ÉTUDES
DE L'IFRI

PROGRAMME GÉOPOLITIQUE DES TECHNOLOGIES

DÉCEMBRE
2022

Sources d'influence

Enjeux économiques et géopolitiques des logiciels *open source*

Alice PANNIER

L'Ifri est, en France, le principal centre indépendant de recherche, d'information et de débat sur les grandes questions internationales. Créé en 1979 par Thierry de Montbrial, l'Ifri est une association reconnue d'utilité publique (loi de 1901). Il n'est soumis à aucune tutelle administrative, définit librement ses activités et publie régulièrement ses travaux.

L'Ifri associe, au travers de ses études et de ses débats, dans une démarche interdisciplinaire, décideurs politiques et experts à l'échelle internationale.

ISBN : 979-10-373-0640-1

Comment citer cette publication :
Alice Pannier, « Sources d'influence. Enjeux économiques et géopolitiques des logiciels *open source* », *Études de l'Ifri*, Ifri, décembre 2022.

Ifri

27 rue de la Procession 75740 Paris Cedex 15 – FRANCE

Tél. : +33 (0)1 40 61 60 00 – Fax : +33 (0)1 40 61 60 60

E-mail : accueil@ifri.org

Site internet : Ifri.org

Auteure

Alice Pannier est chercheuse et responsable du programme Géopolitique des technologies, lancé à l'Ifri en octobre 2020, après avoir été chercheuse associée depuis 2019. Ses recherches portent sur les politiques technologiques européennes et les relations extérieures de l'Europe. Elle a récemment publié « Souveraineté numérique. Bilan du quinquennat et propositions des candidats à la présidentielle 2022 », *Briefings de l'Ifri*, 15 mars 2022 et « Calcul stratégique. Le calcul haute performance et l'informatique quantique dans la quête de puissance technologique de l'Europe », *Études de l'Ifri*, Ifri, octobre 2021.

Avant de rejoindre l'Ifri, elle a été professeure assistante en relations internationales et études européennes à la Paul H. Nitze School of Advanced International Studies (SAIS) de l'université Johns Hopkins à Washington (2017-2020). Diplômée du King's College de Londres et de l'université Paris-I Panthéon-Sorbonne, elle est titulaire d'un doctorat de l'IEP de Paris.

Résumé

L'*open source* tient une place centrale dans le développement des logiciels, sur un mode à la fois parallèle au modèle propriétaire, et de plus en plus imbriqué avec celui-ci. Il est devenu un élément déterminant dans les processus d'innovation des entreprises du numérique et pour le succès et la popularité de leurs produits à l'échelle mondiale. Plus encore, l'*open source* est au fondement de briques logicielles critiques et des langages et protocoles d'internet, et joue un rôle dans le développement de technologies émergentes.

L'*open source* peut toutefois être victime de son succès et souffre d'un manque de moyens dédiés à sa maintenance. Or, les vulnérabilités dans les codes sources ouverts peuvent avoir de graves conséquences, comme l'a illustré la faille « Log4Shell » révélée en décembre 2021.

Les entreprises privées investissent financièrement et humainement au développement et au maintien de l'écosystème. Ce soutien est critique pour pallier les risques liés au manque de maintenance de certains composants. Cependant, cette implication n'est pas sans danger pour l'écosystème *open source*, qui est de plus en plus modelé par les intérêts privés des *Big Tech*.

Parallèlement, les gouvernements sont de plus en plus préoccupés par les risques de l'*open source* en matière de cybersécurité, non seulement du fait de vulnérabilités accidentelles, mais aussi de la manipulation des codes par des criminels et des agents étrangers. L'intérêt des gouvernements pour l'*open source* n'est pas nouveau, mais il évolue : les gouvernements ne cherchent plus seulement à adopter l'*open source* ou à développer des solutions logicielles, mais aussi à contribuer au financement ou même à la gouvernance des écosystèmes *open source*, au niveau national et/ou mondial.

L'analyse des cas américain, chinois et européen montre que l'implication des gouvernements dans l'*open source* n'est pas seulement pragmatique ; elle est de plus en plus politisée et sert à soutenir les ambitions des gouvernements en matière de sécurité nationale, d'influence internationale ou de souveraineté numérique. L'étude met en évidence les dilemmes qui émergent, pour les autorités publiques, des tensions entre le désir de sécuriser des composants *open source* critiques universels, le désir de développer des technologies « souveraines », et le risque d'empiéter sur le fonctionnement horizontal et décentralisé de l'*open source*.

Executive Summary

Open source plays a central role in software development, both in parallel with proprietary software and increasingly intertwined with it. It has become a major factor for companies' innovation processes and for the success and popularity of their products. For users, using open-source software can alleviate risks stemming from proprietary solutions, including data privacy concerns or trade restrictions. Beyond that, open source is the foundation of critical software bricks and Internet languages and protocols.

However, open source is a victim of its own success. It suffers of a lack of resources dedicated to the maintenance of open-source components, even though vulnerabilities in open-source code can have serious consequences, as illustrated by the Log4Shell vulnerability in December 2021.

For these reasons, private companies are investing ever more money and human resources in the development and maintenance of open-source software, and acquiring structuring roles in the governance of the ecosystem. This support, however, is not without risk for the open-source ecosystem, which is increasingly shaped by the private interests of Big Tech companies.

Meanwhile, governments are getting increasingly concerned with the cybersecurity implications of open-source software, and with risks not only of accidental vulnerabilities, but also manipulation of codes by criminals and foreign agents. The interest of governments in open source is not new, but it is evolving: governments are no longer only seeking to adopt open source or to develop software solutions, but also to contribute to the financing or even the governance of open source ecosystems, at the national and/or global level.

An analysis of the US, Chinese and European cases show that government involvement in open source is not only pragmatic ; it is increasingly politicized, and serves to uphold governments' ambitions for national security, international influence, or digital sovereignty. The study highlights the dilemmas that emerge, for public authorities, from the tensions between the desire to secure universally used, critical open-source components, the desire to develop "sovereign" technologies, and the risk of encroaching on the horizontal and decentralized functioning of open source.

Sommaire

Introduction

L'une des tendances technologiques actuelles est celle d'une « softwarisation » toujours plus grande des activités humaines, c'est-à-dire un recours aux logiciels pour un nombre croissant d'activités au niveau des individus, des entreprises et des États. La transformation de l'industrie, la numérisation du service public, le déploiement de la 5G, et l'avènement de l'Internet des objets (*Internet of Things*, IoT) sont autant de facteurs qui contribuent à accroître l'importance stratégique des logiciels. Par conséquent, comme l'explique la fondation Linux dans un récent rapport :

> « Les vulnérabilités et les faiblesses dans les logiciels largement déployés présentent des menaces systémiques pour la sécurité et la stabilité de la société moderne, car les services gouvernementaux, les fournisseurs d'infrastructures, les organisations à but non lucratif et la grande majorité des entreprises privées dépendent des logiciels pour fonctionner[1]. »

Ces mêmes logiciels sont de plus en plus complexes, dans leurs fonctionnalités et dans leurs composants, créant là aussi de nouveaux risques et rendant nécessaire une évolution des analyses de sécurité[2].

Au cœur de ces logiciels se trouve l'*open source* (OS), c'est-à-dire un modèle de développement et de diffusion de logiciels reposant sur des codes sources ouverts[3]. On estime qu'entre 80 % et 96 %, des codes qui composent les logiciels aujourd'hui sur le marché – y compris les logiciels propriétaires – sont d'origine *open source*[4]. Certains constituent des briques technologiques critiques pour des logiciels et serveurs web très largement utilisés dans le monde. Qu'ils le sachent ou non, la plupart des entreprises, des particuliers et des gouvernements utilisent des logiciels ou des

1. « The Open Source Software Security Mobilization Plan », Livre blanc, Linux Foundation et OpenSSF, 2022, p. 3. [Nous traduisons.]
2. « L'ANSSI et le CEA renforcent leur collaboration en cybersécurité », Communiqué de presse, ANSSI/CEA, 29 juin 2022, disponible sur : www.ssi.gouv.fr.
3. Il convient ici de justifier du choix du terme « *open source* » et de le distinguer du terme « logiciel libre ». Les logiciels libres reposent sur quatre libertés édictées à la fin des années 1980 par Richard Stallman de la Free Software Foundation : libertés d'exécuter le programme, d'en étudier le fonctionnement, d'en redistribuer des copies (gratuitement ou non), d'apporter des améliorations et de les partager également. Les logiciels développés en *open source* remplissent généralement les conditions sur « libre », et vice versa ; on parle d'ailleurs souvent de « logiciel libre et *open source* » (« *free and open source software* »). Cela étant, l'*open source* se réfère à un mode de développement de logiciels plutôt qu'à un type de licence, puisque des composants *open source* se retrouvent dans la plupart des logiciels propriétaires. Dans cette étude, nous préférerons l'emploi du terme « *open source* », qui se réfère indistinctement aux logiciels ou à leurs composants.
4. « 2022 Open Source Security and Risk Analysis Report », Synopsis, avril 2022 ; K. Szulik, « Open Source Is Everywhere: Survey Results », Tidelift, 12 avril 2018, disponible sur : https://blog.tidelift.com ; T. Herr, « Responding to and Learning from the Log4Shell Vulnerability », témoignage auprès du Committee on Homeland Security and Government Affairs, Sénat des États-Unis, 8 février 2022.

composants *open source*. Ainsi, selon David Nalley de l'Apache Software Foundation, « l'*open source* n'est pas simplement une composante importante de l'industrie du logiciel, c'est l'un des fondements de l'économie mondiale moderne[5] ». En outre, toutes les technologies émergentes, telles que l'Intelligence artificielle (IA) et l'IoT, comprennent des éléments développés en *open source*, si bien que l'importance stratégique du phénomène va continuer de croître.

Cet état de fait soulève plusieurs questions. Pourquoi et comment l'OS est-il devenu un élément si structurant de l'infrastructure et de l'économie numérique mondiales ? Comment s'organise l'écosystème *open source* mondial aujourd'hui ? Quels liens et quelles tensions existe-t-il entre l'*open source* et les acteurs privés dominants ? Comment les États se saisissent-ils de cet enjeu, et avec quelles conséquences possibles sur l'écosystème ?

Dans la première partie de l'étude, nous verrons que l'*open source* soulève des enjeux à la fois de cybersécurité et des enjeux économiques et d'innovation. L'OS offre des gains pour le développement des logiciels, que ce soit en termes de rapidité, de qualité, de transparence des composants et des éventuelles failles, d'interopérabilité, ou d'autonomie d'usage. Paradoxalement, l'OS souffre toutefois de faiblesses bien connues qui ont trait au caractère principalement bénévole du travail des contributeurs et mainteneurs de projets *open source*, y compris les plus critiques.

Pour ces raisons, l'*open source* fait actuellement l'objet d'une attention accrue, ainsi que de stratégies spécifiques, de la part d'acteurs privés et publics, qui cherchent à en tirer le meilleur parti. Nous examinerons dans une seconde partie le rôle des grands acteurs qui structurent l'écosystème *open source*. Les grandes entreprises technologiques se sont, les premières, saisies de cet enjeu pour des raisons pratiques comme économiques. De fait, elles jouent d'ores et déjà un rôle structurant dans l'écosystème *open source*, qui s'organise par ailleurs autour de grandes fondations et de dépôts de code.

Nous analyserons enfin le rôle des États, où la prise de conscience des enjeux stratégiques de l'*open source* au plus haut niveau politique est récente, mais va croissant. L'analyse des cas américain, chinois et européen montre que l'implication des gouvernements dans l'OS n'est pas seulement pragmatique ; elle est de plus en plus politisée et sert à soutenir les ambitions des gouvernements en matière de sécurité nationale, d'influence internationale ou de souveraineté numérique. L'étude montre également que trouver un équilibre entre la volonté de sécuriser des composants *open source* critiques de portée globale, le désir de développer des technologies « souveraines », et le risque d'empiéter sur le fonctionnement horizontal et décentralisé de l'*open source*, est loin d'être aisé.

5. D. Nalley, « Responding to and Learning from the Log4Shell Vulnerability », témoignage auprès du Committee on Homeland Security and Government Affairs, Sénat des États-Unis, 8 février 2022. [Nous traduisons.]

La montée en puissance de l'*open source* dans les logiciels : opportunités et défis

Les modalités de développement et de diffusion des logiciels se structurent autour de deux grands modèles de licence, et par extension, modèles économiques et politiques : les logiciels propriétaires et les logiciels dits *open source*. Les logiciels propriétaires, ont été initialement dominants, mais présentent des limites, tels qu'un coût économique élevé et des risques, notamment à l'aune de la compétition géopolitique internationale. En parallèle, on constate depuis une vingtaine d'années une montée en puissance de l'*open source*, où des logiciels ou composants de logiciels ont acquis une centralité dans l'infrastructure numérique globale. Il devient cependant de plus en plus difficile de distinguer les deux modèles, du fait d'une hybridation croissante des processus de développement de logiciels. Par ailleurs, l'écosystème est confronté à des cas de failles de cybersécurité et à un manque structurel de moyens alloués à la maintenance de certains composants – éléments qui ont éveillé l'attention des entreprises comme des États.

L'*open source* au cœur de l'infrastructure et de l'économie numériques

La quête d'une alternative au modèle propriétaire

Depuis l'aube de l'ère internet dans les années 1970 jusqu'à la fin des années 1990, les logiciels propriétaires ont proliféré et sont devenus dominants[6]. Dans le modèle propriétaire, le logiciel est généralement développé par une entité privée dans un but lucratif. Le logiciel est payant et mis à disposition du client, par un système de licence ou, notamment pour les logiciels disponibles depuis le *cloud*, via un abonnement. D'autres sources de revenus pour les éditeurs de logiciels incluent les contrats de maintenance, la vente de services associés et des fonctions « premium » ou encore la publicité[7]. Dans le modèle propriétaire, le code source du logiciel n'est généralement

6. K. Brigham, « How Open-Source Software Took Over the World », CNBC, 14 décembre 2019, disponible sur : www.cnbc.com.
7. « The Economic and Social Impact of Software & Services on Competitiveness and Innovation », SMART 2015/0015, Union européenne, 2017, p. 25ff.

pas accessible par l'utilisateur, et le logiciel ne peut donc pas être examiné ou modifié.

La domination des logiciels propriétaires a depuis été remise en question. Pour les utilisateurs, le modèle des logiciels propriétaires pose en effet un ensemble de problèmes et de risques, qui expliquent en partie la volonté des entreprises, gouvernements et particuliers, de recourir à des alternatives, comme les logiciels libres et *open source*. Le contexte de compétition géopolitique mondiale accroît les risques liés aux dépendances à des logiciels propriétaires, notamment lorsqu'ils sont produits par des firmes étrangères : risques de cybersécurité et faibles visibilité sur ces risques, dépendance à des législations extraterritoriales (notamment en matière de traitement des données issues de l'usage des logiciels), voire même des restrictions au commerce et à l'usage de certains logiciels pour des raisons politiques ou de sécurité nationale.

Logiciels propriétaires : risques cyber… et physiques

Des débats animent les communautés d'experts concernant les avantages respectifs des logiciels propriétaires et *open source* pour ce qui concerne la cybersécurité, mais il est généralement admis que l'impact d'une faille de sécurité dans un logiciel dépend avant tout de l'étendue de son usage[8]. Dès lors, les éditeurs de logiciels dominants ont une responsabilité particulière en matière de sécurité de leurs produits et d'information des utilisateurs en cas de faille de sécurité. Ces garanties de sécurité sont d'autant plus importantes pour les logiciels dits « critiques » sur le plan de la sécurité, tels que ceux qui réalisent des fonctions critiques sur le plan de la confiance de l'utilisateur (privilèges ou accès direct aux réseaux et aux machines, par exemple[9]). Les logiciels antivirus notamment sont critiques du fait de leur caractère intrusif.

L'expérience récente de l'attaque SolarWinds est une illustration de l'impact sévère qu'une faille dans un logiciel critique peut produire. Le logiciel Orion, développé par SolarWinds, est un outil de surveillance des performances système, installé dans des milliers d'organisations aux États-Unis, dont l'administration américaine elle-même. Orion a été l'objet d'un code malveillant, révélé en décembre 2020, qui a permis aux attaquants d'accéder pendant de nombreux mois aux données, réseaux et systèmes concernés[10].

Enfin, dans le contexte du développement de l'IoT on peut mentionner le cas des logiciels embarqués. Les accidents impliquant l'avion Boeing 737 MAX, en 2018 et 2019, ont ainsi été causés en partie par des erreurs dans les

8. « Open Source and Commercial Software: An In-Depth Analysis of the Issues », Business Software Alliance, 2005, p. 8-12.
9. « Improving the Nation's Cybersecurity », Executive order n° 14028, Federal Register, 12 mai 2021.
10. « État de la chaine logistique logicielle en 2021 », Sonatype, 2021, p. 13.

logiciels de l'appareil, après que le développement de ceux-ci ait été sous-traité et non supervisé[11]. Ce type de problématiques de cybersécurité est amené à se multiplier avec les objets connectés, notamment dans l'automobile[12].

Protection des données et dérives des plateformes

D'autres problématiques relatives aux solutions propriétaires concernent la protection des données, ainsi que les craintes liées à l'exfiltration et l'exploitation non consentie de ces données. L'un des risques concerne d'éventuelles *backdoors* (portes dérobées) intégrées à dessein dans les logiciels propriétaires, qui peuvent concerner tout type de terminal[13]. Ces derniers temps, l'attention a notamment porté, en Europe, sur les logiciels mis à disposition sur le *cloud* en modalité *Software as a Service* (ou SaaS). Ceux-ci peuvent être sujets aux lois du pays où sont basés les fournisseurs de logiciels, et donc soumis à des obligations de transmettre aux autorités de leur pays des données d'utilisateurs. Les préoccupations liées aux fournisseurs de services *cloud* américains sont bien connues, et régulièrement réitérées par les autorités françaises[14]. Les inquiétudes sont encore plus grandes vis-à-vis des fournisseurs chinois. À titre illustratif, alors que Alibaba est pressenti pour héberger des données dans le cadre des Jeux olympiques et paralympiques de Paris en 2024, la Cour des comptes a identifié des « possibilités d'"exfiltration des bases de données [...] à des fins stratégiques ou d'espionnage économique" ou de "prépositionnement" dans des réseaux "pour mener des actions ultérieures" », si le Comité d'organisation recourait aux services du fournisseur chinois[15].

Ce type d'inquiétudes ne concernent pas que les logiciels *cloud*. L'application de réseau social TikTok fait également l'objet d'une attention accrue de la part de plusieurs gouvernements, inquiets du traitement qui peut être fait des données utilisateurs lorsqu'elles sont transférées vers la Chine. Le gouvernement indien a même interdit depuis 2020 l'usage de TikTok, ainsi que celui d'autres applications chinoises, pour cette raison[16].

Une autre tendance, récente, concerne les inquiétudes face aux pratiques des grandes plateformes, telles que les réseaux sociaux, concernant leur gestion des contenus et leur politique de modération. Ainsi à l'automne

11. P. Robison, « Boeing's 737 Max Software Outsourced to $9-an-Hour Engineers », Bloomberg, 28 juin 2019.
12. R. Csernatoni et M. Blumenthal, « Computers on Wheels: Automated Vehicles and Cybersecurity Risks in Europe », Carnegie Europe, 24 mars 2022.
13. M.-G. Bertran, « La place des logiciels libres et *open source* dans les nouvelles politiques du numérique en Russie », *Hérodote*, n° 177-178, 2020, p. 245.
14. « Audition, à huis clos, de M. Stéphane Bouillon, Secrétaire général de la défense et de la sécurité nationale », Compte rendu, Commission de la Défense nationale et des forces armées de l'Assemblée nationale, 13 juillet 2022, p. 6.
15. A. Guiton, « JO 2024: pour la protection des données, les autorités veulent déminer le problème Alibaba », *Libération*, 26 juillet 2022.
16. D. Milmo, « TikTok's Ties to China: Why Concerns Over Your Data Are Here to Stay », *The Guardian*, 8 novembre 2022.

