La place des logiciels libres et *open source* dans les nouvelles politiques du numérique en Russie

Marie-Gabrielle Bertran[1]

En Russie comme dans de nombreux pays, les autorités ont cherché à tirer profit des intérêts économiques liés au numérique bien avant de se préoccuper des risques posés par ces nouvelles technologies. Le mandat de Dmitrij Medvedev en tant que président de la Fédération de Russie (2008-2012) a représenté une période décisive pour la mise en place d'une économie de l'Internet et du numérique, qui avait d'abord pour but d'assurer le rayonnement économique du pays sur un marché international encore largement dominé par les États-Unis. Les années 2010 ont donc constitué un tournant. C'est avant tout une volonté de redynamisation et de projection de la puissance économique de la Russie qui a guidé les politiques publiques en faveur des secteurs de l'informatique et du numérique, partagée par le gouvernement et des acteurs économiques établis ou émergents[2].

Cependant, à la faveur des révélations d'Edward Snowden fin 2013, la question de la *souveraineté numérique* est devenue une problématique majeure pour les autorités. Après la révélation publique de la surveillance massive exercée sur l'Internet mondial par les services de renseignement des *Five Eyes* (États-Unis, Royaume-Uni, Canada, Australie et Nouvelle-Zélande), les autorités russes se sont recentrées sur la prise en compte des enjeux stratégiques et de sécurité liés au numérique. Elles ont ainsi quitté la posture de relatif laisser-faire qu'elles tenaient

Hérodote, n° 177-178, La Découverte, 2e et 3e trimestres 2020.

1. Doctorante en géopolitique, université Paris 8, EA 353, Centre de recherches et d'analyses géopolitiques (CRAG), chercheuse au centre de recherche Géopolitique de la datasphère (GEODE).

2. Entreprises du numérique créées à la fin de la période soviétique, ou start-up créées dans les années 2000, parfois par opportunisme : suivant les contrats publics offerts par l'État.

jusqu'alors vis-à-vis du développement du numérique sur leur territoire pour en faire la clef de voûte d'une nouvelle indépendance et d'une autosuffisance techniques, mais aussi d'une certaine autonomie dans la gestion et le traitement des données produites par les internautes en Russie. Or, dans ce nouveau paysage du numérique russe, les logiciels libres et *open source* occupent une place de choix, comme en attestent les nombreuses mesures prises depuis 2010 qui visent à favoriser leur emploi sur le parc informatique des institutions publiques.

Le Libre et l'*Open Source* sont des modes de développement de logiciels qui s'appuient sur deux principes : celui de la liberté de l'utilisateur, qui doit pouvoir se servir d'un programme informatique sans que des restrictions importantes ne lui soient imposées, et celui de l'accessibilité du code source des programmes, qui doit pouvoir être consulté en ligne par n'importe quel utilisateur (on parle ainsi de « code source ouvert » ou *open source*). Ces modes de développement dépendent à l'origine de deux mouvements nés à la fin des années 1970 et au début des années 1980 : moment où le développement et la programmation informatiques sont sortis des domaines militaire et de la recherche pour entrer dans le domaine économique, à travers la commercialisation des systèmes d'exploitation[3] puis des logiciels[4] [Perens, 1999]. Ces mouvements ont constitué au départ une tentative de résistance à la commercialisation des programmes informatiques, avant de devenir des courants alternatifs et dissidents dans un secteur du développement numérique devenu largement commercial, en s'inscrivant contre l'idée de son contrôle par des entités privées à but lucratif ou des institutions d'État.

L'emploi de tels modes de production en Russie pour la création de logiciels destinés non seulement à être mis en vente sur le marché, mais encore à être vendus à des institutions étatiques, semble ainsi aller à l'encontre des idées et des principes qui devraient présider à leur développement.

On peut donc se demander comment les thèmes du Libre et de l'*Open Source* ont pu entrer dans le champ des prérogatives et des intérêts de l'État en Russie. L'intérêt accru du gouvernement russe pour les solutions libres et *open source* correspond-il à la mise en place d'un modèle alternatif face à la domination économique et/ou géopolitique des multinationales du numérique, ou des États-Unis ? Ou ne constitue-t-il qu'un mode d'instrumentalisation politique et/ou économique de ces thèmes ?

Nous verrons d'abord comment et à quelles fins les politiques publiques russes ont favorisé l'émergence rapide d'une industrie de production logicielle par le recours aux logiciels libres et *open source*. Nous analyserons ensuite comment, à la faveur

3. Logiciel qui permet de faire fonctionner un ordinateur et de s'en servir.

4. Le matériel informatique (*hardware*) était déjà largement commercialisé dans le domaine industriel depuis les années 1950 [Logé, 1991].

Hérodote, n° 177-178, La Découverte, 2e et 3e trimestres 2020.

des révélations d'Edward Snowden et d'une convergence d'intérêts publics et privés, ces politiques ont pris une dimension sécuritaire et s'inscrivent désormais dans une stratégie assumée de souveraineté numérique. Enfin, nous interrogerons les conséquences de cette convergence d'intérêts, qui se traduit par une externalisation des capacités informatiques publiques, justifiée par le besoin de recourir à des solutions libres et *open source* développées par des acteurs privés : ces logiques permettent-elles réellement d'assurer la sécurité de ces infrastructures, comme le revendiquent les différents acteurs ? Et ne conduisent-elles pas à un détournement des pratiques du Libre et de l'*Open Source* qui pourrait annuler à terme leurs avantages techniques ?

Le développement de logiciels libres et *open source* en Russie : vers une nouvelle industrie russe du numérique

2010, première phase du développement de logiciels libres et open source *en Russie*

Une première stratégie étatique visant à créer une nouvelle industrie du numérique en Russie a émergé autour de 2010, au cours du mandat de Dmitrij Medvedev. Ces efforts se sont notamment incarnés dans la création de la ville technologique de Skolkovo, qui devait devenir le fer de lance de l'industrie des nouvelles technologies en Russie, à l'instar des centres historiques du développement des hautes technologies tels que la ville d'Akademgorodok ou le campus de l'université d'État Lemonosov (MGU). Officiellement lancé le 28 septembre 2010 avec l'inauguration de la Fondation Skolkovo, ce technopôle avait pour objectif l'émergence d'un nouvel écosystème d'entreprises et de start-up innovantes dans le domaine du numérique [Limonier, 2012].

