles que le drapeau blanc-bleu-blanc qui expurge symboliquement la couleur rouge associée au sang). Leurs positions font cependant l'objet de critiques pour l'absence de perspective décolonialiste et de remise en cause du projet même de « Fédération de Russie ».

Les militants ukrainiens, qui luttent pour la survie de leur pays, estiment certes que « La guerre n'est pas une guerre entre deux États mais entre deux systèmes : l'autoritarisme et la démocratie », mais ils dénoncent plus généralement l'oppression coloniale portée par Moscou. Dans son discours de réception du prix Nobel de la paix en décembre 2022, l'avocate et activiste ukrainienne pour les droits humains Oleksandra Matviichuk affirme : « Le peuple russe sera responsable de cette page abjecte de son histoire et de cette tentative de restaurer son ancien empire par la force. (…) C'est pour cette raison que la détermination du peuple ukrainien à résister à l'impérialisme russe est si importante »[23]. Une perspective qui peut être qualifiée de décoloniale et de déconstruction de la Russie gagne en popularité parmi les citoyens ukrainiens mais aussi parmi certains exilés ayant quitté la Russie. Elle est notamment défendue par les organisateurs de l'initiative « Internet sans frontières » qui, dans une déclaration,

23 La traduction en français de ce discours a été publiée par le journal *Le Monde* :

https://www.lemonde.fr/international/article/2022/12/10/discours-du-prix-nobel-de-la-paix-la-guerre-en-ukraine-n-est-pas-une-guerre-entre-deux-etats-mais-entre-deux-systemes-l-autoritarisme-et-la-democratie_6153845_3210.html (consulté le 17 février 2023).

affirment qu'ils « partagent l'interprétation de cette guerre comme impériale et la résistance de l'Ukraine comme décoloniale. Les organisateurs reconnaissent le poids de siècles de relations difficiles entre la Russie et l'Ukraine, que la propagande soviétique et russe a tenté de faire passer pour de la fraternité ou de l'amitié. Les mots "nations fraternelles", tant dans ce contexte que dans le contexte politique, sont interprétés par les organisateurs comme des instruments de colonisation de l'Ukraine et ils ne les partagent pas »[24]. Des projets de média « décoloniaux » et régionalistes, comme *Beda Media*[25], Free Buryatia Foundation[26], Free Yakutia Foundation[27], etc., se développent pour informer les lecteurs russophones sur la question coloniale.

L'exil permet aux opposants russes, nouvellement installés dans les États indépendants voisins de la Russie, d'observer et de vivre des cultures différentes, en mettant en perspective leurs propres cultures politiques, linguistiques, économiques. Cette expérience est source d'auto-critique et de remise en question de ce que signifie être « russe » ainsi que du projet de la « Fédération de Russie » – notamment, en s'informant de plus en plus sur le passé colonial russe. Cette perspective critique change les trajectoires individuelles des militants russes en exil. Certains mettent désormais l'accent sur les problèmes locaux, apprennent la langue locale, essaient de rejoindre les initiatives des pays d'accueil et font un travail de fond sur le vocabulaire qu'ils utilisent au quotidien sur le Net, notamment, en insistant sur le passé colonial russe et en déconstruisant le narratif de la « grande Russie » et de ses « peuples-frères ». Parmi les exemples de ces processus – des militants russes exilés en Arménie s'impliquent dans la campagne pour soutenir la ville d'Artsakh bloquée par l'Azerbaïdjan, dans le projet de « La Maison sous le Toit Rouge » à Bishkek (Kyrgyzstan), un centre culturel ouvert par des citoyens de Russie avec la participation active des communautés locales.

Les positions démocratiques et décoloniales, qui circulent sur le « Runet en exil », ne sont pas nécessairement consensuelles et conduisent à des débats, des controverses[28], voire parfois à des ruptures de coopérations. Cependant, leur existence même témoigne de l'émergence d'un espace public russophone pluraliste hors frontières, échappant aux exigences patriotiques et réactionnaires

24 https://Internetborders.net/statement-on-war/ (consulté le 21 janvier 2023).

25 https://www.beda.media/ (consulté le 17 février 2023).

26 https://instagram.com/freeburyatiafoundation? igshid=YmMyMTA2M2Y= (consulté le 17 février 2023).

27 https://instagram.com/freeyakutiafoundation? igshid=YmMyMTA2M2Y= (consulté le 17 février 2023).