2022, les débats autour de Twitter depuis son rachat par Elon Musk, ont mis sur le devant de la scène l'existence d'alternatives *open source*, comme Mastodon, face aux dérives de la plateforme.

Restrictions au commerce et à l'utilisation des logiciels

Enfin, un ensemble de risques moins répandus à ce stade, néanmoins inquiétants pour les entreprises comme pour les gouvernements, concerne les (potentielles) restrictions au commerce et à l'usage de logiciels propriétaires, selon leur pays d'origine ou de destination. Si ces restrictions au commerce des logiciels, dont certaines datent de la guerre froide, concernent principalement des logiciels à usage militaire, elles tendent à s'étendre à un ensemble croissant de logiciels utiles dans l'ingénierie et le développement de technologies, tels que les semi-conducteurs[17]. Ainsi, certains logiciels, notamment les logiciels américains qualifiés de « *US Origin* » ne peuvent pas être vendus en Chine[18]. Ces restrictions peuvent avoir des effets indirects : si certaines technologies ont été développées à l'aide de logiciels américains concernés par des restrictions, ces technologies sont soumises aux contrôles américains, puisque selon la règle dite *Foreign Direct Product Rule* (FDPR), l'octroi d'une licence américaine est nécessaire pour pouvoir (ré)exporter vers la Chine et d'autres pays certains produits développés à l'aide de machines ou logiciels américains. Par ailleurs, selon les restrictions au transfert de technologies, un utilisateur de solutions *cloud* peut involontairement enfreindre certaines restrictions si les services utilisés en ligne sont routés *via* des pays étrangers, à son insu[19].

Si ces contrôles concernent généralement des technologies de pointe, des restrictions peuvent être placées sur des logiciels à l'usage plus répandu. Ainsi, la Chine a mis en place depuis la fin des années 2000 des restrictions à l'usage de logiciels américains, tels que les outils de Google, sur son territoire, y compris pour les entreprises occidentales qui y sont implantées, ce qui complique grandement leurs activités quotidiennes. Plus récemment, l'invasion russe de l'Ukraine à partir de la fin février 2022 a entraîné une offensive américaine et, dans une moindre mesure, européenne, contre l'entreprise russe de cybersécurité Kaspersky, dont les logiciels antivirus sont largement utilisés en Europe, pour en interdire ou en déconseiller l'usage au sein de l'administration et d'entreprises dans des secteurs sensibles[20].

17. « Commerce Implements New Multilateral Controls on Advanced Semi-conductor and Gas Turbine Engine Technologies », Département américain du Commerce, 12 août 2022, disponible sur : www.bis.doc.gov.
18. M. Velliet, « Convaincre et contraindre : les interférences américaines dans les échanges technologiques entre leurs alliés et la Chine », *Études de l'Ifri*, Ifri, février 2022.
19. « Cloud Computing and Export Control », The Institute of Export & International Trade, 9 septembre 2020, vidéo disponible sur : https://youtu.be.
20. A. Guiton, « Face au Russe Kaspersky, la défiance virale des Occidentaux », *Libération*, 5 mai 2022.

*L'*open source *: élément incontournable du développement de logiciels*

Principes à l'origine des logiciels libres et de l'*open source*

Par opposition aux logiciels propriétaires, les logiciels libres et *open source* sont en principe, sans nationalité et donc sans frontières. Le modèle de licence *open source* revient à rendre disponible aux utilisateurs les codes sources d'un logiciel, permettant ainsi la redistribution, les modifications et les ajouts, avec des restrictions bien moindres que dans le cas des logiciels propriétaires[21]. Historiquement, le mouvement *open source* découle du mouvement pour le logiciel libre, né dans les années 1980 aux États-Unis. Les logiciels *open source* sont également largement utilisés dans les organismes de recherche, du fait de leur caractère adaptable et customisable en fonction des besoins des expériences.

Certains logiciels et composants *open source* sont absolument structurants pour le développement de nombre de logiciels et pour le fonctionnement d'internet ; ils sous-tendent l'infrastructure logicielle globale et sont présents dans les logiciels développés par les entreprises privées. On peut citer les langages de programmation Python et Perl, le système d'exploitation Linux, le navigateur web Mozilla Firefox, le système de gestion de bases de données MySQL, le serveur HTTP Apache, et la plupart des outils Java. Preuve de la vitalité du modèle, 10 000 lignes de code sont ajoutées à Linux chaque jour et 5 000 lignes sont modifiées quotidiennement[22].

L'hybridation des modèles libre et propriétaire

Les éditeurs de logiciels ont été longtemps réticents face à ce modèle qu'ils jugeaient contraire au principe de la propriété intellectuelle, sur laquelle repose leur modèle économique, un représentant de Microsoft allant jusqu'à qualifier l'OS de « *unamerican*[23] » (anti-américain). Toutefois, l'OS a connu une montée en puissance ces dernières décennies après le lancement de Linux en 1991, et particulièrement à partir des années 2010[24]. Les entreprises comme les gouvernements ont commencé à inclure du code *open source* dans leurs produits, pour répondre à leurs besoins spécifiques. Les entreprises contribuent également au développement de l'OS *via* leurs équipes de

21. Notons qu'il existe différents types de licences *open source*, plus ou moins restrictives dans l'accès aux codes sources et l'utilisation qui peut être faite de ceux-ci. Deux modèles cohabitent. D'une part, il a les licences à réciprocité (dites « *copyleft* » en référence à la notion de *copyright*, comme la license publique générale GNU, datant de 1989), qui imposent le repartage selon les mêmes termes du logiciel, voire de toute amélioration ou logiciel développé sur sa base. D'autre part, il y a les licences dites permissives qui permettent la redistribution du code sous d'autres licences sous réserve du maintien de certaines obligations (par exemple, les licences Apache, MIT, etc.).
22. K. Brigham, « How Open-Source Software Took Over the World », *op. cit.*
23. *Ibid.*
24. « The Economic and Social Impact of Software », *op. cit.*

programmeurs ou en mettant à disposition auprès de la communauté OS des programmes développés en interne (cf. *infra*). Symbole de ce revirement du secteur privé, en 2008, Google a lancé le système d'exploitation pour téléphone mobile Android, basé sur une version modifiée de Linux. Ce système est à présent dominant, avec 2,5 milliards d'appareils dans le monde utilisant Android[25].

Il existe donc à la fois une complémentarité et une convergence entre les logiciels propriétaires et les logiciels *open source*. On a vu que des briques technologiques *open source* sont aujourd'hui intégrées dans la quasi-totalité des logiciels propriétaires développés par des entreprises. La réalité est donc souvent un mélange des deux modèles : les développeurs de logiciels créent des assemblages de composants *open source* existants et d'éléments propriétaires. Selon une estimation, les applications logicielles modernes contiennent souvent plus de 100 composants *open source*[26]. Généralement, les bas niveaux du système peuvent être ouverts, alors que les interfaces utilisateurs, où se situent les innovations dans les logiciels et applications, sont propriétaires. Cela créé ce qu'on appelle des dépendances, et parfois une difficulté à tracer tous les composants d'un logiciel (cf. *infra*)[27].

Ensuite, « logiciel libre » ne veut pas nécessairement dire « logiciel non commercial ». Au contraire, un programme libre peut être utilisable, développable et distribuable dans un cadre commercial[28]. Il existe par ailleurs des logiciels dits « *Commercial open source* », tel que ceux développés par Red Hat : l'entreprise développe des produits sous licence OS et assure sa rentabilité en facturant ses clients pour le support, la maintenance et l'installation[29]. En outre, les fonds de capital-risque investissent de plus en plus dans des *start-ups* de logiciels *open source*, et ce secteur a plutôt bénéficié de l'accélération de la numérisation induite par la pandémie de Covid-19[30].

Enfin, on constate une évolution des types de licences utilisées dans l'OS. Les licences « *copyleft* » (telle que la *General Public Licence* – GPL), dont le concept a été développé en 1985, offrent des libertés « d'exécution, de copie, de modification et de distribution du code informatique » et imposent le maintien de ces libertés dans toutes les versions dérivées du logiciel[31]. En d'autres termes, ce type de licence ne permet pas de créer des logiciels propriétaires sur la base de codes sources *copyleft*. Or, les grandes entreprises technologiques tendent à dévoyer ces principes, comme Google,

25. K. Brigham, « How Open-Source Software Took Over the World », *op. cit.*
26. D. Geer *et al.*, « Should Uncle Sam Worry about 'Foreign' Open-Source Software? Geographic Known Unknowns and Open-Source Software Security », Lawfare, 25 août 2022.
27. « Improving the Nation's Cybersecurity », *op. cit.*, p. 14.
28. « Qu'est-ce que le logiciel libre ? », GNU, non daté, disponible sur : www.gnu.org.
29. T. Herr, « Responding to and Learning From the Log4Shell Vulnerability », *op. cit.*
30. « Where Top VCs Are Investing in Open Source and Dev Tools », Tech Crunch, 5 février 2020, disponible sur : https://techcrunch.com.
31. M. O'Neil *et al.*, « Le pillage de la communauté des logiciels libres », *Le Monde diplomatique*, 20-21 janvier 2022.

qui a développé Android sur la base de Linux, mais en lui assignant une licence non *copyleft*, s'affranchissant ainsi de dévoiler les modifications du code source apportées par Google[32].

L'*open source* dans le *cloud* et les technologies émergentes

Enfin, l'*open source* est aujourd'hui intrinsèquement lié au *cloud* et joue un rôle déterminant dans les technologies émergentes (IA, *edge*, IoT). Des composants *open source* sont effectivement utilisés dans la construction d'environnements *cloud*. Si l'infrastructure n'est pas l'élément où se situe la valeur ajoutée des applications mises à disposition sur le *cloud*, l'interopérabilité offerte par l'OS en fait un élément incontournable de l'architecture du *cloud*[33]. Toutes les plateformes *cloud* tendent à converger vers Kubernetes, une technologie *open source* d'orchestration de conteneurs[34]. En retour, le *cloud* en tant que service a également modelé le développement croissant de l'*open source*[35]. Selon Kevin Xu, les platesformes *cloud* ont fondamentalement changé la façon dont les technologies *open source* sont distribuées, si bien qu'on peut presque considérer aujourd'hui le *cloud* comme « un magasin d'applications *open source*[36] ».

L'*open source* est également appelé à jouer un rôle structurant dans le développement des technologies émergentes, parmi lesquels l'IA et l'IoT. Les innovations technologiques et les nouveaux usages associés mènent en effet à une explosion des besoins en logiciels et transforment également l'écosystème de l'industrie logicielle, puisque dorénavant, tout type d'entreprise peut être impliqué dans le développement de logiciels. À titre d'exemple, il y a aujourd'hui plus de lignes de code dans une automobile que dans un avion de chasse F15[37]. Et le nombre de ces appareils « intelligents » et interconnectés ne cesse d'augmenter. Ainsi, entre 2010 et 2020, le nombre d'appareils IoT connectés a connu une augmentation de l'ordre de 1 000 % ; ils représentaient en 2020 plus de 50 % du total des appareils connectés[38]. L'IoT intègre des composants *open source* pour des fonctions telles que la gestion de flotte et les plateformes logicielles des systèmes embarqués. Pour l'Institut français de recherche informatique (Inria), à mesure que l'IoT se généralise et que la complexité des systèmes augmente, ces logiciels doivent être « polyvalents, *open source*, réutilisables sur la palette hétérogène de

32. *Ibid*.
33. Entretien, Sébastien Massart, Directeur de la stratégie, Dassault Systèmes, 23 juin 2022.
34. K. Xu, « Open Source in China: The Trends », Interconnected, 14 mai 2020, disponible sur : https://interconnected.blog.
35. « The Economic and Social Impact of Software », *op. cit.*
36. K. Xu, « *Open Source* in China: The Trends », *op. cit.*
37. K. Brigham, « How Open-Source Software Took Over the World », *op. cit.*
38. « Défis sociétaux et domaines de recherche scientifique pour l'Internet des Objets (IoT) », Livre blanc n° 5, Inria, 2021, p. 17.

matériels et de fournisseurs, et capables d'implémenter un ensemble de normes et d'interfaces de programmation (API) courantes[39] ».

En outre, l'IA ainsi que l'IoT, et plus généralement les logiciels embarqués, posent des risques particuliers en matière de sécurité des systèmes et des personnes, comme évoqué plus haut. Dès lors, selon l'Inria :

> « pour les États, le défi consiste à s'efforcer d'être le moins dépendant possible de solutions techniques susceptibles d'être utilisées de manière hostile[40] ».

Par ailleurs, l'IA et l'IoT posent des défis en termes d'éthique. L'*open source* peut alors être vu comme un moyen de superviser les algorithmes. Pour ce qui est de l'IA, un rapport du Parlement européen pointait en 2019 la nécessité d'inclure le public dans le processus de développement de l'IA et, pour se faire, de « publier en *open source* tous les algorithmes, outils et technologies financés ou co-fondés par le public » et de faciliter l'audit des codes sources[41]. Le rapport souligne toutefois que la transparence des codes sources n'empêche pas d'éventuels biais dans les données, et reconnaît que la divulgation du code source pourrait potentiellement conduire à une utilisation abusive et à la manipulation des algorithmes[42].

Victime de son succès ? Défis et risques de l'*open source*

Enjeux de cybersécurité

Comme tout logiciel, les logiciels *open source* présentent des enjeux spécifiques de cybersécurité, principalement du fait de leur caractère ubiquitaire : comme souligné en introduction, environ 80 % des logiciels contiennent des composants *open source*. Il y a débat sur la question de savoir si l'OS est plus sécurisé que les logiciels propriétaire, un argument en faveur étant que l'accessibilité des codes ouverts multiplie les chances d'identifier les failles[43], quand l'argument d'opposition est que la très grande quantité de lignes de codes OS présentes dans les logiciels peut rendre difficile leur examen[44].

Deux failles de sécurité majeures ont souligné la nécessité d'assurer la cybersécurité des briques OS : celle dite de Heartbleed en 2014 et celle baptisée Log4Shell en décembre 2021. La faille de sécurité Heartbleed provenait d'une erreur dans le code d'OpenSSL, une bibliothèque d'outils de

39. *Ibid.*, p. 95.
40. *Ibid.*, p. 24.
41. « REPORT on a Comprehensive European Industrial Policy on Artificial Intelligence and Robotics », A8-0019/2019, Parlement européen, 30 janvier 2019, p. 45 et 18, disponible sur : www.europarl.europa.eu.
42. *Ibid.*, p. 26.
43. « The Open Source Software Security Mobilization Plan », *op. cit.*, p. 3.
44. « Open Source and Commercial Software », *op. cit.*

chiffrement. L'erreur, présente depuis 2012 n'a été découverte qu'en mars 2014 par l'équipe de sécurité de Google et par des ingénieurs finlandais. L'exploitation de cette faille pouvait permettre d'exposer des contenus cryptés tels que des noms d'utilisateurs, mots de passe, des clés privées et des données échangées *via* ces certificats[45]. OpenSSL est utilisé par environ deux tiers des sites web, dont des sites bancaires et de e-commerce, et des réseaux sociaux. De sorte que, bien qu'il soit difficile d'estimer dans quelle mesure cette faille a été exploitée par des acteurs mal intentionnés, celle-ci a été qualifiée par de nombreux experts comme une des pires failles dans l'histoire de l'internet[46].

D'autres failles peuvent être introduites volontairement par des développeurs mal intentionnés. En 2018, un contributeur GitHub a introduit un module dans une bibliothèque de code utilisée pour les portefeuilles de bitcoins, et s'est servi de ce module pour introduire une *backdoor* et rediriger les fonds vers un serveur localisé à Kuala Lumpur[47].

Plus récemment, en décembre 2021, une faille a touché le composant de logiciel de journalisation Log4J (qui enregistre les activités d'une application), utilisé dans de nombreuses applications et sites web utilisant le langage Java. Celle-ci a été identifiée par un ingénieur de l'entreprise chinoise Alibaba et dévoilée par la Fondation Apache, qui héberge le logiciel Log4J. Cette faille était susceptible de permettre à un attaquant de prendre le contrôle d'une application, voire d'un système d'information. Cette fois, l'exploitation active de la vulnérabilité a été avérée[48] et attribuée à « plusieurs groupes d'attaquants, aussi bien étatiques ou proches d'États », opérant en Russie, en Chine, en Iran et en Corée du Nord, ainsi que des cybercriminels (*botnets* et opérateurs de rançongiciels[49]). La Russie aurait notamment exploité cette faille pour mener des attaques cyber contre l'Ukraine[50]. À son tour, Log4Shell a été qualifiée de « l'un des risques de cybersécurité les plus graves et les plus étendus jamais vus[51] ». Les développeurs du projet ont corrigé l'erreur de code dans les deux semaines suivant l'identification de la faille[52]. Cependant, pour corriger la vulnérabilité, les versions précédentes de Log4J déjà installées doivent être mises à jour, y compris dans de nombreux

45. « The Heartbleed Bug », mis à jour le 6 mars 2020, disponible sur : https://heartbleed.com.
46. L. Ronfaut et B. Ferran, « "Heartbleed" : la faille qui frappe le cœur de la sécurité sur Internet », *Le Figaro*, 11 avril 2014.
47. D. Goodin, « Widely Used Open Source Software Contained Bitcoin-Stealing Backdoor », Ars Technica, 26 novembre 2018, disponible sur : https://arstechnica.com.
48. « L'ANSSI alerte sur la faille de sécurité Log4Shell », Communiqué de presse, ANSSI, 16 décembre 2021, disponible sur : www.ssi.gouv.fr.
49. « Log4j : "Les experts s'accordent pour dire que la faille de sécurité est réellement inquiétante" », *Le Monde*, 16 décembre 2021. Le principal risque se concentre sur les serveurs Web. Beaucoup d'organisations peuvent utiliser des outils Java et cette bibliothèque Log4J sans être nécessairement au courant, par exemple si elles ne connaissent pas dans le détail tous les outils présents sur leur réseau.
50. G. Peters, « Responding to and Learning from the Log4Shell Vulnerability: Opening Statement », Committee on Homeland Security and Government Affairs, Sénat des États-Unis, 8 février 2022.
51. *Ibid.* [Nous traduisons.]
52. D. Nalley, « Responding to and Learning From the Log4Shell Vulnerability », *op. cit.*

cas où des utilisateurs ne savaient pas que ce code était présent dans leurs propres produits[53].

Enfin, les attaques contre les logiciels *open source* évoluent. L'année 2021 a vu une très forte augmentation, estimée à 650 %, par rapport à 2020[54]. Le risque provient notamment d'une nouvelle génération d'attaques, visant à faire en sorte que les développeurs de logiciels téléchargent des programmes malveillants qui prennent le nom de fichiers légitimes, de façon à infiltrer la chaîne d'approvisionnement logicielle en amont.