Le projet s'est cependant heurté à des divergences de vues entre ses tenants, qui considéraient que la ville technologique était attractive pour les start-up et nouvelles entreprises du numérique, et ses détracteurs, restés dubitatifs face à un projet monté de toutes pièces par l'État, qui ne bénéficiait pas (ou peu) de l'appui des acteurs et des réseaux historiques du domaine en Russie (universités et centres de recherches en particulier).

Surtout, les débuts de la troisième présidence de Vladimir Poutine en 2012 ont été marqués par un ralentissement, voire une mise en suspens du projet. Les efforts investis pour son développement ont en effet été fortement réduits, puisqu'il ne revêtait pas la même importance pour V. Poutine[5], et qu'il avait fini

5. Il aurait déclaré : « On ne construira pas la ville du soleil dans une enclave », *in* « Medvedev le prisonnier de Poutine », *Le Point*, 7 juillet 2011.

par pâtir des soupçons de corruption à l'encontre des membres de son conseil d'administration[6].

Mais les tentatives de la présidence Medvedev pour redynamiser la création technologique en Russie après la stagnation des années 1990 (dans le domaine du numérique en particulier) ont aussi été marquées par l'adoption d'un décret émanant de l'exécutif, qui visait explicitement à soutenir la création de systèmes d'exploitation russes selon une logique prioritairement économique : afin de stimuler le marché intérieur du logiciel et l'économie du numérique dans le pays.

La mise en place du décret n° 2299-r [Ministère du Développement numérique, des Réseaux et des Communications de masse de la Fédération de Russie, 2010] le 17 octobre 2010 a ainsi signé le lancement officiel d'un plan de transition en vingt-cinq points vers l'emploi de logiciels libres et *open source* à destination du parc informatique des institutions fédérales, dans le but d'encourager la création et la commercialisation de logiciels en Russie.

Convergence des intérêts publics et privés dans le développement du Libre et de l'*Open Source* en Russie : une production logicielle rapide à coût réduit

Le choix de favoriser des logiciels libres et *open source* n'était pas anodin. Le code des systèmes d'exploitation et des applications logicielles de ce type présente la particularité d'être libre d'accès sur l'Internet. Certaines licences libres et *open source* permettent par ailleurs de se resservir gratuitement de ce code et d'y apporter des modifications, c'est-à-dire de l'utiliser comme un ensemble de briques prêtes à l'emploi pour la fabrication de nouvelles applications. Cette possibilité de réutilisation du code constituait donc une réduction non négligeable du temps et des coûts de recherche et développement (R&D), de conception et de production pour les entreprises. Les licences libres et *open source* leur permettaient, qui plus est, de bénéficier de codes sources déjà éprouvés par une communauté de développeurs – qui continue souvent à les mettre à jour et à les corriger –, et dont l'utilité pour les utilisateurs avait déjà été établie. Concrètement, le recours aux logiciels libres et *open source* leur permettait donc de limiter considérablement leurs risques en termes d'investissements, sachant que les financements placés dans des projets non encore éprouvés peuvent s'avérer fatals pour les PME[7] et les

6. Voir l'enquête sur les possibles détournements de fonds du projet diligentée en 2013 par Vladimir Markin, apparemment avec le soutien de Vladimir Poutine : « Poutine met au pas le cabinet Medvedev », *Le Figaro*, 8 mai 2013.

7. Petites et moyennes entreprises.

Hérodote, n° 177-178, La Découverte, 2e et 3e trimestres 2020.

start-up, si les logiciels produits ne trouvent pas leur public. Cette focalisation des autorités fédérales sur le logiciel libre et *open source* devait donc leur permettre de favoriser le développement rapide d'une industrie de production logicielle russe.

Les acteurs privés russes du numérique ont ainsi commencé à jouer un rôle majeur sur le marché intérieur du numérique en Russie pour réduire la dépendance (en particulier celle des institutions publiques) aux logiciels importés depuis l'étranger, dont le prix a longtemps été élevé[8].

Le coût prohibitif des licences étrangères en Russie a en effet fortement encouragé cette politique d'autonomisation. La falsification des licences Microsoft Windows était une pratique particulièrement répandue en Russie dans les années 1990-2000, à tel point qu'elle a failli conduire au rejet de l'adhésion du pays à l'Organisation mondiale du commerce (OMC) au début des années 2000[9]. En 2001, les écoles russes employaient encore majoritairement des versions piratées de Windows, ce qui pouvait constituer un motif de réticence, voire de refus de la part de certains des membres de l'organisation[10].

Pour pouvoir adhérer à l'OMC, les autorités russes ont donc fait le choix de lancer le développement d'un nouveau système d'exploitation destiné à remplacer Windows sur les postes informatiques des institutions publiques (dont les écoles).

Afin d'assurer ce remplacement dans un délai court, et pour une question de coût, ce système d'exploitation devait reposer sur un noyau *open source* de la famille Linux[11]. Le respect de ce cahier des charges a ainsi permis la création de la distribution ALT Linux[12] : l'une des distributions *open source* les plus utilisées en Russie à l'heure actuelle.

Le succès du lancement d'ALT Linux a constitué un précédent. En 2009, le gouvernement russe a décidé de lancer un système d'exploitation *open source* pour

8. Aujourd'hui, les entreprises telles que Microsoft reviennent sur ce modèle, après avoir perçu son inévitable obsolescence face à la gratuité de nombreux systèmes d'exploitation *open source* et/ou libres.

9. Les copies illégales du système d'exploitation Windows et la vente de clés d'activation/clés de licence ont fini par constituer une forme d'économie parallèle avant la mise en place de mesures de protection par Microsoft au début des années 2000 : <https://www.01net.com/actualites/microsoft-protege-ses-logiciels-des-copies-illegales-133773.html>.

