

La « souveraineté numérique », nouveau vecteur de l'influence russe en Afrique francophone ?

Kevin Limonier | 1 février 2024



Le deuxième sommet Russie-Afrique qui s'est tenu à Saint-Petersbourg en juillet 2023 a été pour la Russie l'occasion de diversifier ses vecteurs de coopération avec les pays africains, dans un contexte marqué par la guerre en Ukraine ainsi que par les contrecoups du putsch raté de feu Evgueni Prigojine en juin 2023. Affichant un bilan contrasté, ce sommet, qui a réuni des représentants de 49 pays dont 17 chefs d'État, n'en a pas moins permis à la Russie de sceller 120 accords. Parmi les très nombreux documents officiels produits pour l'occasion, une [déclaration](#) a été adoptée qui traite spécifiquement de la « sécurité informationnelle ». Dans ce document, la Russie et les représentants des États africains représentés au sommet insistent sur l'importance de développer une coopération dans le secteur des technologies de l'information, en soulignant la nécessité de respecter la « souveraineté numérique » des parties prenantes. Dans son dernier point, le document appelle même à développer des cycles de rencontres régionales entre la Russie et ses partenaires africains dans l'objectif de déboucher sur des « avancées pratiques » ayant trait aux technologies de l'information et de la « souveraineté numérique ».

Peu remarquée, cette déclaration est pourtant remarquable en cela qu'elle est totalement nouvelle. Jusqu'ici, les sommets Russie-Afrique n'avaient pas particulièrement abordé les questions numériques, et encore moins sous l'angle très politisé de la « [souveraineté numérique](#) ». Dans sa première édition en 2019, le sommet Russie-Afrique avait plutôt été pensé pour promouvoir l'émergence de nouveaux réseaux d'intérêts russo-africains sur fond de promotion d'un récit idéologique anti-impérialiste où la Russie se présente comme une puissance anticoloniale, dans la droite ligne de la mythologie soviétique. Si les nouvelles technologies informationnelles sont depuis longtemps au cœur de la stratégie de déploiement de ces réseaux, on constate désormais côté russe une volonté d'aller plus loin, notamment en exportant sur le continent les normes, représentations, pratiques et technologies qui caractérisent l'Internet souverain tel que l'imaginent et le construisent les autorités russes depuis le début des années 2010.

L'objectif de cet article est de montrer comment ce nouvel axe de coopération esquisse des stratégies d'influence russes inédites sur le continent africain. D'abord, en affichant une volonté de faire émerger une nouvelle convergence idéologique pour

proposer à certains gouvernements africains un récit sur la « souveraineté numérique », articulé aux discours anti-impérialistes et panafricanistes tels qu'encouragés depuis plusieurs années par [Moscou](#). Ensuite, en témoignant de la volonté de la Russie de diversifier sa présence sur le continent, en misant notamment sur ses entreprises du secteur numérique et en brisant le monopole exercé au sein du pouvoir russe par certaines structures sur les dossiers africains. *In fine*, cet article se place essentiellement du point de vue des acteurs russes, de leurs discours, et de leurs pratiques. Il n'a pas vocation à analyser leur réception par les autorités et sociétés africaines (dont l'auteur n'est pas spécialiste), mais plutôt à comprendre comment la Russie cherche à exporter la « souveraineté numérique » comme dispositif géopolitique, économique et technique auprès d'États incarnant ce « Sud global » [que Moscou cherche à construire](#) sur fond de guerre en Ukraine et de confrontation avec « l'Occident », autre terme cher aux communicants du Kremlin.

Vers une nouvelle convergence idéologique et narrative

L'émergence d'un discours sur la souveraineté numérique dans le cadre des sommets Russie-Afrique est le produit d'une stratégie qui est née lors du « [Forum international Russie-Afrique sur les technologies de l'information](#) », organisé à Moscou en avril 2023. Présenté comme une rencontre préliminaire au 2^e sommet Russie-Afrique, cet événement affichait l'objectif de réunir des experts russes et africains afin de discuter « des projets actuels et des tendances clés de la transformation numérique, ainsi que des perspectives de coopération russo-africaine dans le domaine des technologies de l'information et de la communication ».

