# Chapitre 2. Surveillance et censure des infrastructures Internet en Russie : marchés, régulation et boîtes noires

Ksenia Ermoshina, Benjamin Loveluck, Francesca Musiani


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

**Genèse d'un autoritarisme numérique**

Presses des Mines

# Chapitre 2. Surveillance et censure des infrastructures Internet en Russie : marchés, régulation et boîtes noires

**Ksenia Ermoshina, Benjamin Loveluck et Francesca Musiani**

DOI : 10.4000/books.pressesmines.9073
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

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).

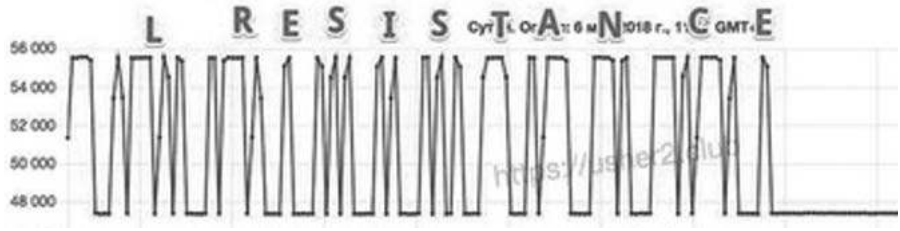


Figure 1. Le message en code Morse de L. Evdokimov.
Source : site de Phil Kouline, hébergeur indépendant, expert et militant pour le RuNet libre (https://usher2.club/articles/msg-digitalresistance/)[15].

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.

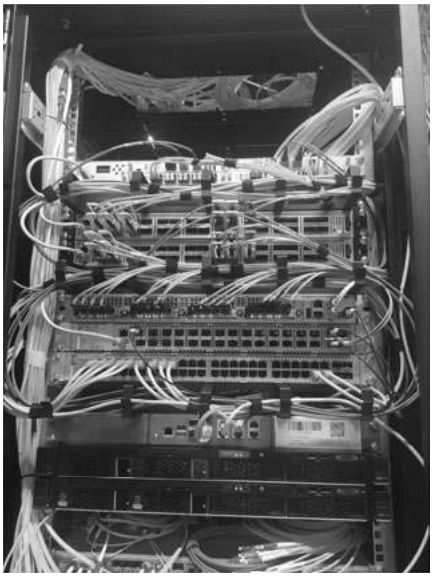

Figure 2. Installation TSPU pour 40Gb/sec.
Source : OrderCom

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.

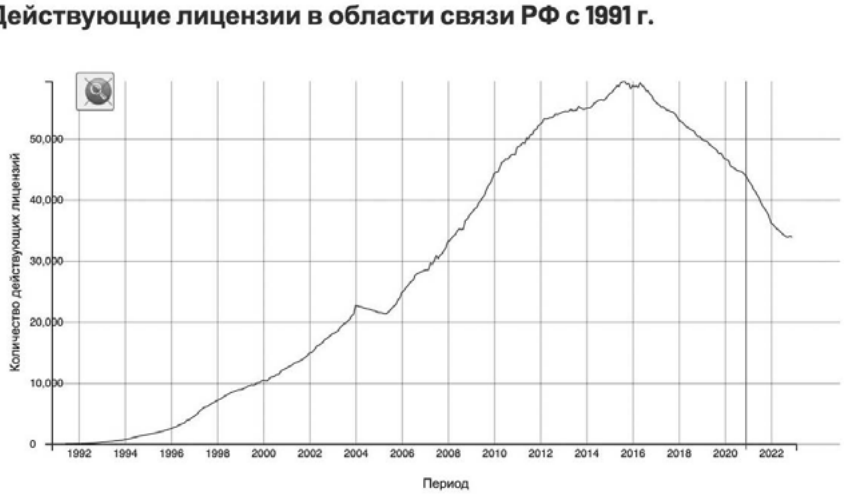


Figure 3. Licences actives délivrées dans le domaine des télécommunications.
Source: https://ifreedomlab.net/connectivity-rating/licenses-russia/

## 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.