10. En particulier de ceux siégeant au sein de l'Organe d'examen des politiques commerciales, du Conseil du commerce des marchandises, du Conseil du commerce des services et du Conseil des aspects des droits de propriété intellectuelle touchant au commerce : <https://www.rferl.org/a/1096319.html>.

11. Système d'exploitation libre. Son développement s'est appuyé sur la structure et le fonctionnement du système UNIX créé en 1969. On compte aujourd'hui plusieurs familles de systèmes d'exploitation développées à partir de ce modèle, dont GNU/Linux, BSD, macOS et iOS.

12. Officiellement lancée en mars 2001.

le domaine de la défense, avec la création d'ASTRA Linux. La conception et le maintien de cette distribution ont été assurés par une entreprise spécialement créée pour l'occasion : RusBITech-ASTRA, une filiale de l'entreprise RusBITech dont les activités sont étroitement liées à des domaines stratégiques pour le gouvernement russe via les solutions qu'elle propose au ministère de la Défense. Depuis 2011, elle fait donc partie des partenaires officiels de la Fondation Linux[13] : statut qui offre une visibilité internationale dans le domaine de l'*open source*.

L'investissement de l'État russe dans le développement logiciel par le biais de la législation a ainsi constitué un choix d'orientation majeur. Il a non seulement incité les différents acteurs russes du développement informatique à investir dans la création de nouveaux logiciels, mais il leur a également ouvert un nouveau marché intérieur : celui de la production de logiciels destinés aux institutions publiques.

D'après Aleksej Smirnov, le directeur général de l'entreprise ALT Linux[14], il a par ailleurs permis d'accroître l'influence des acteurs russes à l'étranger et sur la scène internationale dans le domaine du développement de codes sources ouverts. Ainsi, selon lui, plus le pays investirait le secteur de l'*open source*, plus il aurait de chances de l'influencer[15].

L'entreprise RusBITech est un parfait exemple de la convergence des intérêts publics et privés autour de la production de logiciels *open source*, puisqu'elle a non seulement bénéficié de l'ouverture d'un marché public sur le marché intérieur russe, mais aussi gagné en visibilité sur le marché international du numérique grâce à la création du logiciel ASTRA.

Abandon des logiciels propriétaires étrangers en Russie et ouverture du marché intérieur des logiciels libres et open source *destinés à l'État : une industrie numérique russifiée*

Suite à l'adoption et à la mise en place du décret fédéral n° 2299-r, les autorités russes ont procédé à l'abandon systématique des solutions logicielles conçues par des entreprises domiciliées aux États-Unis qui étaient employées par les autorités publiques. Une solution russe a donc été choisie en remplacement de la solution Cisco qui était auparavant employée comme système de gestion de la

13. <https://www.ukfast.co.uk/linux-news/linux-foundation-adds-seven-new-members.html>.

14. Créatrice et administratrice du système d'exploitation *open source* du même nom.

15. « Gardez à l'esprit que si cet OS [*operating system* : système d'exploitation] sort au format *open source*, plus la Russie investira le mouvement international du logiciel *open source*, plus elle l'influencera. », <http://m.ingenieris.net/content.php?action=extend_article&id=100>.

Hérodote, n° 177-178, La Découverte, 2e et 3e trimestres 2020.

vidéosurveillance de la Ville de Moscou. De la même manière, les services de messagerie Microsoft Exchange Server et Outlook ont tous deux été supprimés des six mille postes informatiques de la Ville de Moscou et remplacés par un logiciel de l'entreprise Rostelecom.

Le gouvernement avait l'intention d'appliquer, à terme, des changements similaires à un ensemble d'environ 600 000 ordinateurs et serveurs sur le territoire. Les services publics russes entendaient ainsi arrêter « l'achat de produits à des entreprises étrangères [dès] lors qu'il exist[ait] des solutions équivalentes développées par des sociétés russes », signe du lien direct entre l'adoption des lois sur l'emploi des logiciels libres et *open source* et la volonté du gouvernement de favoriser l'emploi de logiciels conçus en Russie. Dans les clauses du décret, on apprenait d'ailleurs que cet objectif était encore loin d'être assuré, « les autorités [dépensant à l'époque] environ 300 millions de dollars en acquisition de produits étrangers ».

Afin de favoriser le contrôle et le suivi des logiciels employés par les institutions publiques, la loi fédérale n° 764677-6 du 29 juin 2015 sur « les technologies et la protection de l'information » et sur « le système contractuel dans le domaine de l'attribution des marchés publics de biens et de services » [Douma, 2015] a également imposé la création d'un registre des logiciels domestiques[16].

Depuis son entrée en vigueur le 1er janvier 2016, seules les sociétés dont les solutions appartiennent à ce registre peuvent prendre part à un marché public de fourniture de biens ou de services dans le domaine de l'informatique. L'usage de logiciels étrangers par les autorités fédérales a donc été purement et simplement interdit dans les cas où il existe des alternatives nationales (la loi admet cependant qu'une entité publique emploie des logiciels étrangers en cas de nécessité, s'ils sont *open source*).

Cette loi avait d'ailleurs été pensée par le MinSvjaz′ (ministère des Réseaux et des Communications de masse) comme un véritable « programme de remplacement des produits importés »[17] dans le domaine du numérique, suite à la publication d'une étude dont les résultats s'étaient révélés sans appel : selon cette étude en effet, les systèmes d'exploitation mobiles importés (en particulier Android et iOS) ne trouvaient aucun concurrent de facture russe sur le territoire. Leur pénétration sur le marché russe de la mobilité était donc quasi totale, puisqu'ils représentaient 95 % des systèmes d'exploitation du secteur en Russie. L'importance de ce taux a incité le MinSvjaz′ à proposer un plan pour faire diminuer cette part à 50 % du marché d'ici 2025.

16. « Registre unifié des programmes russes pour les ordinateurs et les bases de données », <https://digital.gov.ru/ru/activity/directions/772/, https://reestr.minsvyaz.ru/reestr/>.