Peu couvert par les médias russes, et africains, ce forum est pourtant un événement clé puisqu'il a été le premier où la diplomatie russe a clairement mis en avant des éléments de langage attestant d'une volonté de faire converger ces deux *success stories* narratives que sont d'une part les récits sur la dimension anticoloniale de la Russie en Afrique, et d'autre part son attachement à la « souveraineté numérique ».

Ainsi, les quelques articles parus dans la presse russe qui font la promotion du forum d'avril 2023 utilisent presque tous l'angle de la « souveraineté numérique » comme futur vecteur de coopération Afrique-Russie. [Dans un long article paru dans le média spécialisé IKS](#), le journaliste Nikolai Nossov explique que le forum est l'occasion pour la Russie d'exporter son modèle de « souveraineté numérique » sur un continent qui reste largement tributaire de plateformes et de solutions techniques occidentales ou chinoises. Même son de cloche [dans les colonnes du journal Mezhdunarodnaya Zhizn' du ministère russe des Affaires étrangères](#), où le « modèle » russe de compétence numérique est mis en avant pour présenter le forum d'avril 2023 et le sommet Afrique-Russie de juillet 2023.

La « souveraineté numérique » russe, un récit géopolitique doublé d'un dispositif technique et économique

Or, le thème de la « souveraineté numérique » est tout sauf anodin lorsqu'il est employé dans le contexte [russe](#). En effet, il constitue en Russie un véritable récit géopolitique, c'est-à-dire un ensemble de discours qui, une fois combinés, produisent une grille de lecture cohérente des rivalités et rapports de force qui se produisent sur un espace précis, en l'occurrence ici le cyberspace. Au fil du temps, ce récit va s'imposer comme une véritable grille de lecture qui oriente progressivement les choix stratégiques de l'État et des entreprises russes du numérique, jusqu'à former un véritable dispositif technique et économique. C'est ce dispositif, structuré autour du développement de nouvelles technologies de censure au nom de la « souveraineté numérique », que certains acteurs russes entendent commercialiser sur le continent africain.

Le récit géopolitique de la « souveraineté numérique » russe commence à se développer dans les années 2000, dans sillage des prises de position diplomatiques de Moscou sur la question du respect de la souveraineté des États comme norme ultime de la vie internationale. A cette époque, le recours au droit d'ingérence humanitaire par la coalition occidentale pour légitimer son intervention militaire en Serbie (République fédérale de Yougoslavie, 1999) puis l'indépendance du Kosovo (2008) est vivement dénoncé par la Russie, qui y voit une entrave au respect de la souveraineté des États et une instrumentalisation du droit international humanitaire. La notion russe de « souveraineté numérique » se développe alors dans le sillage de ces expériences post-yougoslaves, en dénonçant l'hégémonie des structures et des « valeurs » occidentales sur la gouvernance de l'Internet et son fonctionnement. A partir de 2012, un nouveau palier est franchi avec la réélection de Vladimir Poutine pour un troisième mandat. Tout juste réélu, le président inaugure un tournant conservateur visant à réaffirmer la Russie comme protectrice d'un certain nombre de « valeurs morales », tandis qu'Internet est de plus en plus perçu comme une menace à son projet politique mais aussi à la stabilité du régime. Le rôle des réseaux sociaux dans la genèse et la coordination des « Printemps Arabes » en 2010-2011 avait alors marqué les esprits, sur fond de vives manifestations contre le retour au pouvoir de Vladimir Poutine en 2012, qui furent largement organisées sur des plateformes en ligne auxquelles les services de renseignement russe n'avaient pas accès. Quelques mois plus tard, en juin 2013, Edward Snowden révélait au monde un gigantesque programme de surveillance du réseau, initié par la NSA. Ce coup de tonnerre fit grandement les affaires de la Russie qui, en plus d'accorder l'asile politique au

lanceur d'alerte, put à loisir dénoncer l'hégémonie américaine et accuser Internet d'être un vecteur d'influence et de déstabilisation au profit des occidentaux.