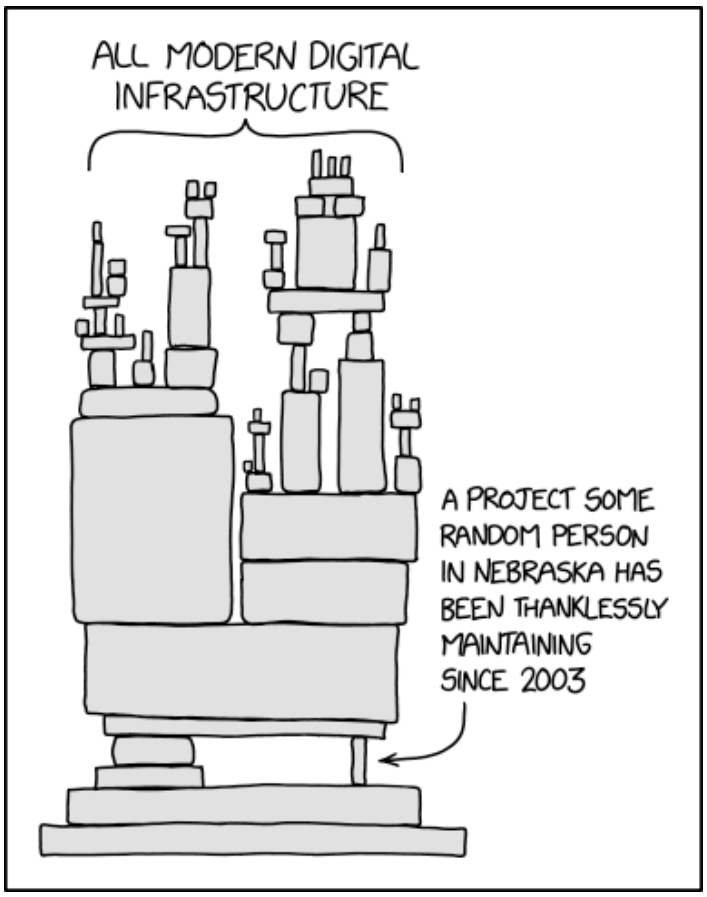
Enjeux de pérennité économique et technique

Comme on l'a vu dans la partie précédente, les logiciels propriétaires comportent eux aussi des failles de sécurité, avec des conséquences tout aussi délétères. Dès lors, les opinions s'accordent sur le fait que Log4Shell et Heartbleed ne représentent pas un échec de l'*open source* en tant que tel. Cela étant, outre leurs conséquences néfastes en termes de sécurité, ces incidents ont eu pour effet de mettre en lumière la précarité économique du modèle des logiciels *open source*. Bien que certains produits deviennent populaires au point de devenir structurants pour l'architecture numérique globale, ces produits reposent pour une large part sur des contributions volontaires de développeurs, qui écrivent, maintiennent et corrigent des lignes de code bénévolement. Notons que ce n'est cependant pas le cas de l'ensemble de l'OS, puisqu'il y a aujourd'hui une profusion de dépôts de code, avec des mainteneurs rémunérés ou même à temps plein[55].

Dans le cas d'OpenSSL, l'équipe de développeurs était très réduite et les donations commençaient à se raréfier[56]. Suite à l'incident Heartbleed, la fondation Linux s'est engagée à soutenir financièrement OpenSSL. Cette question du sous-financement de l'OS, qui avait ainsi été posée dès 2014, est revenue en force suite à Log4Shell, au point que les États se mobilisent, comme nous l'examinons dans la troisième partie de l'étude. En janvier 2022, un programmeur a lui-même saboté le code de projets sur lesquels il travaillait pour dénoncer la précarité du monde de l'OS[57].

53. R. Portman, « Responding to and Learning From the Log4Shell Vulnerability: Opening Statement », Committee on Homeland Security and Government Affairs, Sénat des États-Unis, 8 février 2022.
54. « État de la chaine logistique logicielle », *op. cit.*, p. 4.
55. T. Herr, « Responding to and Learning From the Log4Shell Vulnerability », *op. cit.*
56. K. Brigham, « How Open-Source Software Took Over the World », *op. cit.*
57. A. Horn, « Un développeur sabote son projet *open source* et paralyse des milliers d'applications », Numerama, 10 janvier 2022, disponible sur : www.numerama.com.

Dépendances[58]



Source : « Dependencies », XKCD, 16 août 2020, disponible sur : https://imgs.xkcd.com.

Par ailleurs, la précarité du modèle actuel ne reflète pas la valeur économique produite par les logiciels *open source*. Selon un rapport de 2021, qui examine l'impact des logiciels et matériels *open source* sur l'économie de l'Union européenne (UE), cette contribution est largement sous-estimée. Le rapport estime un impact positif de l'OS sur l'économie de l'ordre de 65-95 milliards d'euros, pour un investissement annuel (en 2018) d'un milliard d'euros au sein de l'UE. Le rapport ajoute qu'une augmentation de 10 % en contribution dans l'OS générerait une augmentation du produit intérieur brut (PIB) de l'ordre de 0,4 % à 0,6 %[59].

Pour ces raisons, économiques et de sécurité, les appels à trouver des solutions pérennes au financement de l'*open source* se sont multipliés. Selon l'Office de l'Union européenne pour la propriété intellectuelle (EUIPO), le système ne peut pas être maintenu sans un mécanisme récompensant les

58. L'image décrit « Toute l'infrastructure numérique morderne » ; la flèche point vers « un projet qu'un individu quelconque dans le Nebraska entretient de façon ingrate depuis 2003 ».
59. « Towards a Sovereign Digital Infrastructure of Commons », European Working Team on Digital Commons, juin 2022, p. 20.

contributions au *pool* commun de connaissances[60]. La plateforme collaborative GitHub (cf. *infra*) a ainsi lancé un programme de parrainage pour permettre aux développeurs de recevoir des donations récurrentes pour leur travail[61]. Comme nous l'expliquons dans la partie suivante, la tendance actuelle est plutôt celle d'une implication de plus en plus importante des grandes entreprises de la tech dans le développement de l'OS, y compris par le rachat de plateformes de dépôt. Si elles contribuent à la bonne santé économique de l'écosystème, cette tendance peut émaner d'intérêts et de pratiques qui vont à l'encontre des principes même de l'*open source*.

Enfin, la centralisation croissante de l'*open source* autour de certains acteurs privés peut aussi devenir une faiblesse. D'une part, dans les cas où de grandes entreprises sont directement impliquées pour développer des projets, il y a un manque de diversité organisationnelle en termes de contributeurs à ces mêmes projets, et un risque qu'un abandon de projet par l'entreprise n'entraîne sa perte pour l'ensemble de la communauté *open source*[62]. D'autre part, la centralisation de l'écosystème autour de plateformes et l'implication croissante des États peuvent entraîner des risques de changements de statuts ou de lois rendant inaccessibles des dépôts, codes, ou licences aux utilisateurs de pays spécifiques. Dans un exemple récent, les contributeurs russes travaillant pour des entreprises russes sanctionnées dans le contexte de la guerre en Ukraine ont vu leurs comptes GitHub suspendus[63].

60. « Open Source Software in the European Union », European Union Intellectual Property Office, 2020, p. 25.
61. K. Brigham, « How Open-Source Software Took Over the World », *op. cit.*
62. G. Link, « Building and Supporting Open Source Communities Through Metrics », Open Source Summit Europe 2022, Dublin, 13 septembre 2022.
63. « GitHub Blocks Accounts of Two Large Russian Banks Amid US Sanctions », HackRead, 16 avril 2022, disponible sur : www.hackread.com.

Évolution de l'écosystème *open source* : l'influence croissante des *Big Tech*

L'écosystème mondial de l'*open source* repose sur les contributions de développeurs, qu'ils soient des individus, des communautés ou des entreprises. Cet écosystème est structuré autour d'acteurs qui hébergent les projets, organisent et rendent accessibles ces contributions aux codes sources, réunissent et mettent en réseau ces acteurs, rétribuent les contributeurs, et promeuvent l'*open source*. Trois types d'organisations, de natures diverses, jouent des rôles structurants et évolutifs : les fondations, les dépôts de codes et plateformes collaboratives, et les grandes entreprises technologiques (les « *Big Tech* »). Ces dernières jouent un rôle croissant, puisqu'elles s'impliquent à la fois directement dans des projets *open source*, et investissent financièrement dans les fondations et les dépôts de code. Cela peut avoir des effets potentiellement délétères sur le modèle *open source* lui-même, du fait de leurs intérêts commerciaux et de risques de captation.

Les facilitateurs de l'*open source*

Les fondations

Les fondations jouent un rôle prépondérant dans la gouvernance, la structuration et l'animation de l'écosystème OS – en d'autres termes, elles permettent la collaboration. Elles ont, plus précisément, plusieurs fonctions : partage d'information au sujet de l'OS auprès des entreprises privées ; hébergement neutre pour les actifs communs, de façon à ce que personne individuellement « ne détienne les clés du château » ; personnalité juridique capable de recevoir de l'argent pour des projets ; infrastructure de projet (serveurs, listes de diffusions, etc.)[64]. Les fondations ont des missions plus ou moins larges, selon qu'elles se concentrent sur un langage de programmation, un projet en particulier (tel que la Linux Foundation, à ses débuts, pour le projet Linux lui-même) ou un domaine (par exemple, infrastructure ou *cloud*), ou qu'elles sont généralistes (telles que la Linux Foundation aujourd'hui).

64. T. Carrez, « The Role of Foundations », Open Source Summit Europe 2022, Dublin, 15 septembre 2022.

L'écosystème mondial de l'OS est aujourd'hui largement structuré par un petit nombre de fondations principalement américaines, dont on peut citer les deux principales : Linux Foundation (LF) et Apache Software Foundation. La LF a été créée en 2007 avec l'objectif de promouvoir Linux et, de plus en plus, de développer des projets d'intérêt commercial dans des domaines variés. Sa mission aujourd'hui revient à rassembler des communautés et des investissements d'ampleur, faciliter l'innovation, accélérer la valorisation des codes, s'assurer que les codes sont écrits de façon sécurisée et aider à la gestion de la propriété intellectuelle[65]. Actuellement, plus de 100 projets relèvent de la LF, dans des secteurs tels que l'IA, les véhicules autonomes, les réseaux ou la sécurité[66].

Linux Foundation compte aujourd'hui 200 employés et 1 000 membres – des entreprises qui utilisent des technologies *open source* dans leurs outils informatiques ou dans leurs produits et services[67]. Les revenus de Linux Foundation, à hauteur de 124 millions de dollars en 2019 (en croissance rapide, puisqu'en 2011 son chiffre d'affaires était de 15,6 millions de dollars) proviennent principalement des conférences organisées par la fondation, de services payants, ainsi que des cotisations des entreprises membres, et d'activités de formations[68]. Linux est impliquée dans un nombre croissant de projets d'envergure, et notamment le soutien à d'autres fondations voir la création de fondations qui sont intégrées en son sein, comme l'Open Source Security Foundation (OSSF), créée en 2020, ou encore les fondations PyTorch (apprentissage machine) et OpenWallet (porte-monnaie électronique), qui l'ont rejointe en septembre 2022. La justification pour que PyTorch, le logiciel développé par Facebook, passe sous la responsabilité de la fondation Linux est que cette dernière dispose des capacités nécessaires pour gérer ce projet auquel 2 400 contributeurs participent[69]. Si LF offre une grande visibilité aux projets qu'elle soutient, elle est aussi accusée de faire le jeu des grandes entreprises de la tech, aux dépens de l'esprit communautaire des débuts[70]. D'aucuns la qualifient même de « consortium industriel qui organise les discussions entre [les GAFAM] [71] ».

Apache est la seconde principale fondation américaine. Elle n'a pas d'employés, mais compte 6 000 volontaires et un budget d'environ 2 millions de dollars. Le projet Apache httpd, hébergé chez la Apache Foundation, est un serveur HTTP[72] qui héberge un tiers des sites web dans le monde. La

65. T. Krazir, « The Linux Foundation Became a Force in Enterprise Tech. Is That a Problem? », Protocol, 3 septembre 2020, disponible sur : www.protocol.com.
66. *Ibid*.
67. Linux Foundation, « Members », *op. cit*.
68. « Nonprofit Explorer: The Linux Foundation », ProPublica, non daté, disponible sur : https://projects.propublica.org.
69. I. Haddad, « Keynote », Open Source Summit Europe 2022, Dublin, 14 septembre 2022.
70. T. Krazir, « The Linux Foundation Became a Force in Enterprise Tech », *op. cit*.
71. D. Sabattier et L. Muselli, « Le logiciel libre, pillé par les Big Tech ? », verbatim, 1er février 2022, disponible sur : www.librealire.org.
72. HTTP : hypertext transfer protocol.

Fondation Apache, a été créée en 1999 pour héberger ce projet et, depuis, environ 200 autres projets[73]. Contrairement à LF, les membres de la fondation Apache sont des individus nommés selon un principe méritocratique, pour leur implication dans des projets de la fondation[74]. Cela étant, les principaux sponsors de la fondation incluent également les principales grandes entreprises de la tech (Microsoft, Apple, AWS, Huawei, etc.).

De nombreuses autres fondations plus petites ou plus spécialisées existent. Comme on le verra dans la partie suivante, l'écosystème se développe de plus en plus en Europe, notamment avec la relocalisation sur le continent des fondations Eclipse et RISC-V, et la création en septembre 2022 d'une branche Europe de la fondation Linux[75].

Plateformes de développement collaboratif et dépôts de code

Outre les fondations, l'écosystème *open source* mondial se structure de plus en plus autour de plateformes de développement collaboratif qui hébergent des dépôts de code. À mesure que l'usage de l'OS s'est généralisé, les communautés de programmeurs se sont organisées et les pratiques se sont standardisées autour de sites qui hébergent des projets de logiciels et permettent d'alimenter et gérer collectivement les codes source.

GitHub est la principale plateforme. Elle compte aujourd'hui plus de 60 millions de contributeurs dans le monde entier[76], contre 40 millions en 2019[77]. L'entreprise, fondée en 2008 à San Francisco, a gagné en popularité à mesure que les grandes entreprises de la tech – dont Google, Facebook et Twitter – ont choisi d'y héberger les codes de leurs projets *open source*, et fermé leurs propres services d'hébergement de codes source[78]. Microsoft a fait de même, avant de racheter GitHub pour 7,5 milliards de dollars en 2018. La qualité, la simplicité et la gratuité de l'interface ont également conduit la fondation Apache à migrer tous ses projets vers GitHub[79]. Elle est également la plateforme recommandée par LF[80].

73. K. Finley, « For Open Source, It's All About GitHub Now », Wired, 30 avril 2019, disponible sur : www.wired.com.
74. Apache Software Foundation, « Members », non daté, disponible sur : www.apache.org.
75. Eclipse est une fondation principalement consacrée à des projets de coopération industrielle dans des domaines tels que le *cloud*, l'*edge*, l'IA, les véhicules connectés, les télécommunications et l'IoT. Pour sa part, RISC-V est une architecture ouverte de jeu d'instructions pour la construction d'un processeur, développée à l'origine à l'université de Californie et disponible en *open source*.
76. GitHub, « Users », non daté, disponible sur : https://github.com.
77. K. Brigham, « How Open-Source Software Took Over the World », *op. cit.*
78. K. Finley, « For Open Source, It's All About GitHub Now », *op. cit.*
79. « The Apache Software Foundation Expands Infrastructure with GitHub Integration », The Apache Software Foundation Blog, 29 avril 2019, disponible sur : https://news.apache.org.
80. « Starting an Open Source Project », The Linux Foundation, non daté, disponible sur : www.linuxfoundation.org.

Pour les contributeurs, le fait que la plupart des projets soient hébergés sur GitHub présente certains avantages. La plateforme leur permet de centraliser leurs contributions, de se constituer un curriculum vitae et un réseau, et de recevoir des parrainages[81]. En outre, GitHub remplit aujourd'hui plusieurs des fonctions qui sont traditionnellement celles des fondations (infrastructure de projets, conseil, par exemple concernant les choix de licence, gestion des paiements faits aux contributeurs…[82]). Cependant, elle n'en a pas le statut. Après le rachat par Microsoft, nombre de développeurs auraient préféré migrer vers d'autres plateformes de dépôt, mais c'est devenu difficile du fait de la centralité acquise par GitHub[83]. Une autre critique adressée à la plateforme est que les plus gros projets hébergés sont soit développés, soit gérés par des grandes entreprises – individuellement ou réunies en consortia. Résultat, la gouvernance de ces projets n'est pas entre les mains des développeurs, mais dérive d'intérêts industriels[84].

L'implication croissante des grandes entreprises technologiques

Financement, rachats et contributions

On l'a vu, le secteur privé est devenu un acteur clé du financement et de la gouvernance de l'écosystème OS. Les grandes entreprises du numérique, en particulier, prêtent une grande attention à la vitalité des communautés qui développent et maintiennent ces composants, et investissent des ressources significatives dans les communautés OS – soit pour qu'ils assurent la continuité de l'infrastructure logicielle de base, soit pour développer leurs propres projets *open source*[85]. Ainsi, « dans l'*open source*, de féroces rivaux commerciaux collaborent tous les jours[86] ».

Les grandes entreprises de la tech sont, pour la plupart, membres ou sponsor des grandes fondations, qu'ils financent : pour être membre platine de Linux Foundation, il faut compter 500 000 dollars annuels. C'est le cas, entre autres, de Microsoft, Huawei, Ericsson, Intel, et Meta[87]. Le soutien à l'OS passe également par la mise à disposition de ressources techniques auprès des communautés *open source*. Ainsi, après être devenue sponsor

81. K. Finley, « For Open Source, It's All About GitHub Now », *op. cit.* ; GitHub, « Sponsors », non daté, disponible sur : https://github.com.
82. T. Carrez, « The Role of Foundations », *op. cit.*
83. M. O'Neil *et al.*, *The Coproduction of Open Source Software by Volunteers and Big Tech Firms*, News & Media Research Centre, Université de Canberra, 2021, p. 14.
84. *Ibid.*, p. 23.
85. « Towards a Sovereign Digital Infrastructure », *op. cit.*, p. 23.
86. K. Brigham, « How Open-Source Software Took Over the World », *op. cit.*
87. Linux Foundation, « Members », non daté, disponible sur : www.linuxfoundation.org.

platine de l'Apache Software Foundation, Amazon a annoncé apporter aussi un soutien aux infrastructures techniques sur lesquelles opère la fondation[88].

Les entreprises de la tech s'impliquent aussi dans l'*open source* par le biais de leurs développeurs, qui contribuent « massivement » aux projets hébergés sur GitHub[89]. Les *Big Tech* jouent un rôle disproportionné par rapport aux autres acteurs privés, selon l'index de contribution à l'*open source* qui liste les entreprises en fonction du volume de contributions de leurs employés sur GitHub : Microsoft, Google et Red Hat sont les trois premiers contributeurs[90]. Ainsi, on estime que seul 15 % du code Linux est encore produit par des bénévoles[91].

Dans certains cas, les *Big Tech* s'impliquent directement dans la structuration et la gestion de l'écosystème mondial de l'OS, par le rachat d'entreprises ou dépôts de code. On a évoqué le rachat de GitHub par Microsoft. La volonté de maximiser cet investissement explique que Microsoft soit de loin l'entreprise dont les employés contribuent le plus à la plateforme[92]. IBM, pour sa part, a fait en 2018 sa plus grosse acquisition en rachetant Red Hat (13 000 salariés, 2,4 milliards de dollars de chiffre d'affaires) pour 38 milliards de dollars – soit la troisième plus importante acquisition de l'histoire de la tech aux États-Unis[93].