17. « Selon le ministère russe des Télécommunications, la Russie a son propre système d'exploitation mobile », *Sputnik*, 19 mai 2015.

Surtout, le gouvernement russe a lancé en 2015 le développement d'un système d'exploitation destiné à être embarqué sur des plateformes mobiles (portables, tablettes) à partir de la distribution *open source* Sailfish, développée par l'entreprise finlandaise Jolla (fondée par d'anciens employés de Nokia).

Cette priorité mise sur le développement de systèmes d'exploitation russes à partir de 2010, par la volonté conjointe du gouvernement, des institutions publiques et de certains acteurs privés du domaine, a donc eu deux objectifs. S'il s'agissait d'abord – à l'instigation de Dmitrij Medvedev – de redynamiser l'économie du numérique en Russie après les années 1990, le gouvernement russe s'est ensuite réapproprié ces logiques pour réduire l'influence des multinationales étatsuniennes sur son territoire, afin d'assurer, à terme, l'autosuffisance technique du pays.

À la faveur de l'affaire Snowden, cet objectif d'autosuffisance technique a été renforcé par un argument de nature (géo)politique : celui de la nécessité d'assurer la *souveraineté numérique* du pays, garante de la sécurité informatique de ses infrastructures dans un monde de plus en plus connecté.

L'après-Snowden : prise en compte du problème de la sécurité informatique en Russie

Les déclarations de Snowden : à l'origine d'une nouvelle réflexion sur la sécurité informatique en Russie

Bien que les autorités russes aient officiellement fait part de leurs inquiétudes face aux risques liés à l'émergence de virus informatiques de grande ampleur dès la fin des années 1990 [Tchernenko, 2013][18], la question de la sécurité informatique est restée à l'arrière-plan de celle de la sécurité informationnelle dans la première décennie des années 2000 [Morenkova Perrier, 2014]. Il a donc fallu attendre que les révélations d'Edward Snowden replacent la question de la sécurité informatique au cœur des préoccupations de sécurité du gouvernement pour voir émerger de nouveaux plans de développement pour le numérique à l'échelle du pays.

Avec ces révélations publiques en effet, le risque de fuite de données stratégiques de l'État par des biais encore peu envisagés, tels que l'accès aux données

18. Elles ont souligné l'importance de ces risques dès 1998, en proposant la première résolution pour des « Développements dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale » à l'Assemblée générale des Nations unies, afin d'empêcher l'usage des nouvelles technologies et moyens de dissémination de l'information « à des fins criminelles ou terroristes » pouvant porter atteinte à la « sécurité des États » [AG NU, 1999].

Hérodote, n° 177-178, La Découverte, 2e et 3e trimestres 2020.

personnelles de citoyens russes sur les réseaux sociaux[19], s'est retrouvé au premier plan.

Cette problématique a fini par devenir cruciale aux yeux des autorités, qui ont rapidement considéré la possibilité qu'il existât des liens et des collaborations de circonstance entre les Gafam (Google, Apple, Facebook, Amazon, Microsoft) et les organes gouvernementaux et de renseignements des États-Unis. D'autant que ces entreprises, officiellement domiciliées aux États-Unis, pouvaient être sollicitées par les autorités dans le cadre d'enquêtes. En 2014, l'existence de ce type de collaborations entre les domaines public et privé aux États-Unis a d'ailleurs été confirmée par les porte-parole des entreprises Google, Facebook, Yahoo et Microsoft, qui ont révélé que la NSA émettait régulièrement des mandats exigeant qu'elles divulguent des données en lien avec certains de leurs utilisateurs[20].

Surtout, le témoignage de Snowden a permis d'établir que la NSA possédait un accès direct à des données stockées sur les serveurs de huit entreprises grâce à un outil de surveillance appelé PRISM : Apple, Facebook, Google, Microsoft, Skype, AOL, YouTube et PalTalk. Selon lui, la mise en place d'un accès direct à la plateforme d'hébergement de fichiers Dropbox était par ailleurs en projet.

En 2013, il est donc apparu évident que les données fournies par les citoyens d'un pays à des entreprises étrangères représentaient un enjeu géopolitique et stratégique majeur. Les autorités russes en ont conclu que les logiciels et applications étrangers représentaient des vecteurs de vulnérabilités, pouvant permettre à d'autres États de conduire des attaques informatiques et informationnelles sur leur territoire, puisque les éditeurs de ces logiciels et applications étaient directement dépendants des lois et de l'autorité des gouvernements des pays dans lesquels ils étaient domiciliés.

Le développement de technologies dites *domestiques* (*otetchestvennye technologii*)[21] est donc devenu un thème central des politiques russes de développement technologique, tandis que les révélations de Snowden sont apparues comme un moyen de justification pour le renforcement des logiques protectionnistes en matière de numérique.

L'asile temporaire accordé à Snowden pour un an par les autorités le 31 juillet 2013[22] et la délivrance d'un permis de séjour à son nom le 1er août 2014 sont en

19. Que ces données soient volontairement divulguées par eux, ou captées par des tiers sur les réseaux et plateformes par lesquels elles transitent. Voir les nombreux cas de soldats russes qui dévoilent leur présence en opérations extérieures en postant des photos sur les réseaux sociaux : « Ukraine. Les soldats russes trop bavards sur les réseaux sociaux », *Le Figaro*, 4 août 2014.

20. « Ce que Google, Facebook et Apple ont révélé à la NSA », *Challenges*, 4 février 2014.

21. On pourrait traduire littéralement par « technologies *patriotiques* », puisque l'adjectif *otetchestvennye* a pour racine le mot *père* : *otets*.

22. Entré en vigueur lors de son accueil officiel sur le territoire russe le 1er août 2013.

effet devenus un outil de communication politique et diplomatique. L'État russe a pu mettre en avant la nécessité d'instaurer une troisième voie face à l'emprise et à la surveillance des États-Unis sur les réseaux, et face à ce qu'il a présenté comme une forme d'inaction politique des autres États vis-à-vis de la protection des données de leurs citoyens.