Entre dénonciation de l'hégémon américain, défense des valeurs morales et impératifs de sécurité nationale, Internet devint alors en Russie l'objet d'une triple convergence conduisant à une intense production législative que la guerre en Ukraine a accélérée. De nombreuses lois sont en effet venues matérialiser une véritable stratégie d'appropriation du cyberspace russe par le pouvoir, comme celle qui [depuis 2017](#) contraint les messageries chiffrées à partager leurs clés de chiffrement avec les autorités. Ce volontarisme politique fut grandement facilité par le fait que la Russie dispose de son propre écosystème national de plateformes d'intermédiation (réseaux sociaux, moteurs de recherche, etc.), fondées et installées dans le [pays](#). En effet, la Russie est l'un des seuls pays au monde à disposer de son propre écosystème de plateformes nationales, qui ont longtemps été plébiscitées en lieu et places des GAFAs occidentaux. Ces plateformes se nomment Yandex, VK, Mail.ru, et se sont développées à une époque où le Runet, le segment russophone du Net, était encore à la marge de l'Internet mondial, notamment en raison de la mauvaise qualité des bandes passantes fournies par les câbles de télécommunication est-ouest hérités de la Guerre froide. Tombées sous le contrôle d'actifs proches du pouvoir russe [au cours des années 2010](#), ces plateformes sont progressivement devenues les instruments grâce auxquels le récit géopolitique de la « souveraineté numérique » a pu se concrétiser. Ainsi, en 2016, [une série d'amendements à la loi sur les télécommunications](#) a obligé ces plateformes à aménager des portes dérobées pour les services de sécurité fédéraux, ou encore de les contraindre à stocker jusqu'à 3 ans de métadonnées de leurs utilisateurs.

De récit géopolitique, la « souveraineté numérique » est rapidement devenue une doctrine opératoire s'appuyant sur un écosystème de plateformes progressivement « mises au pas » durant la décennie 2010, lorsque plusieurs d'entre elles sont passées sous le contrôle d'actionnaires proches du pouvoir. C'est également devenu un dispositif technique, dans la mesure où l'État russe cherche désormais non seulement à réguler les informations qui circulent sur les plateformes, mais également à contrôler les flux numériques entrants et sortants de la Fédération de Russie. C'est tout l'objectif de [la loi sur le « Runet souverain »](#), qui pose en 2019 les bases d'un système de censure à l'échelle du pays, avec comme ambition ultime de doter l'État des capacités techniques nécessaires à l'organisation de sa déconnexion vis-à-vis du reste du monde en cas de « menace extérieure ». Cette législation prévoit, entre autres, d'installer des boîtiers de censure du trafic aux endroits clés du réseau russe, avec comme ambition de déployer un système de contrôle centralisé des « frontières numériques » de la Fédération. Autrement dit, la loi de 2019 inaugure une série de dispositifs techniques qui concrétisent le récit géopolitique élaboré par les autorités près d'une décennie auparavant. C'est ce dispositif, ainsi que les discours, représentations et récits qu'il sous-tend, que la Russie entend désormais promouvoir en Afrique.

L'Afrique, un continent traditionnellement hors du périmètre de l'Internet souverain russe

Traditionnellement, le discours russe sur la « souveraineté numérique » s'adresse plutôt à trois types d'audience ayant peu de liens avec l'Afrique : l'audience intérieure (protéger la Russie des influences occidentales en prenant le contrôle du réseau et des contenus qui y circulent), les compétiteurs stratégiques de la Russie en ce qui concerne la régulation du cyberspace (gouvernance de l'Internet, etc), et enfin les États alliés, généralement situés dans l'« étranger proche », auprès de qui la Russie promeut et commercialise des technologies de contrôle et des modèles de gouvernance issus de la mise en application des lois de 2016 et de 2019 sur le « Runet souverain ». En effet, le récit géopolitique sur la « souveraineté numérique » tel que promu par les autorités repose sur un petit écosystème d'entreprises russes financées principalement par de l'argent public pour développer les outils effectifs de la censure numérique. Il s'agit de groupes comme [IKS Holding](#), qui réunissent plusieurs entreprises exploitant aujourd'hui les technologies et matériels servant au filtrage du trafic Internet en Russie. Parmi ces matériels, on trouve les fameux TSPU (acronyme russe désignant les « [Appareils de lutte contre les menaces](#) »), qui se présentent sous la forme de boîtiers DPI (*Deep Packet Inspection*) et sont censés centraliser de nombreuses mesures de contrôle. Ces matériels et les technologies qu'ils embarquent font aujourd'hui l'objet de projet d'exportations, notamment en Asie centrale, en Iran et en [Afghanistan](#).