28 Voir l'éditorial « Russkie, zatknites' » (Russes, taisez-vous), *Grani.ru*, 22 juillet 2022, https://graniru.org/opinion/editorial/m.285545.html (consulté le 17 février 2023).

du régulateur russe. Elle laisse entrevoir ce que pourrait être un monde numérique libéré des contraintes autoritaires, capable de porter, pour la Russie, d'autres projets que la guerre mortifère engagée contre l'Ukraine. Ces voix alternatives restent cependant faibles et dispersées. En Russie même, la critique est devenue inaudible. Depuis vingt ans, la trajectoire de l'autoritarisme numérique s'est construite par petites touches oppressives, en réponse à la libre inventivité des utilisateurs du Runet. Une multitude d'acteurs, humains et non-humains, ont été enrôlés dans le vaste maillage répressif construit aux multiples échelles d'Internet. Si des espaces limités de liberté en ligne demeuraient possibles jusqu'en février 2022, l'agression militaire de grande ampleur contre l'Ukraine est venue lever les derniers tabous autoritaires, justifiant désormais la censure, la surveillance et les contrôles numériques par la défense de l'intérêt national contre des forces étrangères hostiles. Cet autoritarisme belliqueux et impérial embrasse les nouvelles opportunités techniques, détournant à son profit les promesses d'Internet pour diffuser la propagande d'État auprès des citoyens connectés, pour mobiliser sa société en ligne et pour déstabiliser les pays adverses. La Russie offre ainsi un funeste exemple d'autoritarisme augmenté. À la fois banal dans sa matérialité ordinaire et tragique par le projet politique qu'il porte, il constitue un cas heuristique pour penser et prévenir les dérives autocratiques des sociétés contemporaines que le numérique peut venir renforcer et asseoir.

Références bibliographiques

[Anceschi, 2015] Anceschi, Luca, « The persistence of media control under consolidated authoritarianism: containing Kazakhstan's digital media », *Demokratizatsiya* vol. 23, p. 277-295.

[Bronnikova & Daucé, 2022] Bronnikova, Olga, & Daucé, Françoise, « Un manuel de survie numérique pour s'informer et éviter la censure en Russie », *The Conversation*, 2 mai 2022 (https://theconversation.com/un-manuel-de-survie-numerique-pour-sinformer-et-eviter-la-censure-en-russie-181889).

[Bublatzky, 2022] Bublatzky, Cathrine, « Mobile belonging in digital exile: methodological reflection on doing ethnography on (social) media practices », *Media and Communication* vol. 10, n° 3, p. 236-246.

[Daucé et al, 2020] Daucé, Françoise, Loveluck, Benjamin, Ostromooukhova, Bella & Zaytseva, Anna, « From citizen investigators to cyber patrols: volunteer Internet regulation in Russia », *Laboratorium: Russian Review of Social Research* vol. 11, n° 3, p. 46-70.

[Diminescu, 2005] Diminescu, Dana, « Le migrant connecté : pour un manifeste épistémologique », *Migrations/Société* vol. 17, n° 102, p. 275-292.

[Earl et al, 2022] Earl, Jennifer, Maher, Thomas V., & Pan, Jennifer, « The digital repression of social movements, protest, and activism: a synthetic review », *Science Advances* vol. 8, n° 10.

[Ermoshina, 2023] Ermoshina, Ksenia, « Voices from the island: informational annexation of Crimea and transformations of journalistic practices », *Journalism*, online first

[Favarel-Garrigues, 2018] Favarel-Garrigues, Gilles, « Justiciers amateurs et croisades morales en Russie contemporaine », *Revue française de science politique* vol. 68, n° 4, p. 651-668.

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

[Gillespie et al, 2018] Gillespie, Marie, Osseiran, Souad, & Cheesman, Margie, « Syrian refugees and the digital passage to Europe: smartphone infrastructures and affordances » *Social Media + Society* vol. 4, n° 1.

[Michaelsen, 2020] Michaelsen, Marcus, « Silencing Across Borders: Transnational repression and digital threats against exiled dissidents from Egypt, Syria and Iran », rapport pour la fondation Hivos (Humanist Organisation for Social Change), https://hivos.org/assets/2020/02/SILENCING-ACROSS-BORDERS-Marcus-Michaelsen-Hivos-Report.pdf

[Human Rights Watch, 2021] Human Rights Watch, *Azerbaijan* (2021), https://hrw.org/europe/central-asia/azerbaijan

[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.

[Latonero, 2015] Latonero, Mark, « For refugees, a digital passage to Europe », *Thomson Reuters Foundation News*, 27 décembre 2015 (https://news.trust.org/item/20151227124555-blem7/).

[Le Huérou, 2022] Le Huérou, Anne, « Les paradoxes du recours au droit dans les mobilisations contre les violences policières en Russie », *Champ pénal/Penal field*, vol. 26.

[McCarthy et al, 1991] McCarthy, John D., Britt, David W., & Wolfson, Mark, « The Institutional channeling of social movements by the state in the United States », *Research in Social Movements, Conflicts and Change* vol. 13, n° 2, p.45-76.