La question du respect des droits et des libertés des internautes est, elle, venue justifier la mise en place de mesures protectionnistes et de contrôle du numérique en Russie aux yeux de la communauté internationale et des internautes russes, puisque les acteurs réfractaires à l'application des nouvelles mesures ont dès lors été perçus comme n'étant pas coopératifs dans l'objectif de protection des données de leurs utilisateurs. C'est notamment le cas de Facebook, qui avait refusé de transférer les données d'internautes russes stockées sur ses serveurs vers des hébergeurs (ou de nouveaux serveurs) situés sur le territoire de la Fédération de Russie, en accord avec la « loi de relocalisation [ou de « rapatriement »] des données personnelles des citoyens russes[23] » entrée en vigueur le 1er septembre 2015.

Les politiques publiques en matière de numérique en Russie ont donc suivi trois phases majeures. D'abord, l'autonomisation numérique russe impulsée par la présidence Medvedev pour des raisons économiques a permis de favoriser la création de logiciels domestiques en Russie. Ces logiciels ont ensuite été mis en avant comme un moyen d'émancipation technique vis-à-vis des logiciels produits à l'étranger. Puis, avec les révélations de Snowden, le discours sur l'émancipation économique et l'autosuffisance numérique russes via le Libre et l'*Open Source* a permis de mettre en avant des considérations sécuritaires. Le Libre et l'*Open Source* sont alors devenus, à leur corps défendant, dans les représentations officielles, un moyen d'autonomisation et d'émancipation stratégique : selon les autorités, leur utilisation – obligatoire pour les institutions publiques sur le territoire – doit assurer la sécurité des infrastructures informatiques de l'État contre les risques liés à l'emploi de logiciels produits à l'étranger.

Des logiciels libres et *open source* russes contre les risques stratégiques liés aux logiciels propriétaires conçus à l'étranger

La production de logiciels souverains sur les modèles libres et *open source* a été présentée par les autorités comme une solution particulièrement adaptée à ces nouveaux enjeux de sécurité. Leurs codes sources ouverts offraient en effet des garanties de sécurité, puisqu'ils pouvaient être directement relus et validés par une

23. Consultable en ligne.

Hérodote, n° 177-178, La Découverte, 2e et 3e trimestres 2020.

communauté d'utilisateurs capable d'attester de l'absence de script malveillant ou de failles dans leur fonctionnement.

Le contrôle que l'*Open Source* permet d'exercer sur le fonctionnement des processus informatiques constitue donc un avantage de sécurité majeur, là où les codes des outils informatiques fournis par les entreprises, généralement privés (donc inaccessibles à la lecture), suivent un fonctionnement mal connu, voire tout à fait opaque. Cette méconnaissance rend notamment possible l'exécution de fonctions en arrière-plan par ces programmes privés, à l'insu de leurs utilisateurs. Le cas le plus courant est la communication des données produites par les appareils d'extrémité (ordinateurs, téléphones mobiles, tablettes, objets connectés...) à propos de l'utilisation qui en est faite, vers les serveurs de l'entreprise qui les commercialise. Bien que la communication de ces données doive généralement servir à l'amélioration des logiciels et des services proposés aux utilisateurs[24], elle constitue un risque de fuites de données stratégiques, semblables à celles qui sont provoquées par les portes dérobées (*backdoors*) installées avec des intentions malveillantes (des données étant, là aussi, exfiltrées à l'insu de leurs utilisateurs).

Selon des recherches menées ces dernières années par le Invisible Things Lab[25], on pouvait soupçonner l'emploi de cette pratique dans le cas des microcontrôleurs embarqués (*embeded microcontrollers*) Management Engine de la marque étatsunienne Intel[26]. Ces composants informatiques sont installés sur un nombre particulièrement important de machines vendues dans le monde entier, car l'entreprise bénéficie d'un quasi-monopole auprès de nombreux constructeurs présents sur le marché mondial de l'informatique.

Or, selon les chercheurs, on connaissait mal[27] le fonctionnement interne de cet élément, puisqu'il est géré par un code propriétaire dont l'écriture et le comportement sont particulièrement protégés par l'entreprise. Certains tests et observations indiquaient néanmoins qu'on y trouvait des vulnérabilités, dont il était difficile de dire si elles avaient été conservées par erreur, par négligence (le code propriétaire n'étant pas accessible, l'entreprise avait pu juger inutile de le faire corriger :

24. Une entreprise peut se servir de ces modes de transmission de données (directement prévus et aménagés dans le fonctionnement de ses produits) de manière à évaluer l'expérience utilisateur de l'une de ses solutions. Pour ce faire, elle y implémente des instructions afin que l'appareil ou le logiciel lui communique régulièrement des informations à propos, par exemple, de sa consommation énergétique ou de son temps d'allumage ou d'utilisation.

25. Un laboratoire de recherche en sécurité informatique fondé et dirigé Joanna Rutkowska, chercheuse titulaire du Master en sciences informatiques de l'Université de technologie de Varsovie, fondatrice de la distribution sécurisée Qubes OS.

26. « The trouble with Intel's Management Engine », Hackaday, 22 janvier 2016.

27. Jusqu'en 2017, voir ci-après.

personne n'étant censé pouvoir en connaître les défauts), ou à dessein. En 2017, les chercheurs du département de rétro-ingénierie de l'entreprise russe Positive Technologies ont ainsi démontré qu'il était possible d'accéder (physiquement) au système de fichiers bruts (*ME flash file system*) des puces matérielles porteuses du bus de données du microcontrôleur[28] (système SPI, *serial peripheral interface*) : ce qui pouvait permettre d'altérer son fonctionnement en réécrivant ses fichiers[29].