Motivations des grandes entreprises et effets sur l'écosystème

Quelles sont les motivations des *Big Tech* pour développer et rendre disponible leurs logiciels sous licence *open source* ? Cette pratique (l'*open-sourcing*) peut découler des obligations afférentes à certaines licences, si le projet a été développé lui-même sur une base *open source*. Mais, dans une autre perspective, développer et/ou rendre accessible en *open source* des projets que les entreprises auraient pu mener en interne, est un choix. Ce choix des entreprises, et notamment des géants de la tech, de recourir à l'*open source* pour développer leurs logiciels n'est pas évident de prime abord. D'ailleurs, toutes les entreprises n'ont pas recours à l'*open-sourcing* – celui-ci est fonction de la stratégie de l'entreprise en matière de propriété intellectuelle, de sa culture et de son rapport à l'innovation ouverte, et de leur degré d'information au sujet de l'*open source*, de son fonctionnement et de

88. Z. Bhorat, « Supporting the Apache Software Foundation », AWS Open Source Blog, 28 janvier 2019, disponible sur : https://aws.amazon.com.
89. M. O'Neil *et al.*, *The Coproduction of Open Source Software*, *op. cit.*, p. 29.
90. Données datées de septembre 2022. Open Source Contributor Index, disponible sur : https://opensourceindex.io.
91. L. Muselli, « Les employés des GAFAM, plus gros contributeurs du logiciel libre », Polytechnique Insights, 8 juin 2021, disponible sur : www.polytechnique-insights.com.
92. M. O'Neil *et al.*, *The Coproduction of Open source Software*, *op. cit.*, p. 21.
93. « Enquête sur l'état des lieux de la filière *open source* en France 2020/2021 », Rapport d'étude, Will Strategy, 17 mai 2021, p. 8.

ses acteurs[94]. En effet, les entreprises doivent évaluer le bénéfice de partager leurs codes et leurs connaissances, à l'aune des risques : perdre en contrôle et en capacité de différenciation vis-à-vis des communautés OS et des concurrents potentiels[95]. Toutefois, les avantages de l'OS sont en fait multiples, et dans la balance, compensent largement ces risques, c'est pourquoi l'*open-sourcing* tend à se généraliser.

Économie de ressources et accélération de l'innovation

Le recours à l'*open source* permet d'accélérer le processus et baisser les coûts de développement de nouveaux logiciels. D'une part, l'utilisation de composants *open source* existants permet de ne pas avoir à recommencer à zéro et « réinventer la roue » lorsque les entreprises développent leurs produits[96]. C'est la motivation principale et originale du recours à l'*open source*[97]. Mais puisque l'*open source* est continuellement alimenté par de nouveaux projets, y recourir permet également d'accéder à de nouvelles technologies qui peuvent ensuite être adaptées de façon plus fine et performante en interne, par les entreprises[98].

Cette motivation de recourir à l'*open source* pour accélérer le développement de logiciel et innover ne concerne pas uniquement les entreprises du numérique et éditeurs de logiciels, mais concerne des entreprises de tous les secteurs de l'industrie puisque, comme on l'a évoqué en introduction, les logiciels se trouvent désormais partout. Ainsi, des grands groupes industriels et de grande distribution, comme Walmart, Exxon, ou Mercedes Benz, le font pour cette même raison[99]. À titre d'exemple, dans l'automobile, de grands groupes travaillent de concert au sein de la Fondation Eclipse dans le cadre d'un groupe de travail sur le véhicule défini par le logiciel (« *software defined vehicle working group* »), dans le but de développer des modules de logiciels ouverts et interopérables pour les véhicules autonomes[100].

En plus de gagner du temps et d'accéder à l'innovation, le fait de recourir à l'*open source* permet de réduire les coûts de main-d'œuvre, en économisant le temps de travail des développeurs de l'entreprise. En l'absence de coûts de licence et d'abonnements, des économies sont également réalisées sur les coûts d'utilisation à long terme des logiciels, par comparaison avec les

94. K. Blind *et al.*, « The Impact of Open Source Software and Hardware on Technological Independence, Competitiveness and Innovation in the EU Economy: Final Study Report », Commission européenne, 2021, p. 37.
95. « Open Source Software », European Union Intellectual Property Office, *op. cit.*, p. 26.
96. R. Portman, « Responding to and Learning From the Log4Shell Vulnerability », *op. cit.*
97. « Open Source Software », European Union Intellectual Property Office, *op. cit.*, p. 25.
98. Entretien, Sébastien Massart, Directeur de la stratégie, Dassault Systèmes, 23 juin 2022.
99. K. Brigham, « How Open-Source Software Took Over the World », *op. cit.*
100. W. Gehring, « Drive Your Business Through OS Sponsorship », Open Source Summit Europe 2022, Dublin, 13 septembre 2022 ; Eclipse Foundation, « Software Defined Vehicle », non daté, disponible sur : https://sdv.eclipse.org.

solutions propriétaires[101]. Ce faisant, l'*open source* abaisse les barrières à l'entrée pour les entreprises désireuses d'entrer sur le marché du développement de logiciel[102]. En retour, des solutions *open source* développées par des entreprises peuvent également être monétisées, en facturant les services de support, en développant des versions OS et commerciales, etc.[103].

Cybersécurité et visibilité sur les chaînes d'approvisionnement

On l'a dit, la quasi-totalité des logiciels contiennent des composants OS comme dépendances externes. La connaissance des composants est nécessaire pour respecter les obligations légales relatives aux différents composants de ces logiciels, mais, de plus en plus, la motivation relève de la cybersécurité : des composants *open source* (comme de toute dépendance logicielle) peuvent provenir des vulnérabilités, qui peuvent par ricochet affecter les logiciels propriétaires développés par les entreprises[104]. Ces dernières ont donc tout intérêt à développer une connaissance ou à contribuer à la maintenance des éléments présents dans leurs chaînes d'approvisionnement[105].

Pour pallier ces risques, les grandes entreprises de la tech s'investissent directement dans le renforcement de la sécurité de l'*open source*. À titre d'exemple, Google a pris plusieurs mesures suite à la faille Log4Shell, dont un engagement de 100 millions de dollars pour soutenir des organisations dédiées, telles que l'Open Source Security Foundation[106]. Google a également proposé la mise en place d'une organisation qui servirait de place de marché pour mettre des mainteneurs volontaires (travaillant pour des entreprises de la tech) au service de la maintenance des projets OS les plus critiques[107]. Google a d'ailleurs créé en mai 2022 une équipe interne dédiée à cette mission[108]. Enfin, l'entreprise a lancé en août 2022 un programme dans le cadre duquel elle va rétribuer des chercheurs pour identifier des bogues dans les dernières versions des logiciels *open source* de Google[109]. Le montant de la rémunération pourra aller jusqu'à 30 000 dollars par faille, pour des failles trouvées dans les programmes phares de l'entreprise. Pour sa part, Mercedes-Benz a choisi de soutenir financièrement *via* GitHub les

101. « Open Source Software », European Union Intellectual Property Office, *op. cit.*, p. 69.
102. *Ibid.*
103. K. Brigham, « How Open-Source Software Took Over the World », *op. cit.*
104. R. Portman, « Responding to and Learning From the Log4Shell Vulnerability », *op. cit.*
105. « The Open Source Software Security Mobilization Plan », *op. cit.*, p. 4.
106. K. Walker, « Making Open Source Software Safer and More Secure », Google, 13 janvier 2022, disponible sur : www.blog.google.
107. *Ibid.*
108. J. Lausson, « Google lance une petite équipe spécialisée dans la mise à jour du logiciel libre critique », Numérama, 16 mai 2022, disponible sur : www.numerama.com.
109. S. Gatlan, « Google Launches Open-Source Software Bug Bounty Program », BleepingComputer, 30 août 2022, disponible sur : www.bleepingcomputer.com.

contributeurs aux projets *open source* que l'entreprise automobile considère comme les plus importants[110].

Encourager l'adoption des produits

Si les problématiques de coût et de visibilité sur les chaînes d'approvisionnement ont longtemps été prépondérantes dans le choix de recourir à l'OS, les entreprises de la tech ont aujourd'hui des motivations plus stratégiques lorsqu'elles choisissent de déployer certains projets en *open source*. L'*open-sourcing* vise notamment à encourager l'adoption de leurs produits. Ces motivations sont assumées par les acteurs privés : « Nous n'avons pas [eu recours à l'*open source*] pour recevoir l'aide de la communauté, pour améliorer le produit. On l'a fait comme stratégie de freemium, pour encourager l'adoption », explique ainsi le directeur de l'entreprise qui développe le logiciel de gestion de base de données MongoDB[111].

Encourager l'adoption… voire créer des standards : développer une solution en *open source* permet de créer des effets de réseaux, de maximiser les chances qu'une solution soit utilisée par d'autres, et/ou d'affaiblir la position d'un autre acteur déjà dominant sur un segment de marché[112]. C'est ainsi qu'on peut expliquer pourquoi Apple a ouvert Swift[113], et Meta, PyTorch. Passer des projets propriétaires en *open source* encourage les ingénieurs à développer des applications sur la base de ces technologies, faisant de celles-ci des standards, et accroissant la valeur et l'adhésion aux plateformes Apple et Meta, respectivement[114]. Grâce à cette stratégie, PyTorch est déjà considéré comme « un leader du marché [de l'IA], avec plus de 150 000 projets construits sur GitHub avec PyTorch[115] ». Suite à sa constitution en fondation, PyTorch va même aller jusqu'à offrir des formations gratuites à des cadres d'entreprise, pour qu'ils se familiarisent avec l'outil[116].

Cet intérêt des entreprises à développer des produits qui soient accrocheurs et le fait qu'elles ont comme intérêt sous-jacent l'enfermement propriétaire (*vendor lock-in*) vont à l'encontre des principes de base de l'*open source* et de l'ambition d'interopérabilité[117]. Loin d'empêcher que les

110. W. Gehring, « Drive Your Business Through OS Sponsorship », *op. cit.*
111. « *We didn't open source it to get help from the community, to make the product better. We open sourced as a freemium strategy ; to drive adoption* ». Cité par D. Berkholz, « The Business of Open Source: How Big Money, Investors and Greed Are Changing OS Forever », Open Source Summit Europe 2022, Dublin, 14 septembre 2022.
112. « Open Source Software », European Union Intellectual Property Office, *op. cit.*, p. 25.
113. Swift est le langage de programmation mis au point par Apple pour développer des applications compatibles avec les produits Apple (iOS, Mac…).
114. K. Xu, « Open Source in China: The Game », Interconnected, 10 mai 2020, disponible sur : https://interconnected.blog.
115. S. Vaughan-Nichols, « Machine learning : PyTorch de Facebook passe sous le giron de la Fondation Linux », ZDNet, 16 septembre 2022, disponible sur : www.zdnet.fr.
116. I. Haddad, « Keynote », *op. cit.*
117. D. Berkholz, « The Business of Open Source », *op. cit.* ; K. Xu, « Open Source in China: The Game », *op. cit.*

entreprises, développeurs et utilisateurs de solutions logicielles ne se retrouvent captifs de certains fournisseurs, le recours à l'*open source* par les grandes plateformes peut, finalement, préparer et faciliter cette captivité de façon pernicieuse.

Développer la main-d'œuvre et identifier les talents

Une autre motivation du secteur privé concerne l'identification de développeurs qui, ayant démontré leurs capacités et leur implication sur des projets *open source*, peuvent ensuite être recrutés par les entreprises[118]. Ainsi les entreprises scannent les profils des contributeurs, notamment ceux qui contribuent à leurs projets et ont développé des compétences spécifiques qui peuvent leur être utiles[119].

Enjeux de réputation

Enfin, l'investissement dans l'OS peut être une stratégie marketing et réputationnelle, qui peut confiner à un « *open source washing* ». Comme résumé par une représentante de l'investisseur Zetta Venture Partners : « la beauté de l'*open source*, du point de vue de l'investisseur, c'est la distribution – c'est la contribution au marketing, pas à la [R&D][120] ». Vis-à-vis des autres entreprises et du public, l'*open-sourcing* peut venir contrebalancer les perceptions négatives envers les acteurs dominants, en ce qu'il peut donner l'assurance que l'entreprise n'exercera pas à l'avenir un contrôle excessif sur un logiciel donné[121].

Un autre enjeu, notamment vis-à-vis des pouvoirs publics, relève de la transparence des algorithmes. Dans le cadre de son « engagement pour la science ouverte », Meta a annoncé en mai 2022 le partage du programme Open Pretrained Transformer (OPT-175B), avec ses 175 milliards de paramètres entraînés sur des jeux de données publiques. Le but de Meta est de faciliter « l'engagement communautaire dans la compréhension de cette nouvelle technologie fondamentale[122] ». Malgré l'effort apparent de transparence – le modèle OPT-175B de Meta est disponible sur demande, à des fins de recherche – ce programme ne dit rien des algorithmes utilisés par Meta sur ses applications Facebook et Instagram[123].

118. « Open Source Software », European Union Intellectual Property Office, *op. cit.*, p. 25 ; Entretien, Bruno Sportisse, P.-D.G. d'Inria, 13 juillet 2022.
119. K. Xu, « Open Source in China: The Game », *op. cit.* ; Entretien, Bruno Sportisse, P.-D.G. d'Inria, 13 juillet 2022.
120. Citée par D. Berkholz, « The Business of Open Source », *op. cit.*
121. « Open Source Software », European Union Intellectual Property Office, *op. cit.*, p. 25.
122. S. Zhang *et al.*, « Democratizing Access to Large-Scale Language Models With OPT-175B », Meta AI, 3 mai 2022, disponible sur : https://ai.facebook.com.
123. M. Heikkilä, « Inside a Radical New Project to Democratize AI », *MIT Technology Review*, 12 juillet 2022 ; Protocol Enterprise, « Facebook Opens an Algorithm; No, Not That One », 3 mai 2022, disponible sur : www.protocol.com.

Il y a donc une tension entre cette façade d'altruisme et la volonté de créer de la valeur et de l'adhésion à des produits. Cette tension est résumée dans un billet de blog de l'équipe Diplomatie numérique du Quai d'Orsay :

> « Le soutien des acteurs monopolistiques au développement de briques technologiques en *open source* peut constituer un moyen pour [eux de communiquer] sur leur générosité et valeurs. Car ces briques sont ensuite intégrées dans leurs produits finis, lesquels sont eux étroitement verrouillés et monétisés. [...] ces financements et rachats relèvent donc à la fois d'une stratégie d'image [...] – et de *(re)enclosures* plus ou moins subtiles.[124] »

En somme, le terme « *open source* » tend à être détourné au profit d'intérêts commerciaux[125]. Plus généralement, on constate que les motivations des acteurs privés à investir l'*open source* tendent, dans de nombreux cas, à diverger significativement de la philosophie à l'origine de l'OS.

124. B. Pajot, « Des barbelés sur la prairie Internet : contre les nouvelles enclosures, les communs numériques comme leviers de souveraineté », Diplomatie numérique, 31 juillet 2020, p. 5, disponible sur : www.diplomatie.gouv.fr.
125. D. Berkholz, « The Business of Open Source », *op. cit.*

Les gouvernements s'en mêlent : (géo)politisation de l'*open source* aux États-Unis, en Chine et en Europe

On l'a dit, des composants *open source* sont présents dans la quasi-totalité des logiciels propriétaires. Dès lors, il n'est pas surprenant que le secteur privé soit considéré comme plus « mûr » que les pouvoirs publics, dans la compréhension du rôle de l'OS dans les chaînes d'approvisionnement des logiciels[126]. L'intérêt des États pour l'*open source* n'est pas nouveau. Cela étant, on assiste à une évolution dans l'implication des gouvernements, qui cherchent non plus seulement à adopter l'*open source* ou à développer des solutions logicielles par ce biais, mais désormais également à contribuer au financement voire à la gouvernance des écosystèmes *open source*, aux niveaux national et/ou mondial. Cette implication n'est pas uniquement pragmatique ; elle est de plus en plus politisée, qu'il s'agisse de pallier les risques de potentielles ingérences étrangères dans l'*open source* (comme dans le cas américain), d'appliquer le techno-nationalisme et le contrôle social aux communautés *open source*, comme en Chine, ou de poursuivre une « troisième voie » basée à la fois sur les « communs » et sur la « souveraineté » numériques, comme dans le cas européen[127].

États-Unis : une focale sur la cybersécurité

*Usage de l'*open source *dans les systèmes des agences fédérales*

Aux États-Unis, les enjeux de l'OS sont principalement abordés sous l'angle de la cybersécurité, avec une réponse axée sur les mesures préventives au sein de l'administration fédérale, et sur la coopération public-privé.

126. « Towards a Sovereign Digital Infrastructure », European Working Team on Digital Commons, *op. cit.*, p. 23.

127. D'autres cas mériteraient d'être étudiés plus avant, notamment les cas russe et indien, du fait de la volonté des deux pays de développer des alternatives aux logiciels propriétaires américains et/ou chinois. Voir notamment M.-G. Bertran, « La place des logiciels libres et *open source* », *op. cit.*, et K. Blind *et al.*, « The Impact of Open Source Software », *op. cit.*

Une volonté de généraliser le recours à l'*open source* dans l'administration

Dans les années 1980, le gouvernement américain s'appuyait principalement sur des logiciels propriétaires sur-mesure ; le Département de la Défense (DoD) était le principal acheteur de logiciels personnalisés[128]. Dans les années 1990, un virage s'est opéré vers l'achat de logiciels sur étagère, dans un effort de réduction des coûts de développement des logiciels. En parallèle, les années 1990 ont marqué l'arrivée de logiciels *open source* dans les infrastructures et le *backend* des systèmes informatiques du gouvernement fédéral. Alors que les années 2000 ont vu le secteur privé américain investir massivement dans l'*open source* et dans la promotion de celui-ci (cf. *supra*), le rôle de l'OS dans les activités du DoD, et donc son importance pour la sécurité nationale, ont pris de l'ampleur. Un rapport datant de 2003 explique :

> « Les logiciels libres jouent un rôle plus critique dans le DoD que ce qui a été généralement reconnu. [Par exemple,] l'interdiction des logiciels libres supprimerait certains types de composants d'infrastructure [...] qui aident actuellement à soutenir la sécurité des réseaux. [Par conséquent,] l'interdiction des logiciels libres aurait des impacts immédiats, larges et fortement négatifs sur la capacité de nombreux groupes sensibles et axés sur la sécurité du DoD à se défendre contre les cyberattaques.[129] »

Si les logiciels propriétaires sont restés dominants, la politique fédérale au début de la décennie 2000 incitant la prise en compte des coûts des logiciels sur la durée (incluant les coûts de maintenance) et la protection des données a plutôt encouragé, sans le recommander ouvertement, à recourir à des solutions *open source*[130]. C'est en 2016 que le gouvernement américain a adopté une politique plus assumée en faveur de l'OS (*Federal Source Code Policy*), en vertu d'un mémorandum encourageant l'usage au sein du gouvernement fédéral de solutions OS, l'ouverture des codes sources, et leur réutilisation au sein des différentes administrations, réservant les solutions sur étagère en second recours[131].

Un mémo du *Chief Information Officer* (CIO) du DoD, datant de janvier 2022[132], estime que l'usage de l'*open source* par la puissance publique présente plusieurs intérêts : l'examen continu par les pairs assure la fiabilité et la sécurité des logiciels, dans une plus grande mesure que si les logiciels sont développés par de plus petites équipes ; la possibilité illimitée de modifier le code source permet au DoD de s'adapter rapidement aux situations et besoins changeants ; l'OS réduit les risques liés aux

128. K. Blind *et al.*, « The Impact of Open Source Software », *op. cit.*, p. 296.
129. T. Bollinger, « Use of Free and Open-Source Software (FOSS) in the U.S. Department of Defense », The MITRE Corporation, 2003, p. 2, cité dans *Ibid*, p. 297. [Nous traduisons.]
130. *Ibid.*
131. *Ibid.*
132. « Software Development and Open Source Software », Memorandum, Department of Defense, Chief Information Officer, 24 janvier 2022, disponible sur : https://dodcio.defense.gov.

dépendances aux logiciels propriétaires et aux restrictions qui peuvent en découler (comme le *vendor lock-in*) ; l'OS offre des avantages financiers pour les cas où de nombreuses copies du logiciel sont nécessaires, et pour la maintenance des logiciels ; enfin, l'OS est adapté au prototypage et à l'expérimentation.