Ces stratégies sont généralement mises en œuvre par des cercles diplomatiques ou technocratiques haut placés. Pour ce qui est du discours sur la souveraineté et la gouvernance d'Internet, il s'agit par exemple de diplomates souvent issus des affaires stratégiques du ministère des Affaires étrangères, qui s'intéressent d'abord aux grands partenaires ou compétiteurs stratégiques de la Fédération. De ce fait, le continent africain y est rarement associé puisque la production de discours géopolitiques sur l'Afrique est plutôt laissée soit à des diplomates de terrain (ayant des trajectoires de carrière moins significatives), soit à des acteurs extérieurs à l'administration russe. Il s'agit notamment des médias à vocation internationale (RT et Sputnik) et des entrepreneurs d'influence (Prigozhine, Malofeev, etc) dont le modèle économique dans la région est fondé sur la capacité à faire fructifier des capitaux en accompagnant le retour géopolitique de la [Russie](#). Ce sont ces acteurs extérieurs qui ont promu, au

moins depuis 2016, une série de discours et de personnalités œuvrant pour la « libération de l'Afrique » de l'influence des anciennes colonies, au premier rang desquelles la France. Ces efforts ont grandement contribué à l'émergence d'un mouvement « néo-panafricaniste » qui entend œuvrer à cette « libération » du continent, sur fond de théories du complot et de fantasme sur le rôle de la Russie comme héritière de l'anticolonialisme soviétique.

La « colonisation numérique de l'Afrique » comme vecteur de promotion du dispositif russe de souveraineté numérique

Or, c'est précisément sur la thématique de la lutte contre l'impérialisme occidental que se fait la jonction entre les discours sur la « souveraineté numérique » et ceux qui sont traditionnellement promus par les relais de l'influence russe sur le continent africain. Cette thématique est un véritable « liant narratif » que l'on retrouve en creux des quelques publications qui ont été consacrées au forum international Russie-Afrique sur les technologies de l'information par les médias russes francophones et leurs relais. C'est notamment le cas d'un [article](#) de Sputnik Afrique écrit pour l'occasion, qui explique sommairement que « l'Afrique aspire au partage de l'expertise russe dans le domaine de la digitalisation afin d'en tirer profit ». Dans un [podcast](#) publié sur Sputnik Afrique, Wack Ndiaye, coordinateur technique de l'Agence De l'Informatique de l'État (ADIE) du Sénégal, abonde dans ce sens en expliquant comment la Russie pourrait accompagner l'Afrique dans le processus de construction de sa « souveraineté numérique ». Dans ces publications, le ton reste relativement neutre et technique, ne faisant que sous-entendre la thématique de l'hégémonie occidentale. Le site algérien [lemaghreb.dz](#), relais classique des narratifs russes, est quant à lui beaucoup plus direct, puisqu'il parle directement de « colonisation numérique » pour qualifier la présence des plateformes occidentales sur le [continent](#), et se fonde sur les articles publiés par Sputnik et cités ci-dessus pour construire son argumentation. Il s'agit là d'un [procédé classique](#) de l'influence russe en Afrique : les médias officiels russes créent des contenus au ton relativement neutre et technique qui apportent des éléments confortant certains logiciens idéologiques. Ces contenus sont ensuite repris par des sites ou des influenceurs partageant ledit logiciel, et qui se chargent de les inclure dans des récits beaucoup plus engagés.