[Moss, 2016] Moss, Dana M., « Transnational repression, diaspora mobilization, and the case of the Arab Spring », *Social Problems* vol. 63, n° 4, p. 480-498

[Pan & Siegel, 2020] Pan, Jennifer, & Siegel, Alexandra A., 2020, « How Saudi crackdowns fail to silence online dissent », *American Political Science Review* vol. 114, n° 1, p. 109-125.

[Porlezza & Arafat, 2022] Porlezza, Colin, & Arafat, Rana, « Promoting newsafety from the exile: the emergence of new journalistic roles in diaspora journalists' networks », *Journalism Practice* vol. 16, n° 9, p. 1867-1889.

[Rochel, 202] Rochel, Johan, « Connecting the dots: Digital integrity as a human right », *Human Rights Law Review* vol. 21, n° 2, p. 358-383.

Présentation des auteurs

Olga Bronnikova est maîtresse de conférences à l'Université Grenoble Alpes, et membre de l'ILCEA4 (CESC). Depuis son doctorat, qui portait sur la mobilisation politique des migrants en France et au Royaume-Uni, elle travaille sur les migrations russes post-soviétiques. En tant que membre du projet ANR RESISTIC, elle a pu étudier l'exil des professionnels russes et biélorusses de l'espace public en Union européenne.

Françoise Daucé est directrice d'étude à l'EHESS et directrice du Centre d'études russes, caucasiennes, est-européennes et centrasiatiques (CERCEC). Ses travaux en sociologie politique de la Russie contemporaine portent sur les nouvelles formes de censure et d'emprise sur le monde médiatique à l'heure d'Internet. Elle a coordonné le projet ANR ResisTIC de 2018 à 2022.

Ksenia Ermoshina est chargée de recherche au Centre Internet et Société, CNRS, chercheuse associée au Citizen Lab. Ses recherches portent sur les infrastructures et pratiques de contrôle de l'information, notamment, en zones de guerre et dans les pays à risque. Elle est également impliquée dans le développement des outils de chiffrement (messagerie Delta Chat) et de contournement de censure (navigateur Ceno). En 2022, elle a publié avec Francesca Musiani l'ouvrage *Concealing for Freedom* (Mattering Press).

Valéry Kossov est maître de conférences HDR en études russes à l'Université Grenoble Alpes, directeur du Centre d'études slaves contemporaines au sein du laboratoire ILCEA4. Ses derniers travaux de recherche abordent la problématique de la production et de l'application des lois relatives au domaine numérique et portent sur les pratiques et techniques juridiques des avocats spécialisés dans la défense des droits numériques en Russie contemporaine.

Benjamin Loveluck est maître de conférences en sociologie à Télécom Paris dans le département Sciences Économiques et Sociales, équipe de l'Institut Interdisciplinaire de l'Innovation (i3) et chercheur associé au Centre d'études et de recherches en sciences administratives et politiques (CERSA, CNRS-Paris 2). Ses travaux portent sur les pratiques politiques en ligne, les libertés numériques et la régulation d'Internet.

Francesca Musiani est chargée de recherche HDR au CNRS, co-fondatrice et directrice adjointe du Centre Internet et Société (CIS), chercheuse associée à MINES Paris-PSL et à l'Internet Governance Lab de l'American University.

Ses recherches portent sur les infrastructures et les architectures techniques d'Internet comme outils de gouvernance. En 2022, elle a publié avec Ksenia Ermoshina l'ouvrage *Concealing for Freedom* (Mattering Press).

Bella Ostromooukhova est maîtresse de conférences à Lettres Sorbonne Université (UMR Eur'Orbem). Sociologue de la culture, elle travaille sur l'édition indépendante en Russie post-soviétique, et plus particulièrement sur les mécanismes de censure et les pratiques de contournement de celle-ci déployées par les acteurs de la littérature jeunesse.

Perrine Poupin est chargée de recherche au CNRS, au Centre de recherche sur l'espace sonore et l'environnement urbain (CRESSON-AAU). Elle travaille sur des conflits socio-environnementaux en Russie et a publié ces dernières années de nombreux articles sur une mobilisation d'habitants contre un projet national d'une immense décharge à Shies, dans la région d'Arkhangelsk, au nord de la Russie (2018-2020).

Anna Zaytseva est maîtresse de conférences à l'Université Toulouse Jean Jaurès (laboratoire LLA-Creatis). Elle travaille sur les scènes musicales alternatives, l'entrepreneuriat culturel, la transformation des industries créatives à l'ère du numérique. Ses récentes publications portent sur les formations en sécurité numérique liées au secteur associatif russe. Elle est également traductrice d'ouvrages en sciences sociales et de bandes dessinées.