Pallier les risques de l'ouverture

Toutefois, l'OS présente également des défis, en particulier pour le DoD, et plus généralement pour la sécurité nationale. Le premier est que l'utilisation dans des systèmes critiques de codes gérés en externe crée potentiellement des points d'entrée pour des adversaires qui chercheraient à introduire du code malveillant dans les systèmes du DoD. La sécurité de la chaîne d'approvisionnement des logiciels OS soit donc faire l'objet d'un examen rigoureux. Le mémorandum du *Chief Information Officer* formule les avertissements suivants, pour évaluer la pertinence de l'utilisation d'un logiciel libre pour le DoD :

- **Maintenance sur le long terme** : s'assurer que le logiciel sera correctement maintenu par la communauté OS pendant sa durée de vie.
- **Sources de confiance** : s'assurer que la version du logiciel provient d'une source de confiance, étant donné l'existence de plusieurs versions d'un même logiciel, dont certaines peuvent être non fiables. Pour limiter les risques, le logiciel doit être de préférence maintenu par un consortium établi ou une entité commerciale.
- **Dépendances** : identifier les dépendances à des sous-composants sur lesquels repose le logiciel.
- **Sécurité des composants** : s'assurer de l'utilisation d'outils de détection des vulnérabilités par la communauté de développeurs.
- **Intégrité des composants** : les risques sont limités lorsque les codes sont marqués par des empreintes numériques permettant de garantir l'intégrité du code et s'assurer qu'il n'a pas été modifié.
- **Influence de gouvernements étrangers** : dans la loi américaine, l'*open source* est exempté des mesures qui s'appliquent aux fournisseurs de technologies et services IT ayant des obligations envers des gouvernements étrangers[133]. Toutefois, les gestionnaires de programme doivent être conscients de l'influence potentielle de gouvernements étrangers sur les logiciels. Un audit des contributions à un projet OS peut être nécessaire pour se prémunir contre les ingérences malveillantes.

Ce dernier point fait actuellement l'objet d'une vigilance accrue, comme nous l'expliquons plus loin.

133. Public law 115-232, section 1655 (reference (I)), 2018.

Enfin, un autre défi pour le DoD provient du fait que le partage imprudent de codes développés pour les systèmes de la défense nationale pourrait profiter aux adversaires en divulguant des innovations clés. Dès lors, le ministère doit clairement articuler comment, où et quand il participe, contribue et interagit avec la communauté élargie du logiciel OS. Le principe établi est que le DoD peut partager les codes qu'il développe sous licence *open source*, si ceux-ci ne sont pas des composants de « technologies critiques[134] ».

Après la faille Log4Shell : une approche de plus en plus géopolitique

Les préoccupations américaines pour la sécurité des solutions *open source* ont largement dépassé le cadre du DoD après la faille Log4Shell. Depuis le début de l'année 2022, la Maison-Blanche et le Congrès américain ont prêté une attention accrue aux fonctions larges et stratégiques de l'OS et aux risques qui peuvent y être liés.

Un surcroît d'attention politique après Log4Shell

Déjà en mai 2021, le président Joe Biden avait signé un *Executive Order* (EO) sur la cybersécurité[135], suite à l'attaque SolarWinds (décembre 2020). Dans ce document, où les logiciels sont décrits comme remplissant des fonctions critiques pour la défense des institutions vitales de la Nation, la Maison-Blanche appelait à renforcer la coopération avec le secteur privé pour l'identification et le partage d'informations au sujet des menaces cyber, à mettre en œuvre au sein du gouvernement fédéral des pratiques et des moyens de cybersécurité renforcés (*zero trust architecture*[136], procédures de réponse aux vulnérabilités), et l'examen des chaînes d'approvisionnement des logiciels. Plus précisément, l'EO préconisait l'emploi d'outils, y compris automatisés, pour l'examen de la provenance des codes et composants de logiciels, la généralisation du recours aux *Software Bills of Materials* (SBOM)[137], et, dans le cas des logiciels *open source*, « de s'assurer et

134. Les composants de technologies critiques sont entendus comme « les informations et les données techniques qui font progresser la technologie actuelle ou décrivent une nouvelle technologie dans un domaine d'application militaire important ou potentiellement important, ou qui concernent une déficience militaire spécifique d'un adversaire potentiel ». « Software Development and Open Source Software », Chief Information Officer, *op. cit.*, p. 6. [Nous traduisons.]
135. « Improving the Nation's Cybersecurity », *op. cit.*
136. « Le modèle de sécurité *zero trust architecture* part du principe qu'une intrusion est inévitable ou s'est probablement déjà produite. Il limite donc constamment l'accès aux seuls éléments nécessaires et recherche les activités anormales ou malveillantes ». *Ibid.* [Nous traduisons.]
137. La *Software Bill of Material* est la liste des « ingrédients » présents dans un logiciel, dans la mesure où ceux-ci sont pour une bonne part le résultat d'un assemblage de composants *open source* et propriétaires. Une SBOM permet d'identifier la presence de composants ou de licences présentant des risques ou des failles avérées.

d'attester, dans la mesure du possible, de l'intégrité et de la provenance des logiciels [...] utilisés dans toute partie d'un produit[138] ».

La faille Log4Shell a entraîné une nouvelle série d'initiatives politiques, cette fois centrées sur l'*open source*. En janvier 2022 s'est tenue à la Maison-Blanche une réunion[139] de l'Administration américaine (ministères du Commerce, de la Défense, de l'Énergie, de la Sécurité intérieure ; Cybersecurity and Infrastructure Security Agency [CISA] ; National Institute of Standards and Technology [NIST]), grandes entreprises de la tech américaine (dont Amazon, Apple, Google, IBM, Meta, Microsoft) et acteurs de l'*open source* (GitHub, Linux Foundation, OpenSSF), pour évoquer la sécurité de l'*open source* et son financement. Les échanges ont permis de définir trois grands objectifs[140] :

- sécuriser la production des logiciels *open source*, avec une focale sur la prévention des failles de sécurité et vulnérabilités dans le code et les packages *open source* ;
- améliorer les processus de détection et de la correction des vulnérabilités ;
- raccourcir le temps de réponse pour la distribution et la mise en œuvre des correctifs.

Selon les fondations Linux et OpenSSF – auteures du rapport issu de la réunion –, ces efforts doivent être réalisés dans une collaboration public-privé. Le rapport estime que le secteur public a un rôle à jouer dans le renforcement des infrastructures logicielles critiques, dont la chaîne d'approvisionnement OS, et propose une amélioration de la formation des développeurs aux enjeux de sécurité, ainsi que la création d'une plateforme publique dédiée à l'analyse des risques liés aux composants *open source*[141].

Le Congrès américain a également lancé des travaux législatifs. Le Sénat a mené des auditions en février 2022 dans le but d'identifier les leçons à tirer de la crise. Le *CHIPS and Science Act*, voté à l'été 2022, enjoint le NIST à renforcer la sécurité des logiciels *open source*, en diffusant les informations liées aux vulnérabilités identifiées, et en produisant des directives volontaires pour aider les entités qui maintiennent les dépôts de code à découvrir les vulnérabilités et y répondre[142]. Cette mesure est peu ambitieuse, par comparaison à ce qu'avaient proposé certains membres du Congrès, dont un amendement dans le cadre du projet de loi *COMPETES Act*, pour la création d'une série de centres d'excellence pour les technologies critiques, dont un sur l'*open source*. Un tel centre d'excellence aurait permis de

138. « Improving the Nation's Cybersecurity », *op. cit.*, p. 7. [Nous traduisons.]
139. J. Lausson, « Log4j : la Maison-Blanche réunit le gratin de la tech pour discuter de la sécurité de l'*open source* », Numérama, 13 janvier 2022, disponible sur : www.numerama.com.
140. « The Open Source Software Security Mobilization Plan », *op. cit.*, p. 5.
141. *Ibid.*, p. 3.
142. « CHIPS and Science Act of 2022 », Sec. 10224. « Software security and authentication. (a) Vulnerabilities in Open Source Software », Sénat des États-Unis, 2022.

canaliser des financements publics directement dans les projets et outils *open source* jugés les plus critiques[143].

Des initiatives pour renforcer la sécurité de l'OS aux États-Unis sont cependant toujours en cours. Le 14 septembre dernier, le gouvernement a publié des directives visant à limiter les risques de vulnérabilités dans les chaînes d'approvisionnement logicielles. Ces dernières directives exigent des fournisseurs de logiciels qu'ils fournissent une auto-attestation (comprenant le nom du concepteur du logiciel) ou, dans le cas des produits *open source*, qu'ils soient évalués par une organisation certifiée par le *Federal Risk and Authorization Management Program* (FedRAMP)[144]. Dans le même temps, les sénateurs Rob Portman et Gary Peters ont introduit une proposition de loi pour « sécuriser les logiciels *open source* », qui entend charger l'agence fédérale de cybersécurité et de sécurité des infrastructures (CISA) de développer des moyens d'examiner, évaluer et réduire les risques liés aux composants *open source* utilisés par les agences fédérales[145].

La crainte de l'ingérence étrangère

La perception des risques liés à l'*open source* ne relève pas uniquement des vulnérabilités accidentelles dans les composants, mais aussi et de plus en plus d'une manipulation des codes par des acteurs mal intentionnés et travaillant potentiellement pour le compte de gouvernements étrangers. Dans le but de mieux identifier concrètement ces risques d'ingérences, la Defense Advanced Research Projects Agency (DARPA) a annoncé en 2020 un projet, baptisé SocialCyber, qui vise à :

> « explorer les capacités de détection et de lutte contre les opérations cyber-sociales qui peuvent viser les communautés de développeurs de logiciels libres [, comme la] soumission de codes ou de designs défectueux, les campagnes sur les réseaux sociaux contre les développeurs et les responsables de logiciels libres, critiquant les failles, ainsi que les rapports de bogues trompeurs, l'obscurcissement des discussions techniques et la capture sociale de l'autorité fonctionnelle sur les projets de logiciels libres[146] ».

143. W. Loomis et L. Wolff, « Defending Fire: A Need for Policy to Protect the Security of Open Source », Lawfare, 8 février 2022.
144. « Enhancing the Security of the Software Supply Chain Through Secure Software Development Practice », Memorandum, Executive office of the President, 14 septembre 2022, disponible sur : www.whitehouse.gov. Le FedRAMP fournit notamment des agréments pour les services *cloud*.
145. T. Stark, « Senators Introduce a Bill to Protect Open-Source Software », *Washington Post*, 22 septembre 2022.
146. « Hybrid AI to Protect Integrity of Open Source Code (SocialCyber) », DARPA-PA-20-02-07, DARPA, non daté, p. 2, disponible sur : https://imlive.s3.amazonaws.com. [Nous traduisons.]

Peu d'informations sont disponibles sur la façon dont a été mis en œuvre ce projet[147], mais il est intéressant de constater que l'*open source* est désormais abordé comme un domaine au sein duquel des adversaires peuvent déployer des actions non seulement de sabotage mais aussi de désinformation.

Cette analyse des risques n'est pas neutre sur le plan géopolitique. De fait, on constate, venant de la Maison-Blanche et du DoD, un vocabulaire suggérant une géopoliticisation de l'OS, avec les références à la sécurité nationale, aux adversaires, et à l'ingérence étrangère. Quatre chercheurs et ingénieurs américains ont récemment rapporté les propos d'officiels et fonctionnaires selon lesquels certains composants OS sont évités, du fait de la contribution d'individus chinois ou russes dans leur développement, et cela même en l'absence de problèmes de sécurité dans les composants :

> « Nous avons entendu des anecdotes d'un employé de la défense selon lesquelles le serveur Web NGINX, un logiciel populaire pour stocker et diffuser des pages Web, a été banni de certains réseaux gouvernementaux parce que l'un des développeurs associés au projet est russe[148]. »

Les chercheurs ont analysé les nationalités indiquées sur les profils GitHub des cent principaux contributeurs à deux projets OS structurants (paquets Python et JavaScript). Seule une fraction (moins de 10 %) des contributeurs *open source* de ces programmes populaires semble être basée en Russie ou en Chine. La majorité des contributeurs déclarent être localisés aux États-Unis ou dans un autre pays. De plus, le nombre de contributeurs qui n'ont pas indiqué leur localisation géographique dépasse les 50 % pour certains paquets, rendant l'analyse peu opérante.

Les auteurs concluent par ailleurs que leurs recherches sur la sécurité des chaînes d'approvisionnement logicielles ne suggèrent pas qu'une connaissance des localisations géographiques des développeurs aurait pu permettre d'éviter la compromission d'un logiciel *open source*. En d'autres termes, les données ne permettent pas de statuer sur l'effectivité de l'influence de développeurs russes ou chinois sur les logiciels libres, ni sur le fait que ceux-ci agiraient pour le compte de leurs gouvernements. Cependant, l'inquiétude des autorités américaines à ce sujet a toutes les chances de croître, à mesure que – comme nous allons le voir – les développeurs russes et chinois investissent l'*open source* : la proportion de développeurs GitHub basés en Chine a augmenté de 15 % entre 2020 et 2021, et la part de développeurs basés en Russie de 30 %[149].

147. P. H. O'Neill, « The US Military Wants to Understand the Most Important Software on Earth », *MIT Technology Review*, 14 juillet 2022.
148. D. Geer *et al.*, « Should Uncle Sam Worry About 'Foreign' Open-Source Software? », *op. cit.* [Nous traduisons.]
149. *Ibid.*

Chine : gagner en indépendance et en influence

Des projets open source *de portée mondiale*

Comme on l'a dit, la part de contributeurs chinois aux communautés mondiales est en nette augmentation, depuis la décennie 2010, et particulièrement depuis 2020[150]. Entre 2012 et 2018, le nombre de membres chinois de la Fondation Linux a crû de plus de 400 %[151]. Parmi les 73 millions de contributeurs à GitHub, en 2021, 7,5 millions étaient basés en Chine, représentant ainsi un peu plus de 10 %, et la nationalité la plus représentée derrière les États-Unis[152]. La communauté OS chinoise est donc fleurissante, et de nombreux projets GitHub développés par des Chinois comptent des centaines de contributeurs, des milliers de *forks*[153] et ont reçu des milliers d'évaluations positives[154]. Il est notable que sur les cinq comptes GitHub les plus suivis en 2020, deux étaient ceux de développeurs chinois (mais un seul en 2022)[155]. En mars 2021, Alibaba, Huawei et Tencent figuraient toutes les trois pour la première fois dans le top 20 des contributions au dépôt GitHub[156]. Parmi les projets influents, on peut citer OpenResty. Ce projet d'API[157] Gateway est l'un des projets OS chinois les plus anciens, puisqu'il a débuté en 2011, et les plus utilisés, puisqu'il est utilisé par des entreprises telles que CloudFlare, Target et Lyft[158].

En dehors de GitHub, il existe également des plateformes chinoises, telles que celles fondées par Tencent et Alibaba, et Gitee, la plateforme leader en Chine[159]. Gitee compte aujourd'hui plus de 8 millions d'utilisateurs[160]. Certains développeurs préfèrent d'ailleurs utiliser Gitee plutôt que GitHub, pour ses meilleures performances techniques (du fait de la proximité de la

150. B. Cameron Gain, « China's Open Source Activity Surged in 2020 », 5 mai 2021, disponible sur : https://devops.com.
151. R. Arcesati et C. Meinhardt, « China Bets on Open-Source Technologies to Boost Domestic Innovation », MERICS, 19 mai 2021, disponible sur : https://merics.org.
152. Z. Yang, « How Censoring China's Open-Source Coders Might Backfire », *MIT Technology Review*, 30 mai 2022.
153. Littéralement « fourche » ou « embranchement », un *fork* se réfère à un nouveau logiciel créé à partir du code source d'un logiciel existant.
154. K. Xu, « Open Source in China: Next Four Years », Interconnected, 21 décembre 2021, disponible sur : https://interconnected.blog.
155. K. Xu, « Open Source in China: The Players », Interconnected, 7 mai 2020, disponible sur : https://interconnected.blog ; GitHub, « Users », non daté, disponible sur : https://github.com.
156. B. Cameron Gain, « China's Open Source Activity Surged in 2020 », *op. cit.* Les contributions à GitHub sont comptabilisées comme le nombre total de fourches, de commits, d'étoiles, de pull requests, de commentaires sur les problèmes et d'autres mesures.
157. API est l'acronyme de *Application Programming Interface* (interface de programmation d'application) qui facilite l'interaction entre plusieurs logiciels, c'est-à-dire leur offre l'accès aux fonctionnalités et services d'autres programmes.
158. K. Xu, « Open Source in China: Next Four Years », *op. cit.*
159. Z. Yang, « How Censoring China's Open-Source Coders Might Backfire », *op. cit.*
160. *Ibid.*

localisation de la plateforme, sur le territoire chinois) et l'absence de risque d'ingérence étrangère (cf. *infra*)[161].

Selon la China Academy for Information and Communications Technology, environ 87,4 % des entreprises chinoises auraient recours aux technologies *open source*[162]. Comme toutes les entreprises du numérique du monde, elles le font pour développer leurs programmes, accroître la visibilité de leurs projets et encourager l'adoption, attirer des talents, et plus généralement gagner en influence sur le monde numérique[163]. Par ailleurs, la volonté chinoise de s'autonomiser des technologies américaines est une motivation croissante à recourir à l'OS.

Preuve de la place de plus en plus centrale de la Chine dans l'écosystème, et de son ambition d'utiliser l'OS pour développer des technologies critiques, on peut citer plusieurs domaines dans lesquels les grandes entreprises chinoises sont particulièrement investies : les systèmes d'exploitation, les semi-conducteurs, le *cloud* et l'IA.

Système d'exploitation

Huawei, entreprise de réseaux télécoms, de téléphonie mobile et de *cloud*, est un contributeur important et un bénéficiaire clair, de l'*open source*. L'entreprise, placée en 2020 sur liste rouge par les États-Unis, est en fait le plus gros contributeur au « noyau[164] » (*kernel*) du système d'exploitation Linux, qui est « la pierre angulaire de la quasi-totalité du *cloud*, de pratiquement tous les supercalculateurs, de l'ensemble de l'internet des objets, de milliards de smartphones, etc.[165] ».

En retour, de nombreux pans des technologies de Huawei reposent sur des contributions étrangères aux logiciels *open source*, en premier chef Android. En mai 2019, Huawei a perdu la licence d'exploitation lui permettant d'utiliser le système Android de Google, à la suite des sanctions prises par la Maison-Blanche contre l'entreprise chinoise. En retour, Huawei a accéléré ses plans pour développer une alternative au système d'exploitation de Google, mais elle aussi basée sur Android : Harmony OS. L'ambition est non seulement de s'accommoder des restrictions imposées par les États-Unis, mais aussi de développer un concurrent aux deux offres dominantes, celle de Google et celle d'Apple (iOS) pour conquérir les marchés internationaux, notamment en Afrique, où les terminaux mobiles

161. *Ibid.*
162. R. Arcesati et C. Meinhardt, « China Bets on Open-Source Technologies », *op. cit.*
163. *Ibid.*
164. Le noyau (*kernel* en anglais) est un composant central de certains systèmes d'exploitation, qui gère les ressources de l'ordinateur et permet aux différents composants (logiciels et matériels) de communiquer entre eux.
165. M. O'Neil *et al.*, « The US Military Wants to Understand », *op. cit.*

chinois (notamment de la marque Transsion) sont déjà les plus populaires[166]. Enfin, Huawei, avec Harmony OS, vise également le marché de la 5G et de l'IoT[167].

Semi-conducteurs

Outre les systèmes d'exploitation pour terminaux mobiles, les entreprises chinoises sont également tributaires de l'*open source* dans le matériel et les logiciels utilisés pour la fabrication des semi-conducteurs. La Chine, à travers notamment Alibaba et Huawei, a investi, aux côtés de géants américains tels que Google et de l'européen NXP, la communauté du projet RISC-V pour des designs de semi-conducteurs *open source*. La technologie RISC-V fait depuis 2018 l'objet en Chine d'un investissement accru *via* la « China RISC-V Alliance », composée d'instituts de recherche et d'entreprises[168].