Par ailleurs, ce nouveau récit de promotion d'une souveraineté numérique africaine soutenue par la Russie porte en lui les germes de stratégies plus offensives, notamment à l'égard des opérateurs et plateformes occidentales présents dans la région – au premier rang desquelles les entreprises françaises comme Orange. Présent dans de nombreux secteurs de l'économie ouest-africaine, le groupe français pourrait très bien se retrouver la cible de campagnes antifrancaises sur fond de dénonciation de la perpétuation d'un « néocolonialisme numérique » auquel la Russie pourrait apporter des solutions grâce aux entreprises de l'écosystème du Runet souverain. Ce risque est d'autant plus prégnant que plusieurs pays d'Afrique de l'Ouest, où l'entreprise est très implantée, peuvent voir leurs gouvernements adopter des réflexes autoritaires en termes de contrôle du réseau – à l'instar du blocage de nombreux réseaux sociaux au Sénégal en marge des manifestations contre la condamnation d'Ousmane Sonko.

Plus largement, le discours sur la « souveraineté numérique » africaine tel que produit par la Russie pourrait encourager les influenceurs néo-panafricanistes à faire du contrôle d'Internet un enjeu « civilisationnel », dans le sillage de ce que les autorités russes ont pu faire pour le Runet au début des années 2010. À l'époque, Vladimir Poutine avait qualifié Internet « d'invention de la CIA » et de vecteur de corruption morale – une posture dans la droite ligne des doctrines ultraconservatrices du Kremlin sur les questions sociétales, elles-mêmes centrales dans le dispositif d'autopromotion de la Russie comme « puissance conservatrice ». Ce récit réactionnaire, particulièrement apprécié des extrêmes droites européennes, a servi de prétexte aux premières tentatives de régulation des contenus sur le Runet, et a constitué l'un des fondements de la doctrine de « souveraineté numérique ». Aujourd'hui, on voit en Afrique des influenceurs comme Nathalie Yamb fustiger la « [promotion de l'homosexualité](#) » à laquelle se livreraient selon elle certains gouvernements ouest-africains. De tels discours créent *de facto* les prémices d'une convergence russo-africaine sur les questions sociétales, dont l'aboutissement logique serait, à l'image de ce qui s'est passé en Russie, la moralisation d'Internet comme arme de censure et, *in fine*, la promotion d'une « souveraineté numérique » anti-occidentale, illibérale et réactionnaire.

Perspectives et limites à la promotion de la souveraineté numérique à la russe en Afrique

La convergence des discours sur la « souveraineté numérique » russe d'une part, et sur l'anti-impérialisme occidental en Afrique d'autre part, n'en sont qu'à leurs balbutiements. Pourtant, le phénomène mérite d'être considéré, car il pourrait dessiner des opportunités tant économiques que politiques pour la Russie. En effet, l'Afrique constitue un potentiel marché pour de nombreuses grandes entreprises russes du secteur numérique, désormais confrontées à la fermeture ou à la restriction de nombreux marchés occidentaux suite aux sanctions. Si certaines entreprises du secteur parviennent à maintenir leur activité grâce à l'implantation de filiales en Israël, en Turquie ou ailleurs, beaucoup ont dû se résigner à quitter les marchés américains ou européens. De fait, l'Afrique constitue pour elles un horizon de prospection de ressources d'autant plus crédible qu'on

remarque déjà quelques *success stories* russes sur le continent, comme celle du service de taxi et de livraison à domicile Yango. Filiale du géant russe Yandex et détenue à 10% par l'américain Uber, Yango a métamorphosé la pratique des mobilités dans ce pays d'Afrique de l'Ouest. En Côte d'Ivoire, où Yango est devenu hégémonique, les anciens taxis sauvages ont presque disparu des rues d'Abidjan, remplacés par de petites voitures japonaises rouges, couleur de la charte graphique de Yandex. Devenu indispensable pour de nombreux trajets du quotidien de l'importante classe moyenne abidjanaise, Yango s'est étoffé d'un service de livraison à domicile relativement efficace et très prisé dans cette métropole où convergent de nombreux flux économiques de la sous-région. L'interface de Yango est quant à elle calquée sur celle de Yandex Taxi (disponible en Russie et dans de nombreux pays de l'ex-URSS), et ne fait pas mystère de ses origines russes.