Table des matières

Suite des titres de la collection

Alaric Bourgoin,
Les Équilibristes. Une ethnographie du conseil en management

Catherine Rémy et Laurent Denizeau (dir.),
La Vie, mode mineur

Florian Charvolin, Stéphane Frioux,
Méa Kamour, François Mélard
et Isabelle Roussel,
Un air familier? Sociohistoire des pollutions atmosphériques

Francesca Musiani,
Nains sans géants.
Architecture décentralisée et service Internet

Michel Callon *et al.*,
Sociologie des agencements marchands. Textes choisis

Emmanuel Kessous et Alexandre Mallard (dir.),
La Fabrique de la vente.

Jérôme Michalon,
Panser avec les animaux.

Jérôme Denis et David Pontille,
Petite sociologie de la signalétique.

Madeleine Akrich, Michel Callon
et Bruno Latour,
Sociologie de la traduction. Textes fondateurs

Nathalie Darène,
Fabriquer le luxe. Le travail des sous-traitants

Liliana Doganova,
Valoriser la science. Les partenariats des start-up technologiques

Geneviève Teil, Sandrine Barrey, Antoine Hennion
et Pierre Floux,
Le Vin et l'environnement. Faire compter la différence

Dominique Boullier, Stéphane Chevrier
et Stéphane Juguet,
Événements et sécurité.

Jérôme Bourdon,
Histoire de la télévision sous de Gaulle

Cyril Lemieux,
Un président élu par les médias?

Fabien Granjon et Julie Denouël (dir.),
Communiquer à l'ère numérique.

Anne-France de Saint Laurent-Kogan
et Jean-Louis Metzger (dir.),
Où va le travail à l'ère du numérique?

Alexandre Mallard,
Petit dans le marché.

Madeleine Akrich, Yannick Barthe,
Fabian Muniesa et Philippe Mustar (dir.),
Débordements. Mélanges offerts à Michel Callon

Madeleine Akrich, Yannick Barthe
et Catherine Rémy (dir.),
Sur la piste environnementale.

Cyril Lemieux,
La Sociologie sur le vif

Annemarie Mol,
Ce que soigner veut dire.
Repenser le libre choix du patient

Madeleine Akrich, Cécile Méadel
et Vololona Rabeharisoa,
Se mobiliser pour la santé.

Alain Desrosières,
Pour une sociologie de la quantification.
L'Argument statistique I

Alain Desrosières,
Gouverner par les nombres. L'Argument statistique II

Michel Armatte,
La Science économique comme ingénierie.
Quantification et modélisation

Antoine Savoye et Fabien Cardoni (dir.),
Frédéric Le Play. Parcours, audience, héritage

Frédéric Audren et Antoine Savoye (dir.),
Frédéric Le Play et ses élèves.
Naissance de l'ingénieur social

Fabien Granjon,
Reconnaissance et usages d'internet.

Bruno Latour,
Chroniques d'un amateur de sciences

Marcel Calvez, avec Sarah Leduc,
Des environnements à risques. Se mobiliser contre le cancer

Vololona Rabeharisoa et Michel Callon,
Le Pouvoir des malades.

Sophie Dubuisson et Antoine Hennion,
Le Design : l'objet dans l'usage.

Françoise Massit-Folléa, Cécile Méadel et Laurence
Monnoyer-Smith (eds.),
Normative Experience in Internet Politics

Madeleine Akrich, João Nunes, Florence Paterson
& Vololona Rabeharisoa (eds.),
The Dynamics of Patient Organizations in Europe

Maggie Mort, Christine Milligan, Celia Roberts
& Ingunn Moser (eds.),
Ageing, Technology and Home Care

Dans le sillage de la fin de l'URSS, l'Internet russe s'est d'abord développé librement, laissant l'initiative à de nombreux acteurs inventant des outils numériques ajustés à leurs usages. Cependant, depuis le début des années 2010, le tournant autoritaire au sommet de l'État russe a entraîné le déploiement d'un maillage d'emprises et de contraintes qui s'est resserré tant sur les acteurs que sur les infrastructures numériques du pays.

Alors que le réseau a longtemps porté les espoirs de démocratisation de la sphère publique russe, son encadrement s'est constitué progressivement, au fil de controverses et d'épreuves. Malgré les critiques et les contournements militants et citoyens, l'oppression numérique a participé de la souverainisation politique et de la dynamique belliciste dont le moment culminant a été l'invasion de l'Ukraine en février 2022.

Le livre, nourri par les enquêtes de terrain réalisées dans le cadre du projet ANR ResisTIC, dessine un panorama de la gouvernance coercitive et des usages numériques émancipateurs en Russie, de la paix à la guerre. Il met l'accent sur les multiples acteurs et objets numériques au cœur des controverses politiques et des tensions d'usage dans l'espace numérique russe dans les années 2010. 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. Au prisme du cas russe, ce sont les reconfigurations numériques contemporaines, de la surveillance à la souveraineté, que ce livre interroge.

9 782356 719720

29 euros