Si RISC-V, en tant que projet OS, ne tombe pas sous le coup des restrictions américaines à l'export, certains aux États-Unis ont exprimé des craintes quant au fait que le projet permet à la Chine de développer son écosystème de production de semi-conducteurs. Un rapport du Congressional Research Service estime ainsi que des plateformes comme RISC-V permettent à des entreprises et instituts chinois qui préoccupent le gouvernement américain d'accéder à des technologies et capacités américaines matérielles et logicielles dans ce domaine jugé stratégique[169]. Il est à noter que l'Europe cherche aussi à développer ses capacités de supercalcul sur la base de RISC-V[170]. En outre, la fondation, à l'origine basée aux États-Unis, s'est récemment relocalisée en Suisse afin de se prémunir contre de potentielles restrictions américaines à l'avenir – un mouvement aux conséquences *a priori* favorables pour les utilisateurs chinois[171].

Cloud

Comme expliqué plus haut, les fondements technologiques de l'informatique en nuage sont constitués de briques *open source*. Du fait de la croissance de l'usage du *cloud* en Chine, les entreprises chinoises sont très impliquées dans le développement de ces technologies, notamment à travers la Cloud Native Computing Foundation, qui fait partie de la Fondation Linux[172]. Selon un responsable de GitHub, Kevin Xu, la Chine est le triosième plus grand contributeur à ces projets, derrière les États-Unis et l'Allemagne. Parmi les

166. H. Tugendhat, « Huawei Is Trying to Avoid U.S. Sanctions: That May Change the U.S.-China Tech Rivalry in Africa », *The Washington Post*/Monkey Cage, 30 avril 2021, disponible sur : www.washingtonpost.com.
167. R. Arcesati et C. Meinhardt, « China Bets on Open-Source Technologies », *op. cit.*
168. C. Meinhardt, « Open Source of Trouble », *op. cit.*
169. K. M. Sutter, « China's Recent Trade Measures and Countermeasures: Issues for Congress », Congressional Research Service, Rapport R46915, 10 décembre 2021, p. 42.
170. R. Loukil, « Pourquoi Intel et l'Espagne investissent dans une nouvelle génération de microprocesseurs », *L'Usine Nouvelle*, 9 juin 2022.
171. S. Nellis et A. Alper, « U.S.-Based Chip-Tech Group Moving to Switzerland over Trade Curb Fears », Reuters, 25 novembre 2019.
172. K. Xu, « Open Source in China: The Players », *op. cit.*

entreprises contributrices, PingCAP (bases de données) et Huawei sont les plus actives[173]. Cette dernière est également « un membre actif et un soutien » du projet d'infrastructure de *cloud* européenne, Gaia-X – infrastructure que Huawei dit vouloir contribuer à rendre « à la fois extrêmement ouverte et extrêmement sûre[174] ».

Intelligence artificielle

Enfin, les entreprises chinoises sont impliquées dans des projets *open source* dans l'IA. Comme expliqué plus haut, les *frameworks* de *deep learning* les plus utilisés au niveau mondial sont celui de Google, TensorFlow et celui de Meta, PyTorch. En 2016, Baidu a voulu développer une alternative chinoise, avec la plateforme de *deep learning* PaddlePaddle. Depuis, Huawei et XDL ont lancé eux aussi leurs plateformes. À ce stade, toutefois, le dépôt TensorFlow compte huit fois plus de contributions que PaddlePaddle[175].

La Chine connaît davantage de succès dans des domaines plus spécialisés et émergents, tels que l'IA pour les véhicules autonomes[176]. Baidu a rencontré un franc succès avec Apollo, un système de conduite autonome. Des entreprises chinoises comme européennes (BMW, Volkswagen) se sont jointes au projet[177]. Si bien qu'Apollo pourrait devenir, d'ici 2025, la principale alternative *open source* à la pile logicielle de conduite autonome de Tesla, pour sa part totalement fermée et propriétaire[178].

Une forte implication du gouvernement chinois

Un historique d'implication gouvernementale et de collaborations internationales

À mesure que l'*open source* acquiert une place centrale dans le processus de développement de solutions logicielles, et devient une condition *sine qua non* de l'innovation, Kevin Xu estimait en 2020 que :

> « la Chine devrait adopter le mode de fonctionnement de l'*open source*, comme une gouvernance transparente, des discussions ouvertes avec les parties prenantes et les développeurs, et des procédures équitables pour l'élaboration des règles[179]. »

Ce faisant, le pays pourrait tirer sur le plan domestique les bénéfices technologiques de l'*open source* mais aussi devenir un joueur responsable et digne de confiance à l'échelle internationale[180]. Ce n'est toutefois pas la

173. *Ibid.*
174. « About Huawei *Open source* », non daté, disponible sur : www.huawei.com.
175. R. Arcesati et C. Meinhardt, « China Bets on Open-Source Technologies », *op. cit.*
176. *Ibid.*
177. *Ibid.*
178. K. Xu, « Open Source in China: Next Four Years », *op. cit.*
179. K. Xu, « Open Source in China: The Players », *op. cit.* [Nous traduisons.]
180. *Ibid.*

direction que semble prendre le gouvernement de Pékin. Au contraire, on assiste à une implication croissante du gouvernement chinois dans l'*open source*, qui s'explique par des intérêts économiques et de sécurité, et une volonté de gagner en indépendance vis-à-vis des technologies américaines[181]. À l'origine, cette implication s'est faite à travers des projets en coopération internationale et une participation aux communautés OS globales, mais elle se traduit de plus en plus par une vision nationaliste de l'OS et une volonté de contrôle étatique sur les communautés *open source*, allant ainsi à l'encontre de l'esprit et de la logique de l'*open source*.

La volonté du gouvernement chinois de contribuer au développement de l'*open source* s'inscrit dans une stratégie plus large visant à s'imbriquer dans des réseaux collaboratifs internationaux pour s'émanciper de la dépendance aux technologies américaines, et à contourner les restrictions empêchant la Chine d'acquérir certaines technologies, par exemple par le rachat d'entreprises étrangères. Ainsi, l'effort dans l'OS s'accompagne d'autres initiatives, dont la constitution de *joint-ventures*, partenariats de recherche, programmes visant à attirer des talents étrangers, etc.[182].

L'implication du gouvernement chinois dans l'OS n'est pas nouvelle, Déjà en 2007, Guohua Pan et Curtis Jay Bonk écrivaient :

> « Contrairement à la spontanéité du mouvement *open source* en Amérique du Nord, le développement de logiciels *open source* en Chine [...] est une activité orchestrée dans laquelle différents niveaux du gouvernement chinois jouent un rôle vital dans le parrainage, l'incubation et l'utilisation de logiciels *open source*[183]. »

Ainsi, la communauté OS chinoise a émergé à partir des années 2000 d'initiatives gouvernementales, et largement dans un contexte de coopération internationale. L'un des projets phares a été le système d'exploitation Red Flag, basé sur Linux, développé et distribué à partir de 2000 par l'institut de recherche sur le logiciel de l'Académie des Sciences chinoise[184]. Ensuite, l'alliance pour le logiciel *open source* a été créée en 2004, autour de Red Flag et en partenariat avec des entreprises américaines telles que IBM, Intel, et HP[185]. La même année, la Chine a également lancé une coopération avec la France autour du développement d'une pile logicielle d'infrastructure *open source* (avec le CEA, l'Inria, Bull et STMicrolectronics[186]) et de l'établissement d'une plateforme *open source*

181. Depuis les années 2010, les autorités chinoises ont interdit certains logiciels américains (on a évoqué le cas des outils Google) à des fins de censure ou par crainte de risques d'espionage. L. Whitney, « Microsoft, China Clash Over Windows 8, Backdoor-Spying Charges », CNET, 6 juin 2014.
182. K. M. Sutter, « China's Recent Trade Measures and Countermeasures », *op. cit.*, p. 31.
183. G. Pan et C. J. Bonk, « The Emergence of Open-Source Software in China », *International Review of Research in Open and Distance Learning*, vol. 8, n° 1, 2007, résumé. [Nous traduisons.]
184. *Ibid.*, p. 2.
185. D. Legard, « Open Source Software Alliance Formed in China », NetworkWorld, 11 août 2004, disponible sur : www.networkworld.com.
186. T. Gasperson, « France and China Sign Open Source/Open Standards Deal », Linux.com, 11 octobre 2004, disponible sur : www.linux.com.

pour les logiciels *middleware*, baptisée OW2[187]. OW2 existe encore aujourd'hui, mais elle est depuis devenue une fondation indépendante et généraliste de droit français.

Vers une communauté *open source* nationale ?

En parallèle de ce mouvement d'imbrication et de collaboration internationale, on constate toutefois un mouvement vers les technologies OS nationales, qui a tendu à se renforcer.

Dès 2006, le gouvernement chinois a annoncé que toutes les agences gouvernementales devaient utiliser des « logiciels produits localement », une ambition qui devait être atteinte en 2010[188]. Ce type d'argumentaire n'a fait que se répandre (côté chinois comme côté américain) au cours de la décennie 2010, et plus encore depuis 2020, à mesure que les tensions géopolitiques s'accroissent et que la volonté de « découplage » s'étend à de nouveaux domaines technologiques. Ainsi, aujourd'hui, selon l'Académie des Sciences chinoise, si la participation du pays dans l'OS a crû, elle reste insuffisante, car le pays reste trop dépendant des fondations étrangères qui font vivre l'écosystème mondial de l'OS[189]. De fait, à l'aune des sanctions américaines contre Huawei, décidées en 2019, le gouvernement chinois a commencé à s'inquiéter de son niveau de dépendance à GitHub, détenue par Microsoft[190]. Et, en retour, du fait que les technologies *open source* sont, par défaut, sans frontières, les contributions chinoises sont susceptibles d'être utilisées par les géants de la tech américains[191]. Les institutions ayant des liens avec le gouvernement chinois ont donc plutôt tendance à utiliser la plateforme chinoise Gitee[192].

L'accélération de la compétition États-Unis/Chine a poussé les secteurs stratégiques de l'industrie chinoise (banque, assurance, télé-communications) à adopter soit des technologies nationales, soit des technologies *open source*, mais de préférence des technologies *open source* nationales[193]. En parallèle, l'attention du gouvernement chinois, et sa volonté de contrôle sur l'*open source*, s'est clairement renforcée depuis 2020. Par crainte de possibles futures restrictions américaines sur la diffusion des technologies *open source* (qui sont pour l'heure exemptes de contrôle des

187. « Introducing OW2 », OW2, non daté, disponible sur : www.ow2.org.
188. P. DeGroot, « Chinese PC Makers to Ship Legal OSs », 25 décembre 2006, cité dans G. Pan et C. J. Bonk « The Emergence of Open-Source Software in China », *op. cit.*
189. Y. Long *et al.*, « Development Experience of International Open Source and Its Enlightenment to Construction of Open Source Innovation System in China », *Bulletin of Chinese Academy of Sciences*, vol. 36, n° 12, 2021.
190. Z. Yang, « How Censoring China's Open-Source Coders Might Backfire », *op. cit.*
191. K. Xu, « Open Source in China: The Trends », *op. cit.*
192. Z. Yang, « How Censoring China's Open-Source Coders Might Backfire », *op. cit.*
193. L. Y. Chen, « China's Biggest Startups Ditch Oracle and IBM for Home-Made Tech », Bloomberg, 24 juin 2019. [Nous traduisons.]

exportations[194]), la Chine mise sur le développement de communautés nationales. Le précédent iranien où, en 2019, GitHub avait restreint l'accès à sa plateforme à la suite des sanctions américaines, fait craindre le pire à la Chine[195]. La première fondation chinoise pour l'*open source*, OpenAtom, a été créée en 2020, comme une leçon tirée du cas iranien[196].

Dans la foulée, le « 14e Plan quinquennal chinois 2021-2015 », publié en mars 2021, est le premier qui fait mention de l'*open source* comme priorité stratégique nationale[197]. Suite à cela, le ministère de l'Industrie et de l'Information a fixé l'objectif de « créer deux à trois communautés *open source* avec une influence internationale » d'ici 2025[198]. Aux côtés du ministère de l'Éducation, Huawei s'est récemment impliquée dans la diffusion de connaissances sur les logiciels *open source* auprès des étudiants dans les lycées et universités[199].

Cependant, les ambitions chinoises de contribuer à la communauté globale OS sont confrontées à une autre ambition de l'État chinois, qui est de contrôler davantage la communauté nationale de développeurs. Il arrive régulièrement que des projets hébergés sur Gitee soient censurés parce qu'ils contiennent un langage (de nature politique ou obscène) qui enfreint les lois chinoises[200]. Mais le contrôle semble avoir atteint un niveau supplémentaire. Le 18 mai 2022, tous les projets *open source* hébergés sur Gitee ont été verrouillés et cachés à la vue du public, sans que les développeurs à l'origine de ces codes n'aient été avertis. Beaucoup soupçonnent que l'État chinois a forcé Gitee à censurer les codes[201]. Dans un communiqué, Gitee a seulement indiqué que désormais, tous les nouveaux codes déposés seraient examinés manuellement avant de pouvoir être officiellement publiés, et que les projets déjà présents sur la plateforme seraient eux aussi temporairement rendus privés afin d'être examinés[202]. Et Gitee impose désormais à tout visiteur de

194. « Understanding US Export Controls with Open Source Projects », The Linux Foundation, non daté, disponible sur : www.linuxfoundation.org ; « 开源与美国出口管制 » [« Open Source and U.S. Export Controls »], OSChina.net, 12 août 2020, disponible sur : https://mp.weixin.qq.com.
195. R. Arcesati et C. Meinhardt, « China Bets on Open-Source Technologies », *op. cit.* L'accès des développeurs iraniens à la plateforme GitHub a été rétabli en 2021. N. Friedman, « Advancing Developer Freedom: GitHub Is Fully Available in Iran », GitHub blog, 5 janvier 2021, disponible sur : https://github.blog.
196. R. Arcesati et C. Meinhardt, « China Bets on Open-Source Technologies », *op. cit.*
197. Y. Long *et al.*, « Development Experience of International Open Source », *op. cit.* ; « Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035 », CSET, 13 mai 2021, disponible sur : https://cset.georgetown.edu.
198. K. Xu, « Open Source in China: Next Four Years », *op. cit.* ; Ministère de l'Industrie et des Technologies de l'information de la République populaire de Chine, "十四五"软件和信息技术服务业发展规划》解读 [« Interprétation du plan de développement de l'industrie des services logiciels et des technologies de l'information "14e plan quinquennal" »], 11 novembre 2021, disponible sur : www-miit-gov-cn.translate.goog. [Traduction automatique.]
199. « About Huawei Open Source », Huawei, non daté, disponible sur : www.huawei.com.
200. Z. Yang, « How Censoring China's Open-Source Coders Might Backfire », *op. cit.*
201. *Ibid.*
202. Zihu.com, « 如何看待 5 月 18 日 Gitee 仓库开源须审核，已开源部分仓库暂时关闭，审核通过后再次公开？ » [« « Que pensez-vous du fait que l'open source de l'entrepôt Gitee doit être revu le 18 mai, et que

créer un compte utilisateur pour pouvoir télécharger les codes sources. La plateforme a indiqué ne pas avoir eu le choix dans cette démarche.

Par ailleurs, au mois de juin 2022, le *South China Morning Post* a rapporté que le fondateur et président de ArcherMind Technology (parfois considéré comme l'équivalent chinois de l'américain Red Hat), Wang Jiping, avait été placé en détention dans le cadre d'une « enquête disciplinaire » à propos de laquelle peu de détails sont disponibles[203].

La démarche nationaliste chinoise dans l'*open source* présente de nombreuses limites. D'une part, les technologies *open source* existantes, telles que RISC-V, ne sont pas suffisantes pour garantir que la Chine pourra rivaliser avec les puces américaines ou combler les manques générés par les restrictions aux transferts de technologies[204]. D'autre part, la volonté de créer un écosystème indigène isolé des communautés internationales pourrait nuire à la qualité des logiciels développés et à la possibilité qu'ils trouvent un marché à l'international. Enfin, il est évident que cette attitude de fermeture et de censure va à l'encontre des principes fondamentaux de l'*open source*.

Europe : l'*open source*, outil de la « troisième voie » ?

Souveraineté numérique et promotion des « communs »

La vision européenne de l'OS et les initiatives politiques en cours s'appuient sur le rôle historique des Européens dans l'*open source*, la notion de « communs numériques » au sein desquels s'inscrit en partie l'OS, et l'ambition d'une souveraineté numérique européenne, à laquelle l'OS contribue.

L'Europe dans l'OS : un rôle historique et une participation qui se maintient

L'Europe, aux côtés de l'Amérique du Nord, a joué un rôle pionnier dans les logiciels libres et *open source*. À titre d'exemple, en 1993 l'Organisation européenne pour la recherche nucléaire (CERN) a mis le protocole du Web, inventé par le chercheur britannique Tim Berners-Lee, dans le domaine public, et diffusé la version suivante sous licence libre, contribuant ainsi à l'émergence et à la diffusion de l'internet[205]. On peut par ailleurs noter que le fondateur de Linux, Linus Torvald, est finlandais et a développé ce projet

certains entrepôts qui étaient *open source* sont temporairement fermés, et seront à nouveau rendus publics après le passage de l'examen ? »], fil de discussion, disponible sur : www.zhihu.com. [Traduction automatique.]

203. J. Li, « China's Answer to Open-Source Software Giant Red Hat Says Its Boss Was Taken Away for Disciplinary Investigation », *South China Morning Post*, 8 juin 2022.

204. R. Arcesati et C. Meinhardt, « China Bets on Open-Source Technologies », *op. cit.*

205. « La naissance du Web », CERN, non daté, disponible sur : https://home.cern/fr.

lorsqu'il était étudiant en Finlande. Du fait de ces rôles pionniers, l'Amérique du Nord et l'Europe dominaient numériquement le monde de l'OS jusque dans les années 1990, suite à quoi la diversité géographique des contributeurs s'est accrue[206].

Aujourd'hui, les contributions de développeurs européennes représentent un peu moins d'un tiers des communautés OS mondiales. Le Mercator Institute for China Studies (MERICS) estime que l'Europe représente 26,8 % des contributions à la plateforme GitHub, derrière l'Amérique du Nord (34 %) et l'Asie (30,7 %). Au niveau national, toujours selon MERICS, ce sont les États-Unis qui contribuent le plus (22,7 %), devant la Chine (9,67 %) et l'Inde (5,2 %)[207]. Les communautés OS en Europe sont particulièrement développées en Roumanie, République tchèque, France, Allemagne et au Royaume-Uni[208]. Pour sa part, un rapport de l'UE de 2021 classe l'Allemagne, le Royaume-Uni et la France dans les trois premières positions, en termes de *commits*[209] et de nombre de contributeurs sur GitHub[210].

Un rapport de l'EUIPO montre une implication dans et un usage de l'*open source* parmi les entreprises technologiques européennes stables (54-60 % des interrogés) ou en augmentation (22-26 % des interrogés), au cours de la période 2018-2020[211]. Quarante pourcents des entreprises interrogées déclarent avoir des employés qui développent des programmes *open source* sur leur temps de travail[212]. Selon ce même rapport, la raison principale pour laquelle des entreprises européennes développant des logiciels décident de ne pas recourir à l'*open source* (dans le développement ou l'usage de logiciels) est le modèle de gouvernance de l'OS, dont elles estiment qu'il ne garantit pas la pérennité du développement des produits, ce qui pourrait nuire à leur modèle économique à l'avenir[213].