Cette *success story* d'un service VTC russe en Afrique de l'Ouest est donc un message d'espoir pour de nombreux entrepreneurs russes en quête de nouveaux horizons. Or, c'est aussi et surtout un signe d'encouragement pour les autorités, qui entretiennent avec Yandex des liens ambigus et complexes. En effet, Yandex, souvent présenté comme le « google russe », est un acteur incontournable du Runet, utilisé quotidiennement par des dizaines de millions de clients en Russie, en Afrique et ailleurs. A ce titre, il est l'objet d'une attention toute particulière de la part du FSB qui, en vertu des lois de surveillance numérique de 2016, a théoriquement accès à 6 mois d'activités des utilisateurs de [Yandex](#) (ce qui avait à l'époque demandé le développement de technologies spécifiques de stockage). Or, on sait que depuis le 1^{er} septembre 2023, Yandex et sa filiale Yango sont également tenus [de partager avec les services de renseignement](#) russe les données relatives aux courses de taxi effectuées via leurs services. Cette information est à rapprocher de l'étonnante fonctionnalité de l'application Yango en Côte d'Ivoire qui consiste à enregistrer les conversations tenues dans l'habitacle du taxi le temps de la course pour « l'amélioration du service » – chose dont le client est prévenu en pénétrant dans la voiture qu'il a commandée (la fonctionnalité, qui n'est pas enclenchée par défaut, se retrouve néanmoins dans de nombreux VTC abidjanais).

A travers l'exemple de Yandex en Côte d'Ivoire, on voit donc se dessiner un puissant dispositif de contrôle numérique, qui découle en partie des lois adoptées par la Fédération de Russie dès 2016 au nom de la « souveraineté numérique » et des technologies de collecte de données que les entreprises ont dû mettre en place pour s'y conformer. On voit également se dessiner une autre tendance : celle de l'utilisation des entreprises russes du secteur numérique non seulement comme vecteur d'influence économique, mais aussi possiblement politique et sécuritaire. En effet, l'installation de la guerre en Ukraine dans la longue durée a transformé l'Afrique subsaharienne en une sorte de « deuxième front » par la Russie dans sa guerre contre « [l'Occident global](#) », alors que la mort de Evgueni Prigojine a brisé le monopole symbolique que celui-ci exerçait sur des pans entiers de la politique africaine de la Russie. Or, comme nous l'avons souligné plus haut, la thématique de la souveraineté numérique est aussi un formidable argument marketing pour vendre les technologies de contrôle qui sont aujourd'hui développées en Russie. Par exemple, les gouvernements d'Afrique subsaharienne favorables à la Russie, souvent issus de putsch militaires, constituent autant d'acheteurs potentiels de solutions de censure numérique développées par des entreprises russes, sur fond de promotion du récit géopolitique de la « souveraineté numérique ». Ainsi, il est très probable que les entreprises qui prospectent actuellement en Asie Centrale, Iran et Afghanistan pour vendre des solutions DPI russes soient également en train d'investir le très prometteur marché africain – notamment dans les pays où ont eu lieu des coups d'État militaires. C'est en tous cas ce que suggère un faisceau d'indices concordants à propos de l'entreprise IKS Holding, dont il a été question plus haut : en effet, cette entreprise connue pour ses liens avec les services de sécurité russe, dont on sait qu'elle prospecte actuellement dans plusieurs endroits du monde pour vendre des solutions de censure très sophistiquées, a régulièrement promu l'exportation de la vision russe de la souveraineté numérique sur le continent africain via son journal en ligne IKS Media, dont un contenu a été cité au début de cet article. Plus largement, de nombreuses entreprises russes du secteur s'intéressent désormais de près à l'Afrique comme nouveau marché pour l'exportation de technologies de contrôle, à l'instar de celles qui entretiennent des relations étroites avec les organes de force et [ont participé au forum Afrique-Russie](#) de Saint Pétersbourg à l'été 2023. C'est par exemple le cas de Vympelcom, géant russe du secteur des infrastructures [habitué aux interceptions électroniques](#) pour le compte des services de sécurité fédéraux.