Finalement, les recherches effectuées ont fini par démontrer que ce microcontrôleur embarqué constituait une véritable machine dans la machine, bénéficiant d'un accès total à la mémoire des microprocesseurs des ordinateurs dans lesquels il est installé (et ce sans que les ordinateurs hôtes ne le détectent), ainsi qu'un accès complet à la zone chargée du traitement des protocoles de connexion Internet et de transmission des données (pile TCP/IP), lui permettant d'envoyer et de recevoir de l'information (des paquets réseaux) indépendamment du système d'exploitation de la machine hôte ; en outrepassant donc purement et simplement ses pare-feu (*firewall*). Selon ces découvertes, le Management Engine d'Intel représentait non seulement un point de vulnérabilité majeur pour les millions d'ordinateurs dans lesquels il était embarqué[30], mais aussi l'équivalent d'une porte dérobée capable d'accomplir ses propres tâches et de communiquer en réseau (d'envoyer et de recevoir de la donnée) à l'insu de ses utilisateurs[31]. Plus grave encore, il est apparu que les failles présentes dans le code propriétaire des composants d'Intel avaient pu être effectivement exploitées par des pirates informatiques[32].

Les méthodes de transmission d'informations mises en œuvre dans ces composants par les entreprises constituent donc de véritables risques en termes de

28. Élément matériel (composé de conducteurs électriques) géré par un programme qui transfère des données entre différents blocs matériels et logiques. Ces blocs reçoivent des instructions du bus qui permettent de les mettre en marche et de gérer leur fonctionnement. Dans un ordinateur, le bus de données fait la liaison entre le processeur, la mémoire centrale et les contrôleurs de périphériques (contrôleur USB, carte réseau, carte graphique, clavier, etc.).

29. Le fonctionnement de ces puces pouvait en effet être modifié de manière arbitraire, grâce à l'obtention immédiate des droits de lecture/écriture sur leurs fichiers de configuration, ce qui constituait une vulnérabilité grave. Voir « Intel ME : flash file system explained », Blackhat, décembre 2017. D'autres failles massives ont finalement été découvertes sur ce microcontrôleur en 2017, forçant l'entreprise à admettre les défauts de son produit : « Intel admits to serious security flaw in PC chips », Pymnts, novembre 2017.

30. Lily Hay Newman, « Intel chip flaws leave millons of devices exposed », *Wired*, 20 novembre 2017.

31. Jack Wallen, « Is the Intel management engine a backdoor ? », TechRepublic, 1er juillet 2016.

32. Peter Bright, « Sneaky hackers use Intel management tools to bypass Windows firewall », ArsTechnica, 9 juin 2017.

Hérodote, n° 177-178, La Découverte, 2e et 3e trimestres 2020.

sécurité. Elles peuvent être détournées à des fins de renseignement sur la nature ou le fonctionnement d'un matériel, notamment en vue de préparer des attaques destinées par exemple à pratiquer du renseignement industriel ou étatique, voire à corrompre ou à détruire le matériel d'un concurrent ou d'un ennemi, d'une entreprise ou d'un État. En ce sens, tout logiciel propriétaire au code privé n'est donc pas loin de pouvoir constituer une porte dérobée.

Après l'affaire Snowden, mais aussi des découvertes telles que celles de l'entreprise Positive Technologies en 2017, le gouvernement russe a donc décidé de renforcer la création d'alternatives aux produits conçus aux États-Unis, afin de réduire les risques de fuites de données par des portes dérobées et des *rootkits* (programmes malveillants qui dissimulent leur activité), en favorisant encore davantage le développement de solutions *open source* produites en Russie.

Mais cet emploi sécuritaire des logiciels libres et *open source* par les autorités étatiques russes s'oppose au principe de liberté des utilisateurs qui devrait présider à leur développement selon les mouvements Libre et l'*Open Source*. L'instrumentalisation du principe du code source ouvert pour assurer le contrôle des logiciels employés en Russie constitue un détournement évident des valeurs défendues par ces mouvements, qui s'inscrivaient d'abord contre tout contrôle du numérique par des entités de pouvoir (étatiques et privées).

Le sens même de ces mouvements disparaît donc dans ces nouveaux discours autour de la souveraineté et de la sécurité numériques russes, qui servent une convergence d'intérêts économiques et politiques sans lien avec les objectifs de défense de la liberté des utilisateurs et des créateurs de logiciels. Les investissements de l'État dans des alternatives logicielles domestiques vont en effet de pair avec une externalisation accrue des capacités numériques des institutions publiques (pour la sécurisation de leurs infrastructures en particulier), qui semble surtout avantager les acteurs privés.

On peut donc se demander si les logiciels libres et *open source* permettent réellement d'atteindre un objectif de souveraineté numérique en Russie, ou s'ils servent à favoriser les intérêts d'entreprises qui voudraient bénéficier de contrats publics. Si tel est le cas, l'instrumentalisation et le dévoiement de l'esprit du Libre par des acteurs privés ne remettent-ils pas en cause jusqu'aux avantages mêmes qu'il présente en termes de sécurité ?

Derrière les arguments de la souveraineté et de la sécurité informatiques, une convergence d'intérêts opportuniste

Une externalisation des mesures de sécurité informatique par l'État qui profite d'abord aux acteurs privés

Avec la prise en compte du problème de la sécurité informatique, et la mise en avant de l'idée de *souveraineté numérique* en Russie, différents acteurs, provenant en particulier du secteur privé, se sont réapproprié les nouvelles orientations de l'État afin d'être directement parties prenantes – voire de s'assurer un rôle de premier plan – dans la définition des nouvelles logiques à mettre en place, notamment au sujet de la gestion des données des citoyens russes.

L'idée de souveraineté numérique (*cifrovoj suverenitet*) est en effet devenue un élément prépondérant de ces nouvelles logiques à l'initiative, notamment, de l'oligarque Igor Ashmanov, principal détenteur du groupe InfoWatch qui évolue dans le domaine de la sécurité informatique et de la sécurisation des données pour les secteurs public et privé. En contribuant activement à la réflexion autour de la sécurité des données et en particulier des données de l'État, I. Ashmanov a en effet présidé à l'établissement du concept de souveraineté (*suverenitet*) comme un élément de doctrine à part entière pour le développement d'un numérique souverain en Russie[33].