Il est à noter que, si les entreprises européennes font usage de l'*open source* et y contribuent, elles contribuent à une échelle moindre que leurs homologues américaines et chinoises. Ainsi, en 2022, seules deux entreprises européennes de logiciels, les allemandes SAP et SUSE, figurent dans le

206. D. Rossi *et al.*, « Geographic Diversity in Public Code Contributions: An Exploratory Large-Scale Study over 50 Years », The 2022 Mining Software Repositories Conference, Pittsbrugh, mai 2022, disponible sur : https://hal.archives-ouvertes.fr.
207. R. Arcesati et C. Meinhardt, « China Bets on Open-Source Technologies », *op. cit.*
208. J. Zemlin, « Keynote », Open Source Summit Europe 2022, Dublin, 14 septembre 2022.
209. Un *commit* est l'enregistrement d'une modification sur un code ou fichier, dans le contexte d'un système de gestion de versions.
210. « Enquête sur l'état des lieux de la filière *open source* en France 2020/2021 », Rapport d'étude, Will Strategy, 17 mai 2021, p. 8.
211. « Open Source Software », European Union Intellectual Property Office, *op. cit.*, p. 37-40.
212. *Ibid.*, p. 74.
213. *Ibid.*, p. 40.

top 20 des contributeurs à GitHub[214]. Les auteurs d'un rapport commandé par la Commission européenne notent par ailleurs :

> « Dans l'UE, ce sont les employés des petites et très petites entreprises qui sont le plus susceptibles de contribuer à la production de codes de logiciels libres [...], tandis qu'aux États-Unis les *commits* sont principalement produits par les grandes entreprises du secteur des TIC, qui fondent avec succès leurs modèles commerciaux pertinents sur le vaste corpus de codes de logiciels libres disponibles gratuitement et en constante amélioration.[215] »

Les contributeurs européens sont cependant nombreux. Aujourd'hui, la fondation Linux estime que 31 % de ses membres sont européens[216]. Pour refléter cette forte implication – et le rôle moteur de l'UE en tant qu'acteur supranational – dans la promotion de l'OS et de normes internationales dans le numérique (tel que le Règlement général sur la protection des données – RGPD), la fondation a annoncé en septembre la création de Linux Foundation Europe (LF Europe), dont le siège sera établi en Europe.

L'objectif de préservation des « communs numériques »

L'ambition européenne dans le numérique, dans ses valeurs et son héritage historique, peut être rapprochée de l'imaginaire des « communs numériques ». En effet, la préservation des communs numériques reviendrait à « préserver la vision originelle d'internet, un internet diversifié, non monopolistique et non privatisé[217] » que promeut l'Europe. Plus précisément, Europe et communs numériques partagent, selon la diplomatie française, certains objectifs : « préservation de l'intérêt général, libre concurrence, neutralité du Net, protection des données personnelles, soutenabilité écologique[218] ».

Il convient de distinguer ici l'*open source* des communs numériques. Les seconds sont plus ambitieux puisqu'ils recoupent les notions de gouvernance collaborative, de données ouvertes, de logiciels libres et de standards ouverts[219]. La vision et les principes « libristes » restent défendus par les communautés OS, et par les entreprises numériques de taille réduite, mais

214. Selon le Open Source Contributor Index, disponible sur : https://opensourceindex.io. En août 2022, on compte deux entreprises européennes dans le top 20 (SAP, 10e, et SUSE, 16e), trois entreprises chinoises (Huawei, Tencent et Alibaba, respectivement, 12e, 13e et 15e contributeur), et 15 entreprises américaines dans le top 20.
215. K. Blind *et al.*, « The Impact of Open Source Software », *op. cit.*, p. 15. [Nous traduisons.] Ce constat est partagé dans le rapport de l'European Union Intellectual Property Office, « Open source Software », *op. cit.*
216. J. Zemlin, « Keynote », *op. cit.*
217. « Pour que les communs numériques deviennent un pilier de la souveraineté numérique européenne », Médiapart, 20 juin 2022, disponible sur : https://blogs.mediapart.fr.
218. B. Pajot, « Des barbelés sur la prairie Internet », *op. cit.*, p. 4.
219. « Towards a Sovereign Digital Infrastructure », European Working Team on Digital Commons, p. 2.

ils n'ont pas été respectés par les grands groupes technologiques[220]. Selon les défenseurs des communs, ces principes sont mis à mal par les « stratégies d'enfermement » qui sont celles d'autres États et de grandes entreprises[221]. Ainsi, si tous les communs sont basés sur le code et/ou les données ouvertes, tous les composants *open source* ne sont pas des « communs », selon les stratégies des entreprises en termes de licences.

L'attachement aux principes libristes et aux communs entraîne également des réticences face aux communautés *open source* nord-américaines du fait de la pénétration de l'industrie numérique. Les activistes « libristes » regrettent le rachat de GitHub par Microsoft[222] et encouragent à recourir à et soutenir d'autres plateformes collaboratives alternatives, comme le suggère une récente tribune signée par des acteurs français du libre[223]. Au sein du gouvernement français, cette vision est portée par l'Ambassadeur pour le numérique, Henri Verdier, qui résume ainsi les enjeux :

> « Plus vous avez de ressources gratuites, de logiciels OS, plus vous construisez votre économie sur des biens communs numériques, plus vous êtes libre, car personne ne peut vous exproprier, ni changer les prix ni vous imposer des choix technologiques. [C'est pourquoi nous avons introduit la notion de biens communs dans le débat.] Nous savons que parfois vous pouvez avoir une stratégie prédatrice, une stratégie de capture, à travers l'*open source*. L'OS seul ne suffit pas. Si j'ouvre mon code source mais que je contrôle les *commits*, je reste le maître de l'écosystème et je contrôle l'écosystème.[224] »

Certains projets européens viennent concrétiser cette ambition de préservation des communs. L'Inria, avec le soutien de l'Organisation des Nations unies pour l'éducation, la science et la culture (UNESCO), est à l'origine du projet Software Heritage, lancé en 2016. L'objectif du projet est de collecter tous les logiciels accessibles au public sous forme de code source avec leur historique de développement, de les répliquer massivement pour assurer leur préservation et de les partager avec tous ceux qui en ont besoin[225].

220. M. O'Neil *et al.*, « Le pillage de la communauté », *op. cit.*
221. « Pour que les communs numériques », Médiapart, *op. cit.*
222. M. O'Neil *et al.*, « Le pillage de la communauté », *op. cit.*
223. « Pour que les communs numériques », Médiapart, *op. cit.*
224. H. Verdier, « Open Source: Driving the European Digital Decade », Open Forum Europe, Conférence, Brno (République tchèque), 16 septembre 2022, disponible sur : www.youtube.com (minute 51'). « *The more you have free resources, OS software, the more you build your economy on digital commons, the freer you are, because no one can expropriate you, nor change the prices nor impose to you technological choices. [That is why we introduced the notion of "commons" in the debate.] We know that sometimes you can have predatory strategy, a capture strategy, through open source. OS alone is not enough. If I open the source of my code but I control the commits, I'm still the master of the ecosystem and I control the ecosystem* ». [Nous traduisons.]
225. « FAQ », Software Heritage, non daté, disponible sur : www.softwareheritage.org.

L'*open source* comme outil de la souveraineté numérique européenne

L'intérêt politique renouvelé pour l'*open source* en Europe s'articule, en parallèle, avec l'ambition affichée de construire une souveraineté numérique européenne. Au cœur des infrastructures technologiques, et donc de cette souveraineté recherchée, se trouvent les logiciels et les standards technologiques[226]. La création « d'infrastructures logicielles et matérielles, ouvertes et partagées en tant que communs numériques mondiaux » est ainsi présentée comme le quatrième pilier du chantier de cette souveraineté technologique européenne, aux côtés de la sécurisation du cyberespace, de la régulation juridique et économique du marché numérique, et de la capacité européenne d'innovation[227]. La souveraineté numérique doit permettre à l'Europe, face aux tensions croissantes entre les États-Unis et la Chine « porteuses de pénuries et d'un possible découplage technologique entre les deux blocs », « d'assurer son autonomie tout en évitant un alignement forcé et inconditionnel[228] ». Le refus de l'alignement forcé explique que les solutions *open source* logicielles et matérielles sont notamment poursuivies et promues par l'Europe en réponse aux sanctions et restrictions au commerce des technologies[229].

Selon Bruno Sportisse, P.-D.G. d'Inria, pour qu'il ne soit pas qu'une idéologie, mais contribue directement à la souveraineté numérique et à la politique industrielle, et crée de la valeur sur le plan économique, l'*open source* doit être porté par des entreprises privées[230]. De fait, outre les avantages économiques de l'OS pour les entreprises que nous avons évoqués dans les cas d'étude précédents, les entreprises européennes justifient également le recours et la contribution à l'OS selon des arguments politiques. Ainsi, un représentant de l'entreprise logicielle allemande SAP a donné l'exemple des applications de traçage des contacts au début de la pandémie de Covid-19 : le recours à des solutions *open source* était pour l'entreprise un moyen d'assurer la transparence de la solution technologique et gagner ainsi la confiance du public[231]. SAP a par ailleurs annoncé en septembre 2022 être membre inaugural de Linux Foundation Europe, justifiant cette participation comme une démarche contribuant à la « souveraineté européenne[232] ». Dans la même veine, l'éditeur de logiciels d'ingénierie et fournisseur de *cloud* Dassault Systèmes (ou 3DS) a conclut un partenariat avec Netframe (espace

226. S. Rolland, « "Il n'y aura pas de souveraineté numérique européenne sans maîtrise du logiciel", Bruno Sportisse, Inria », *La Tribune*, 22 février 2022.
227. « Conférence "Construire la souveraineté numérique de l'Europe" », Présidence française du Conseil de l'Union européenne, 5 février 2022, disponible sur : https://presidence-francaise.consilium.europa.eu.
228. T. Breton, « Géopolitique technologique : il est temps pour l'Europe de jouer ses cartes », Blog de la Commission européenne, 11 octobre 2021, disponible sur : https://ec.europa.eu.
229. N. Flaherty, « European Processor Project Shows Shift to RISC-V », EE News Europe, 23 décembre 2021, disponible sur : www.eenewseurope.com.
230. Entretien, Bruno Sportisse, P.-D.G. d'Inria, 13 juillet 2022.
231. V. Chandrasekhara, « Keynote: How Can the LF Enable Europe to Collaborate Locally and Innovate Globally », Open Source Summit Europe 2022, Dublin, 14 septembre 2022.
232. *Ibid.*

de travail collaboratif) et Nexidi (éditeur de logiciels libres) pour une offre logicielle conjointe dans l'*edge* et le *cloud*. Leur communiqué met en avant la maîtrise de l'ensemble des briques technologiques en Europe et une offre « compatible avec l'émergence du Splinternet et résiliente aux ruptures géopolitiques, comme les sanctions économiques sur les marchés à l'export » en s'appuyant sur une « base *open source* souveraine[233] ». On retrouve cet argumentaire pour l'*open source* dans le *hardware*, dans la mesure où l'Europe, comme la Chine, s'appuie sur l'architecture ouverte de microprocesseurs, RISC-V, pour développer ses semi-conducteurs[234].

Comment généraliser le recours à l'*open source* dans le secteur privé et contribuer à cette ambition de souveraineté *par* l'*open source* ? Du point de vue des représentants français, l'Europe doit pouvoir répliquer les réussites de l'*open source* à l'international, comme les logiciels chinois Appolo pour les véhicules autonomes, développés plus rapidement que les systèmes Tesla[235]. On peut également avancer des arguments économiques en faveur d'un plus grand recours à l'OS au sein de l'industrie européenne. L'OS représente un impact économique positif au PIB de l'UE estimé entre 65 et 95 milliards d'euros pour l'année 2018, pour un total d'un milliard d'euros investis par les entreprises[236]. Le rapport de la Commission européenne, cité plus haut, estime par ailleurs que si les contributions des entreprises européennes à l'*open source* croissaient de 10 %, cela entraînerait potentiellement une augmentation du PIB de l'UE de 100 milliards d'euros, et la création de 1 000 entreprises numériques par an[237].

Une mobilisation croissante de l'UE et des États membres

Du fait des objectifs européens, relevant de la préservation des « communs » et de la quête de souveraineté numérique, les États européens et l'UE se mobilisent de plus en plus pour adopter l'*open source*, développer des logiciels ouverts, assurer la cybersécurité de ces solutions et financer l'écosystème. On a noté que l'*open source*, dans les stratégies des grandes entreprises de la tech, peut être un outil de domination business, et l'animation de communautés OS, un enjeu de marketing. De fait, les grandes fondations structurantes, qui jouent un rôle dans sa capacité à atteindre une « souveraineté numérique », sont américaines. Cela pose un ensemble de questions pratiques : comment s'impliquer dans la gouvernance de ces organisations et dans le développement des codes, comment financer des

233. « À l'occasion de Vivatech, la startup netFrame s'associe avec Dassault Systèmes et Nexedi, ainsi que Docaposte comme partenaire technologique, pour proposer une suite collaborative souveraine sur l'infrastructure *cloud* de confiance et souveraine 3DS OUTSCALE », Communiqué, Netframe, 13 juin 2022.
234. C. Meinhardt, « Open Source of Trouble: China's Efforts to Decouple From Foreign IT Technologies », MERICS, 18 mai 2020, disponible sur : https://merics.org.
235. Entretien, chargé de mission auprès de l'Ambassadeur pour le Numérique, 18 juillet 2022.
236. K. Blind *et al.*, « The Impact of Open Source Software », *op. cit.*
237. *Ibid.*

projets étrangers, ou comment attirer des développeurs étrangers. Dès lors, l'Europe peut se trouver démunie dans ses moyens d'action, face à des acteurs établis à l'étranger.

Adopter l'*open source* dans l'administration et les services publics

Les pays européens occupent les premières places des classements Open Data Barometer et Open Knowledge Foundations' Global Open Data Index[238]. La principale ligne d'action des pouvoirs publics européens (au niveau des États membres comme de l'UE) a consisté à développer l'usage de l'OS au sein des administrations en réponse à leurs besoins, et à ouvrir les codes et les données produits par les institutions publiques.

En France, l'implication du gouvernement dans l'adoption de solutions OS au sein des administrations s'est accrue ces dernières années. Le narratif en faveur de recourir à l'*open source* repose sur les enjeux de transparence et de démocratie, de science et d'innovation ouvertes, et de qualité de l'action publique[239]. En 2020, un rapport supervisé par le sénateur Éric Bothorel et remis au Premier ministre préconisait la création d'un *Open source Program Office* (OSPO) en France, comme il en existe dans un nombre croissant de gouvernements et d'entreprises[240]. Peu de temps après, en avril 2021, une circulaire du Premier ministre Jean Castex – la première sur le sujet depuis 2012, qui avait permis à la France de se placer « à l'avant-garde européenne de la politique de la donnée et des codes sources » – faisait du logiciel libre et des données ouvertes une « priorité stratégique de l'État[241] ». L'ambition portait notamment sur un renforcement de l'ouverture des codes source et des algorithmes publics, et de l'usage du logiciel libre et ouvert au sein des administrations[242]. En juin 2021, le député Philippe Latombe publiait un rapport sur la souveraineté numérique suggérant d'« imposer au sein de l'administration le recours systématique au logiciel libre, en faisant de l'utilisation de solutions propriétaires une exception[243] ».

En septembre 2021 furent nommés des Administrateurs ministériels des données, des algorithmes et des codes sources (AMDAC) dans tous les ministères[244], puis un « Plan d'action logiciels libres et communs numériques » fut élaboré et lancé en novembre, portée alors par la ministre

238. « Towards a Sovereign Digital Infrastructure », *op. cit.*, p. 10.
239. « Mission Bothorel – Pour une politique publique de la donnée », Gouvernement, décembre 2020, p. 6.
240. *Ibid.* Un OSPO est une équipe qui supervise la stratégie d'une entité (gouvernement, entreprise) dans l'*open source* (besoins, contributions, enjeux de licence, réutilisation de composants…).
241. « Politique publique de l'*open source* en France : 2021, une année pleine de promesses », Systematic, 2 janvier 2022, disponible sur : https://systematic-paris-region.org.
242. *Ibid.*
243. « Bâtir et promouvoir une souveraineté numérique nationale et européenne », Rapport d'information, n° 4299, Assemblée nationale, 29 juin 2021, p. 139.
244. « Données, algorithmes et codes sources : une mobilisation générale sans précédent, à travers 15 feuilles de route ministérielles », Gouvernement, 27 septembre 2021, disponible sur : www.numerique.gouv.fr.

de la Transformation et de la Fonction publiques, Amélie de Montchalin[245]. Le plan d'action, qui s'appuie sur un investissement de 30 millions d'euros, ambitionne notamment de diffuser la connaissance et l'emploi des logiciels libres et communs numériques dans l'administration, et de valoriser les contributions publiques aux projets et communautés *open source*[246].

La Commission européenne a, pour sa part, mis à jour et étendu sa stratégie pour l'*open source* en 2020, en l'articulant avec l'ambition d'« autonomie numérique ». Dans la foulée, la Commission a créé un OSPO dont le rôle est de faciliter la mise en œuvre de la stratégie et de son plan d'action[247]. Si l'OSPO a été créé en 2020, il ne s'est pas réuni en personne avant le 15 septembre 2022, en marge d'un événement à Brno dans le cadre de la présidence tchèque du Conseil. Lors de ce même événement, la Direction générale de l'informatique (DGIT) de la Commission européenne a annoncé le lancement d'une plateforme de dépôt pour les institutions européennes, pour héberger une centaine de projets et partager les solutions OS développées par la Commission[248].

(Co-)développer des logiciels *open source*

Comme expliqué dans les cas américain et chinois, le secteur public ne se contente pas d'utiliser des solutions logicielles *open source*, mais développe également ce type de solutions – soit pour répondre aux besoins de l'administration soit, dans une démarche de partenariat public-privé pour contribuer, par les financements et la recherche publics, à co-développer des solutions *open source* à destination de l'industrie et du secteur privé. À nouveau, des exemples peuvent être tirés du cas français, où l'État, en partenariat avec des entreprises, développe des solutions en *open source* pour des briques logicielles critiques dans différents domaines émergents, tels que l'IA, l'analyse des données et l'IoT.

L'Inria a développé Scikit-learn, une boîte à outils *open source* d'intelligence artificielle pour l'analyse de données. Scikit-learn se place parmi les principales solutions de *data science* de rang mondial, en concurrence avec PyTorch (Meta) et Tenserflow (Google)[249]. L'entreprise française Data Iku, l'une des principales entreprises françaises de l'IA qui a désormais son siège aux États-Unis, a développé son business à partir de Scikit-learn[250]. L'ambition de l'Inria est bien d'encourager d'autres

245. « Plan d'action logiciels libres et communs numériques », Gouvernement, mis à jour le 16 novembre 2022, disponible sur : www.numerique.gouv.fr.
246. « Politique publique de l'*open source* en France », Systematic, *op. cit.*
247. « Open-Source Software Strategy 2020-2023 », Commission européenne, 21 octobre 2020, disponible sur : https://ec.europa.eu ; « EC Open Source Programme Office », Commission européenne, non daté, disponible sur : https://joinup.ec.europa.eu.
248. A. Thévenet, « The European Commission Announces code.europa.eu at OFE Event in Brno », Open Forum Europe, 23 septembre 2022, disponible sur : https://openforumeurope.org.
249. S. Rolland, « Il n'y aura pas de souveraineté numérique européenne sans maîtrise du logiciel », *op. cit.*
250. Entretien, Bruno Sportisse, P.-D.G. d'Inria, 13 juillet 2022.

entreprises à développer des outils numériques sur la base de la solution française Scikit-learn, plutôt que sur les solutions américaines[251].