Un écosystème numérique russe désorganisé par la guerre

Est-ce à dire que la Russie a toutes les cartes en main pour réussir à exporter son récit géopolitique sur la « souveraineté numérique », et *in fine* parvenir à y commercialiser son dispositif de contrôle et de censure ? Si de nombreux éléments évoqués dans cet article étayaient cette thèse, d'autres permettent de relativiser – pour l'heure – le risque. D'abord, il convient de rappeler que la guerre en Ukraine a profondément désorganisé les entreprises russes du numérique. Ainsi, nombreux sont les travailleurs du numérique à avoir fui le pays dès le début de la guerre, soit par conviction politique, soit pour échapper à la mobilisation, soit pour contourner certaines sanctions risquant de mettre à mal certains modèles économiques dans le domaine des services digitaux. Plusieurs poids lourds du secteur ont quitté le pays avec fracas, à l'instar d'Elena Bunina, CEO de Yandex, qui a

démisionné et quitté le pays en avril 2022 pour s'installer en Israël – pays où vit aussi depuis 2019 le fondateur et propriétaire du groupe, Arkadi Volozh.

Même si de nombreux travailleurs du numérique semblent être rentrés au pays après plusieurs mois d'installation temporaire dans les capitales des anciennes républiques soviétiques du Caucase ou d'Asie centrale, l'exemple de Bunina et de Volozh montre que certaines grandes plateformes centrales du Runet sont aujourd'hui menacées de dislocation : si Yandex demeure une entreprise russe, la branche israélienne semble prendre de plus en plus d'importance au sein du groupe, notamment en ce qui concerne l'activité cruciale de la R&D. Dans le même temps, de nombreux actifs semblent être déplacés vers sa filiale néerlandaise, dont [certains observateurs](#) pensent qu'elle a vocation à devenir le centre de gravité du groupe. De fait, Yandex, comme d'autres entreprises, organisent l'illisibilité des périmètres de compétence de ses différentes filiales, elles-mêmes éclatées sur plusieurs régimes juridiques, afin probablement d'échapper à certaines obligations imposées en Russie par les services de sécurité en termes d'écoutes, d'interceptions, de contraintes sur des personnels qualifiés potentiellement mobilisables dans l'armée, mais aussi de contournement des sanctions occidentales. Dès lors, la principale limite à cette nouvelle stratégie de promotion de souveraineté numérique en Russie pourrait bien être les entreprises russes elles-mêmes, qui comme une grande partie de la population, imaginent tout un tas de stratagèmes pour rester le plus loin possible des « aventures géopolitiques » organisées depuis le Kremlin. Cela n'empêcherait certes pas la reprise du récit de la « souveraineté numérique » de l'Afrique par tout un écosystème d'influenceurs et de relais qui génèreraient assurément beaucoup de clics grâce à lui. Pour autant, cela en limiterait considérablement la crédibilité, puisque la Russie ne serait pas en capacité de partager l'expertise suffisante en matière de contrôle numérique. À moins qu'une nouvelle industrie d'exportation du modèle russe de censure numérique ne voie le jour pour satisfaire ce nouveau marché, notamment dans le sillage de la Chine. En effet, les dispositifs de contrôle développés par Moscou, de même que le *storytelling* géopolitique qui les accompagnent, sont complémentaires des grands projets d'infrastructures numériques développés par la Chine en Afrique avec lesquels ils ne rentrent que rarement en concurrence. Il pourrait même en résulter à terme un ensemble cohérent de normes et de technologies incarnant les ambitions du « Sud global » dans le cyberspace.

Crédits photo : [Gorodenkoff](#)



Kevin Limonier

Kevin Limonier ([@kevinlimonier](#)) est géographe, maître de conférences à l'Institut français de géopolitique (Université Paris 8), directeur adjoint du centre GEODE et membre de l'Institut Universitaire de France. Il est spécialiste du cyberspace russophone et plus largement de la cartographie géopolitique des réseaux numériques.

Comment citer cette publication

Kevin Limonier, « La « souveraineté numérique », nouveau vecteur de l'influence russe en Afrique francophone ? », *Le Rubicon*, 1 février 2024 [<https://lerubicon.org/la-souverainete-numerique-nouveau-vecteur-de-linfluence-russe-en-afrique-francophone/>].