Une nouvelle doctrine sur la sécurité informationnelle (*informacionnaja bezopasnost*), elle-même dépendante d'une certaine souveraineté informationnelle (*informacionnyj suverenitet*), a ainsi été approuvée par la Présidence en décembre 2016, également avec le concours et les conseils de l'oligarque [Présidence de la Fédération de Russie, 2016].

Dans ce cadre, les infrastructures informatiques publiques sont devenues un nouveau marché intérieur considérable pour les acteurs privés, puisqu'il devenait nécessaire de les sécuriser. Leur implication active dans la réflexion autour de la mise en place de nouveaux standards de sécurité leur a donc permis de s'assurer qu'ils pourraient répondre au mieux à ces nouveaux besoins de l'État qu'ils avaient eux-mêmes contribué à définir. L'efficacité de leur démarche transparaît à travers une tendance à l'externalisation des compétences des institutions publiques en matière de numérique à l'instigation de l'État lui-même, en particulier dans le domaine de la sécurité informatique.

L'entreprise InfoWatch est un bon exemple des acteurs privés qui ont pu bénéficier de ces nouvelles logiques, puisqu'elle possédait en 2015 environ 50 % des

33. Voir sa présentation du 14 juillet 2015 au iForum : « Souveraineté de l'information – la nouvelle réalité », <http://files.runet-id.com/2015/tersm/tersm15-3--ashmanov.pdf>.

Hérodote, n° 177-178, La Découverte, 2e et 3e trimestres 2020.

marchés publics dits DLP (*Data Leak(age) Protection*[34]) destinés à la protection des données de l'État, et plus largement à la protection informatique contre les menaces extérieures[35].

Les relations entre cet acteur privé et les institutions publiques sont étroites par ailleurs, puisque N. Kasperskaja fait partie des conseillers les plus sollicités par le gouvernement et la Présidence sur les questions numériques et, à ce titre, a activement participé à la mise en place du grand projet d'indépendance de l'Internet russe (RuNet) vis-à-vis des infrastructures internationales en 2019. Elle est, en outre, la compagne de l'oligarque Igor Ashmanov évoqué plus haut.

Mais, cette tendance à l'externalisation des compétences étatiques en matière de sécurité informatique pose question, y compris du point de vue de la sécurité même des institutions qui y ont recours. On peut remarquer, en effet, qu'au moins deux entreprises contractuelles des services de sécurité russes en matière de sécurité de numérique ont subi des attaques informatiques, qui ont conduit à la plus importante fuite de données connue de l'histoire des services de renseignement du pays : celle de l'entreprise SyTech, le 13 juillet 2019.

Les liens entre le secteur privé de l'informatique et les institutions publiques en Russie sont révélateurs des nouvelles logiques de défense numérique du pays, qui mobilisent tous les acteurs du domaine. Mais ils sont également le signe de l'influence décisive d'acteurs privés qui ont su profiter des nouvelles lois sur l'emploi de logiciels libres et *open source* par les institutions publiques ; et qui ont su faire concorder leurs besoins avec ceux des autorités, si ce n'est ceux des autorités avec les leurs.

*Les nouveaux acteurs du Libre et de l'*open source *en Russie : primauté des questions économique et technique sur les questions politiques et militantes liées à ces mouvements*

Conséquence des politiques incitatives mises en œuvre par l'État en Russie, les mouvements Libre et *open source* semblent y avoir perdu leur valeur politique de contestation de la domination des entités privées et gouvernementales sur le numérique, au détriment de la liberté des utilisateurs de logiciels.

Les acteurs qui s'intéressent à la production de logiciels libres et *open source* en Russie sont en effet de moins en moins attachés aux questions politiques et

34. Protection contre la fuite de données : *predotvraščenie utečk informacii*.

35. Selon le directeur général de l'entreprise Natalija Kasperskaja, ex-épouse d'Eugène Kaspersky, le créateur et détenteur de l'entreprise Kaspersky Lab (cofondée par les époux en 1997).

militantes qu'ils sous-tendent. Force est de constater que l'appui discursif, législatif et financier apporté par l'État russe au Libre et à l'*open source* dans le pays a eu pour principal effet d'en privatiser le développement et l'emploi. Ces logiciels sont désormais produits en priorité par les entreprises qui souhaitent bénéficier de contrats étatiques et employés par des utilisateurs qui en perçoivent d'abord les avantages économiques (logiciels moins chers) et de sécurité : les logiciels russes devant être perçus comme plus sûrs pour le citoyen russe que les logiciels étrangers, ce qui est loin d'être assuré. La fuite de données de SyTech a en effet montré que des acteurs privés pouvaient produire des solutions informatiques en collaboration avec les services de sécurité, dans le but de faciliter la surveillance des internautes dans le pays.

L'aspect largement superficiel et opportuniste de cette apparente prise de position des entreprises russes pour le développement libre et *open source* transparaît ainsi ponctuellement.

En ce sens, il intéressant de noter que le logiciel libre ASTRA Linux employé par les forces armées russes n'est pas tout à fait libre en réalité. Si le noyau Linux et les fonctions primaires du système d'exploitation sont accessibles en ligne, téléchargeables et modifiables par n'importe quel utilisateur[36], la version de la distribution qui est employée par les forces armées correspond, elle, à une version fermée appelée « Édition spéciale ». L'entreprise RusBITech-ASTRA peut ainsi bénéficier de la commercialisation de cette version aux forces armées russes, qui ne respecte pas les exigences du Libre[37].

Conclusion

Depuis les années 2010, on observe un intérêt incontestable de l'État russe pour les pratiques et modes de production informatique dits libres et *open source*, qui a conduit à une augmentation de leur promotion et leur emploi par les secteurs public et privé. Avec les révélations de Snowden en 2013, les principaux arguments avancés pour les favoriser sont passés des avantages offerts par leur faible coût d'achat et de production, à un emploi qui devait redynamiser l'industrie russe du numérique sur le territoire et, enfin, à la nécessité de les employer pour assurer

36. Cette « Édition commune » (*Common Edition*) est donc bien libre.

37. Ce modèle (mi-libre/mi-privateur et commercial) constitue d'ailleurs une source de conflit dans les milieux de l'*open source* et du Libre. Les entreprises qui le mettent en œuvre font valoir que les logiciels qu'elles commercialisent leur permettent de maintenir le développement de leurs logiciels libres et gratuits, en rémunérant les développeurs et codeurs qui y contribuent.

Hérodote, n° 177-178, La Découverte, 2e et 3e trimestres 2020.

la sécurité informatique des infrastructures publiques et la souveraineté numérique du pays.

Parallèlement, l'État russe et les différents organes et administrations qui en dépendent sont devenus un important marché intérieur que cherchent à conquérir des entreprises russes peu sollicitées, voire désormais indésirables à l'étranger à la suite, notamment, du scandale provoqué aux États-Unis par les collusions supposées entre l'entreprise Kaspersky Lab (qui commercialise l'antivirus Kaspersky) et les services de renseignement russes.

Ce marché intérieur, caractérisé par sa volonté d'acquérir des solutions libres et/ou *open source*, a donc fini par faire de ces modes de développement un argument marketing décisif sur le territoire. Leur promotion modifie ainsi à la fois l'écosystème du développement numérique en Russie, et le sens même de ce que signifiaient le Libre et l'*open source*. Car les aspects politiques et militants que recouvrent ces deux modes de production-mouvements ont été peu à peu évacués pour laisser place à des logiques économiques et commerciales.

Le principe du code source ouvert des logiciels libres et *open source* a ainsi été détourné de sa fonction première – permettre aux utilisateurs de solutions informatiques de choisir et de contrôler le fonctionnement de leurs logiciels – pour favoriser à la place le contrôle des autorités étatiques sur les pratiques de ces utilisateurs et les infrastructures informatiques en Russie. L'accessibilité des codes libres et *open source* suscite donc la convoitise de différents acteurs publics et privés, qui ont recours à de véritables logiques de prédation, contre tous les principes qui sont défendus par ces mouvements.

La descente de police qui s'est déroulée le 13 décembre 2019 dans les locaux de l'entreprise Nginx à Moscou et a conduit à l'arrestation de plusieurs employés, dont le développeur Igor Sysoev, le montre. Elle a en effet eu lieu à la demande de l'entreprise Rambler, créatrice de l'important moteur de recherche russe Rambler.ru qui revendique la paternité du logiciel NGINX *open source* créé en 2002 par I. Sysoev. Au moment de la création du logiciel, celui-ci travaillait pour Rambler : ce que l'entreprise met en avant pour en récupérer les droits[38].

Cette soudaine revendication de Rambler n'est pas un hasard : en février 2019, le serveur Web du système NGINX est devenu le serveur le plus utilisé au monde. Ce succès a attiré les investissements de l'entreprise étatsunienne F5 Networks, qui a racheté NGINX Inc. en mars 2019. L'événement laisse donc place à différentes interprétations, depuis la volonté de Rambler de récupérer les importants

38. I. Sysoev a, en effet, créé NGINX afin de gérer l'important trafic du portail Web Rambler.ru. Le logiciel était cependant considéré depuis comme un logiciel libre et n'appartenait pas à l'entreprise, selon la volonté de son créateur.

bénéfices que lui procurerait la propriété du logiciel, à la volonté de contrer l'influence d'un acteur domicilié aux États-Unis sur le premier serveur mondial.

Dans tous les cas, la nouvelle place centrale du Libre et de l'*open source* en Russie, au cœur des volontés de dynamisme économique, de sécurité informatique et de souveraineté numérique, expose leurs logiciels à toutes les convoitises, et altère peu à peu leur efficacité pour la sécurité des utilisateurs et le sens des mouvements qui leur ont donné naissance.

Bibliographie

ASSEMBLÉE GÉNÉRALE DES NATIONS UNIES (1999), *Résolution A/RES/53/70*, URL : <https://undocs.org/A/RES/53/70>.

DOUMA D'ÉTAT (2015), loi fédérale n° 764677-6, URL : <http://pravo.gov.ru/proxy/ips/?docbody=&nd=102374921>.

GILES K. (2016), *Handbook of Russian Information Warfare*, Collège de Défense de l'Otan.

KURTCHERJAVYJ M. (2014), « Politique d'État pour la souveraineté informationnelle de la Russie dans un monde moderne mondialisé », *Conseil en gestion*, n° 9, p. 7-14.

LIMONIER K. (2012), « Analyse géopolitique des enjeux d'une politique de puissance : le cas de la science et de l'innovation en Russie », *Hérodote*, vol. 146-147, n° 3, p. 193-216.

LOGÉ Y. (1991), *L'URSS. Le défi technologique, la révolution inachevée*, Paris, PUF.

MINISTÈRE DU DÉVELOPPEMENT NUMÉRIQUE, DES RÉSEAUX ET DES COMMUNICATIONS DE MASSE DE LA FÉDÉRATION DE RUSSIE (2010), « Plan de transition des organes fédéraux des autorités de l'exécutif et des institutions du budget fédéral vers l'utilisation de logiciels libres de sécurité pour la période 2011-2015 », URL : <http://minsvyaz.ru/uploaded/files/2299p.pdf>.

MORENKOVA PERRIER E. (2014), « De la sécurité informationnelle à la cybersécurité : la redéfinition de la doctrine stratégique russe », *Revue défense nationale*, tribune n° 586, p. 1-7.

PERENS B. (1999), « La définition de l'*Open Source* », *in* DIBONNA C., OCKMAN S. et STONE M., *Open Sources. Voices from the Open Source Revolution*, trad. Sébastien Blondeel, O'Reilly & Associates, en ligne.

PRÉSIDENCE DE LA FÉDÉRATION DE RUSSIE (2016), « Doctrine de la Fédération de Russie pour la sécurité de l'information », URL : <http://publication.pravo.gov.ru/Document/View/0001201612060002?index=1&rangeSize=1>.

TCHERNENKO E. (2013), « Cold War 2.0 ? Cyberspace as the New Arena for Confrontation », *Russia in Global Affairs*, n° 1, URL : <https://eng.globalaffairs.ru/number/Cold-War-20-15929>.