Un autre projet de solution *open source* dans l'IA est le projet de traitement automatique de langage naturel multilingue, BLOOM (pour *BigScience Large Open-science Open-access Multilingual Language Model*). Ce projet, entraîné sur le supercalculateur français Jean Zay, a été officiellement lancé en juillet 2022[252]. Mille chercheurs volontaires ont participé au projet BigScience, co-financé par le gouvernement français et la plateforme d'IA *open source*, Hugging Face[253]. À la différence d'autres grands modèles de langues, tels que le GPT-3 de OpenAI et le LaMDA de Google, qui sont des solutions propriétaires et dont le code et les modèles AI sont fermés, BLOOM se veut responsable et transparent. Les chercheurs partageront des détails sur les données sur lequel le modèle est entraîné, les défis rencontrés dans son développement, et l'évaluation de sa performance[254]. Le programme est disponible en téléchargement sur le site Web de Hugging Face[255]. Autre spécificité, le modèle est entraîné sur des données multilingues, et il est actuellement capable de générer du texte dans 46 langues différentes[256].

Assurer la cybersécurité de l'*open source*

Préoccupée par la sécurité des logiciels *open source*, l'UE a mis en place en 2016 un projet pilote d'audit des logiciels, FOSSA (*Free and Open Source Software Auditing*), sur la base d'une initiative du Parlement européen suite à la faille Heartbleed[257]. Dans ce cadre, l'UE a organisé des *bug bounties* (récompenses financières offertes à des individus qui identifient et rapportent des bogues et failles dans les logiciels) pour les solutions *open source* utilisées par les institutions européennes, ainsi que des *hackatons*, des réunions de développeurs visant à identifier collectivement des solutions à des problématiques communes.

L'UE prévoit actuellement 200 000 euros pour son programme de chasse aux bogues, avec des récompenses de l'ordre de 5 000 euros, aux ingénieurs qui identifient des failles. Les *bug bounties* sont principalement organisés par des entreprises, dont les grandes entreprises technologiques américaines, si bien qu'il y a « une véritable concurrence économique autour

251. *Ibid*.
252. E. Gibney, « Open-Source Language AI Challenges Big Tech's Models », *Nature*, 22 juin 2022, disponible sur : www.nature.com ; A. Vitard, « Un millier de chercheurs ont développé un modèle de langue multilingue en *open source* », *L'Usine Digitale*, 13 juillet 2022, disponible sur : www.usine-digitale.fr.
253. M. Heikkilä, « Inside a Radical New Project to Democratize AI », *op. cit*.
254. *Ibid*.
255. « Bloom LM Version 1.0 », Hugging Face, 26 mai 2022, disponible sur : https://huggingface.co.
256. « Introducing the World's Largest Open Multilingual Language Model: BLOOM », BigScience Blog, non daté, disponible sur : https://bigscience.huggingface.co.
257. « EU-FOSSA 2 – Free and Open Source Software Auditing », Commission européenne, non daté, disponible sur : https://ec.europa.eu.

des failles de sécurité[258] ». Dès lors, les montants proposés par l'UE peuvent sembler « modestes » par rapport aux sommes que ces entreprises peuvent offrir pour sécuriser des logiciels propriétaires[259].

L'initiative FOSSA a été suivie par le projet pilote FOSSEPS, lancé en 2021, qui poursuit les *bug bounties*, et mène un travail plus large, en vue d'identifier les logiciels *open source* les plus critiques utilisés dans les services publics européens, et de créer un inventaire en vue d'identifier les dépendances européennes dans les composants OS qui « pourraient être dans un état de santé critique – c'est-à-dire des logiciels en danger d'arrêt, des mises à jour logicielles en cours et des corrections de bogues[260] ». L'inventaire ainsi que toute la méthodologie utilisée pour l'analyse des dépendances ont été rendus publics par l'UE.

Des démarches d'inventaire sont également en mises en place au niveau des États membres. En juin 2022, un partenariat de trois ans a été signé entre l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et le Commissariat à l'énergie atomique et aux énergies alternatives (CEA), pour mettre en œuvre de nouvelles approches pour vérifier l'absence de vulnérabilités dans les logiciels en phase de conception et d'intégration. Pour ce faire, les équipes du CEA et le l'ANSSI utiliseront notamment une plateforme d'analyse automatique de code, Frama-C, développée par le CEA et l'Inria et publiée en *open source*, qui permet la détection exhaustive d'une classe de vulnérabilités logicielles » et « l'évaluation en vue de certification de produits de sécurité aux niveaux les plus exigeants[261] ».

Enfin, l'UE a adopté en septembre 2022 le *Cyber Resilience Act*. Cette loi, portant sur la cybersécurité dans son ensemble, prévoit la mise en place d'un équivalent de *Software Bills of Materials* (SBOMs), requérant des éditeurs de logiciels qu'ils identifient et documentent les composants contenus dans leurs produits[262]. Ces listes ne seront pas requises pour les programmes publiés sous licence libre sans but commercial. Cependant, ces listes identifieront nécessairement des composants OS, dans la mesure où ils sont présents dans la quasi-totalité des logiciels, y compris propriétaires.

258. « Log4j », *Le Monde*, *op. cit.*
259. J. Lausson, « LibreOffice, Mastodon : l'UE offre 200 000 € pour sécuriser certains logiciels libres », Numérama, 24 janvier 2022, disponible sur : https://www.numerama.com.
260. S. S. Arora, « Call for Contributions to Help Identify Europe's Most Critical Open Source Software », FOSSEPS, Commission européenne, 23 mars 2022, disponible sur : https://joinup.ec.europa.eu. [Nous traduisons.]
261. « L'ANSSI et le CEA renforcent leur collaboration en cybersécurité », *op. cit.*
262. « Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 », COM(2022) 454 final, Commission européenne, 15 septembre 2022, art. 37 et art. 10.

Financer l'*open source*

Ainsi, les acteurs publics européens (États, UE), s'investissent de plus en plus dans l'OS, que ce soit pour en généraliser l'usage dans les administrations, (co-)développer des solutions logicielles, ou œuvrer à la cybersécurité des systèmes informatiques. Un autre moyen d'action de la puissance publique dans l'OS concerne le financement de l'écosystème, en vue de le soutenir, l'aider à se développer, et en assurer la maintenance. Ici, aussi, on constate une évolution vers une plus grande implication de l'UE et des États.

L'initiative de l'UE *Next Generation Internet* (NGI), pilotée par la DG CONNECT, est un véhicule de financement. Il soutient des projets *open source* qui contribuent au développement d'un « *human-centered internet* » c'est-à-dire contribuant à offrir aux utilisateurs des alternatives sur tous les éléments de la stack logicielle, respectueux de la législation européenne (RGPD), et favorisant la confiance, l'inclusivité et le multilinguisme[263]. Alors qu'il a un temps en partie soutenu des projets d'entreprises développant des produits ou solutions propriétaires, le NGI finance désormais uniquement des projets *open source*. Le NGI part du constat que les systèmes de financement européen de la recherche, tels que le programme Horizon, sont peu compatibles avec la dynamique du monde numérique et l'*open source* : ce sont souvent des financements d'ampleur nécessitant des équipes multi-pays, alors que les projets *open source* sont généralement produits et maintenus par des individus ou des petites équipes[264]. Les 82 millions d'euros du NGI pour la période 2018-2020 ont été alloués à environ 800 projets, portés à 80 % par des individus et pour 90 % basés en Europe (également certains projets au Royaume-Uni, aux États-Unis et en Asie). Environ 103 millions d'euros sont alloués pour la période 2021-2024.

Certains États membres sont également mobilisés pour soutenir financièrement l'écosystème *open source*. L'Allemagne a lancé en octobre 2022 le *Sovereign Tech Fund*[265]. Le projet est ambitieux. Il cherche notamment à s'attaquer à des problématiques souvent négligées de maintenance et de mise à l'échelle des programmes *open source* qui s'avèrent devenir des composants structurants de l'infrastructure logicielle[266]. La principale nouveauté est la création d'un fonds à destination d'individus, petites et moyennes entreprises, projets collectifs, ou communautés développant des technologies fondamentales dans différents domaines prioritaires : protocoles internet, certificats de sécurité, serveurs DNS et systèmes d'exploitation, compilateurs, bases de connaissances, gestion de serveurs… Le budget envisagé pour ce projet est de 10 millions d'euros par an.

263. Entretien, DG CONNECT, septembre 2022.
264. *Ibid.*
265. « Sovereign Tech Fund : Feasibility Study to Examine a Funding Program for Open Digital Base Technologies as the Foundation for Innovation and Digital Sovereignty », Open Knowledge Foundation Deutschland, octobre 2021, disponible sur : https://sovereigntechfund.de.
266. *Ibid*, p. 4.

Vers une approche plus stratégique ?

Comme on l'a évoqué, les pays UE sont parmi les meilleurs élèves en matière d'ouverture des données publiques, et une vision européenne politique de l'OS existe, ancrée dans les problématiques de souveraineté et de maintien d'un internet ouvert et collaboratif. Pour autant, les niveaux de connaissances des décideurs, de politisation et de pensée stratégique autour de la question des logiciels, et de l'*open source* en particulier, restent faibles et en tout cas moindres qu'aux États-Unis et en Chine[267].

On constate toutefois depuis le début de l'année 2022 une attention politique renouvelée pour le sujet. Au niveau de la Commission européenne, l'implication va croissant ; c'est un processus incrémental qui avance « pas à pas[268] ». Cette prise en compte politique est notamment le fait de la faille Log4Shell et de l'action la France, qui a détenu la présidence du Conseil de l'UE au premier semestre 2022. En février, la France a déclaré vouloir mettre en place une stratégie européenne pour les communs numériques et a lancé une invitation aux États membres pour la constitution d'une équipe de travail sur le sujet. Dix-neuf États membres ont répondu positivement[269], conduisant à une série de huit réunions sur quatre mois. Certains États membres participants ont indiqué n'avoir jamais traité de ce sujet auparavant, si bien que l'invitation française a permis de créer une « étincelle », de mettre le sujet sur la table et, pour ces États, d'envisager d'inclure l'*open source* et les communs dans leurs stratégies numériques nationales[270].

L'équipe de travail a publié en juin 2022 un rapport proposant une approche commune des communs numériques. Ils souhaitent notamment impliquer plus directement les décideurs politiques dans une approche plus large et plus stratégique de l'OS :

> « Il est frappant de constater que la grande majorité des initiatives en cours à tous les niveaux vise à encourager et à soutenir le développement, l'utilisation et l'achat de FLOSS et de communs numériques dans l'administration publique [...] Cependant, une stratégie pour les communs numériques ne peut être conçue avec un regard centré sur le service public.[271] »

267. « Towards a Sovereign Digital Infrastructure », *op. cit.* Entretien, DG CONNECT, septembre 2022 ; entretien, chargé de mission auprès de l'Ambassadeur pour le Numérique, 18 juillet 2022.
268. V. Daffey, « Open Source: Driving the European Digital Decade », Open Forum Europe, Conférence, Brno (République tchèque), 16 septembre 2022, disponible sur : www.youtube.com (minute 42).
269. Allemagne, Belgique, Croatie, République tchèque, Danemark, Espagne, Estonie, Finlande, France, Irlande, Italie, Lettonie, Luxembourg, Malte, Pays-Bas, Pologne, Portugal, Slovénie, Suède.
La Commission et le SEAE ont soutenu l'initiative, sans être impliqués directement dans la rédaction du rapport.
270. Entretien, chargé de mission auprès de l'Ambassadeur pour le Numérique, 18 juillet 2022.
271. « Towards a Sovereign Digital Infrastructure », *op. cit.*, p. 25-26. [Nous traduisons.]

Les auteurs appellent ainsi à identifier de manière pro-active les technologies émergentes nécessitant un développement en termes de protocole de langage et de logiciels, et de diriger des fonds vers certains domaines ou infrastructures clés – au-delà des outils de *e-government*[272]. Des exemples d'enjeux logiciels stratégiques pour l'Europe incluent les systèmes d'exploitation, les moteurs de recherche, les réseaux sociaux, ou encore les microprocesseurs[273]. Enfin, le rapport note un manque de coordination entre les initiatives européennes pour l'*open source*, qui sont pour la plupart développées à l'échelon national.

Face à ces constats, le rapport propose des pistes d'action :

- créer un guichet unique pour recueillir et centraliser les informations sur les programmes nationaux et européens de financement de l'OS, et faciliter le processus de candidature pour les développeurs et mainteneurs ;
- lancer des appels à projets multi-pays pour des projets OS européens dans des composants *open source* stratégiques ;
- établir une fondation européenne pour les Communs numériques. Cette structure autonome pourrait émerger sur la base du guichet unique, et pourrait être gouvernée collégialement par les acteurs des communs et de l'*open source*, les États membres et l'UE. Une telle structure permettrait d'« assurer l'indépendance vis-à-vis des organisations de droit étranger, et de promouvoir le développement d'innovations numériques fondées sur les valeurs éthiques européennes[274] ». Alternativement, la structure pourrait prendre la forme d'un partenariat public-privé, tel que celui qui existe dans la photonique. La structure viserait à animer l'écosystème OS européen, organiserait le soutien financier envers les communs, formulerait des recommandations politiques, piloterait les efforts de sécurisation et d'audit des composants *open source*, et offrirait une plateforme de dépôt de codes libre.

La mise en place d'une nouvelle structure européenne n'est pas l'issue la plus probable à ce stade. Mais on peut déjà noter que la présidence française du Conseil de l'UE a cédé la place à la présidence tchèque, qui au second semestre 2022, a poursuivi la réflexion et les efforts de sensibilisation des décideurs européens sur l'*open source*. Cette plus grande attention politique et cette vision plus stratégique de l'*open source*, ainsi que la relocalisation de fondations et l'ouverture de Linux Europe, indiquent que l'influence de l'UE et ses États membres sur l'écosystème *open source* mondial va continuer de croître, et que la vision européenne mérite d'être promue.

272. *Ibid*.
273. Entretien, DG CONNECT, septembre 2022.
274. « Towards a Sovereign Digital Infrastructure », *op. cit.*, p. 29.

Conclusion : l'*open source* au risque de la géopolitique ?

L'*open source* tient une place centrale dans le développement des logiciels, sur un mode à la fois parallèle au modèle propriétaire, et de plus en plus imbriqué avec celui-ci. Il est devenu un enjeu de taille pour le succès des entreprises du numérique. Au-delà, l'*open source* est au fondement de briques logicielles critiques et des langages et protocoles d'internet, et joue un rôle dans le développement de technologies émergentes. L'*open source* peut toutefois être victime de son succès et du manque de moyens mis en œuvre pour sa maintenance, comme l'ont illustré des cas récents de failles ayant des conséquences de portée mondiale. Dans le même temps, les entreprises privées investissent financièrement et humainement au développement et au maintien de l'écosystème. Ce soutien est critique pour pallier les risques liés au manque de maintenance de certains composants. Cependant, nous avons vu que cette implication n'est pas sans risque pour l'écosystème *open source*, qui est de plus en plus modelé par les intérêts privés des *Big Tech*.

Deux dynamiques cohabitent donc : une où l'*open source* est structurellement fragile malgré son importance stratégique, sur le plan économique et de la sécurité, et subit un manque de ressources notamment pour la maintenance des composants ; et l'autre où il est l'objet d'investissements et de captation, voire d'un dévoiement, par les grandes entreprises technologiques. Ces deux tendances créent des frustrations dans l'écosystème *open source* et peuvent entraîner le souhait de tendre vers un idéal qui autonomiserait les communautés *open source* des acteurs du secteur privés, bien que leur imbrication soit un fait. La question reste de savoir comment garantir que les intérêts du secteur privé ne détournent pas les principes de l'*open source* et, par extension, n'altèrent pas la valeur ajoutée de ce modèle.

Mais une troisième dynamique est également à l'œuvre : les États ont compris l'importance critique de l'*open source*, qui se constitue comme enjeu stratégique. Nous avons examiné comment les États-Unis, la Chine, et l'Union européenne et ses États membres se sont emparés du sujet. On observe que les motivations des États à investir dans l'*open source* peuvent découler de différents types d'objectifs :

1) accéder à des solutions technologiques de confiance dans le cadre de la numérisation de l'administration et des services publiques ;

2) assurer la cybersécurité en investissant dans la pérennité de l'écosystème et la maintenance des composants OS utiles à l'État et plus largement à l'architecture numérique globale ;

3) développer une industrie logicielle locale et réduire la dépendance vis-à-vis des logiciels propriétaires étrangers ;

4) préserver une certaine idée d'un espace numérique ouvert, public, commun et collaboratif.

Il n'est cependant pas aisé de développer des outils de politique publique pour se saisir d'un objet tel que l'*open source*[275]. Une difficulté est que les gouvernements ne peuvent pas agir à l'échelle des communautés OS, de leur gouvernance ou de leur structuration juridique, qui sont les fonctions remplies par les fondations. Ils ont aussi des moyens d'action limités concernant l'usage qui est fait par les entreprises privées de l'*open source*, ou face au dévoiement des principes de l'*open source* et des licences libres. L'action de l'État se concentre alors sur la sécurité et la maintenance des composants. Aux États-Unis et en Europe émergent des initiatives parallèles pour impliquer davantage les pouvoirs publics dans l'inventaire des composants *open source* critiques, dans l'examen des risques de sécurité, et dans le financement et la maintenance de ces composants, dans une approche public-privé.

Si l'intérêt des États pour cet enjeu stratégique est louable, on peut s'interroger sur les effets qu'aura cette plus grande implication des gouvernements sur l'écosystème *open source* où l'État n'était, jusqu'à récemment, qu'un consommateur et contributeur parmi tant d'autres. La cohérence entre ces différentes initiatives au niveau international doit être considérée, de façon à ne pas dupliquer les efforts ni créer des normes contradictoires, et à éviter les dérives sécuritaires. L'intérêt de disposer d'un entrepôt qui archive et sécurise les codes sources les plus utilisés est partagé par tous. Les outils développés par les pouvoirs publics pour améliorer la sécurité des logiciels, comme les *Software Bills of Materials* américains et de leur équivalent européen, pourraient aussi être harmonisés[276]. Un effort de coordination doit donc être fait.

275. Un constat fait également par les responsables de l'initiative sur l'*open source* du *think tank* américain Atlantic Council, lancée en juillet 2022. Ils estiment que les principes responsables du succès de l'*open source* – faibles barrières à l'entrée, transparence et collaboration – sont difficiles à naviguer en usant des outils politiques traditionnels. Lire « Atlantic Council Launches Open-Source Software Security Effort », Communiqué de presse, Atlantic Council, 18 juillet 2022.

276. C. Carey, « EU's Efforts to Secure Open Source Software », Open Source Summit Europe 2022, Dublin, 14 septembre, 2022.

Une autre dynamique autrement plus préoccupante concerne l'intrusion de la géopolitique dans les enjeux de l'écosystème mondial de l'*open source*. Aux États-Unis, les acteurs de la sécurité nationale identifient des risques d'ingérences dans les codes *open source* via des contributeurs travaillant pour des gouvernements étrangers. On a également évoqué le fait que les développeurs issus de pays sous sanctions américaines peuvent être suspendus de la plateforme GitHub, comme ce fut le cas avec l'Iran et aujourd'hui la Russie. Par ailleurs, certains voient dans l'*open source* le risque que des adversaires des États-Unis, au premier chef la Chine, s'en servent pour acquérir des technologies américaines et de contourner les sanctions. En Chine, le contrôle du gouvernement sur les communautés *open source* se renforce, alors que Pékin tente d'appliquer des principes techno-nationalistes à l'*open source*.

Toutes ces tendances risquent d'entraîner à la fois une fragmentation et une centralisation des communautés au niveau des États, ce qui serait nuisible à un écosystème aujourd'hui décentralisé et relativement horizontal. Le discours européen, lui, cherche à combiner les ambitions de souveraineté numérique et de préservation des communs numériques. Si sa marge de manœuvre a été jusqu'à présent moindre, dans la mesure où la plupart des grands acteurs de l'OS sont américains, l'Europe bénéficie de cet écosystème mondialisé, et son approche ouverte et moins sécuritaire qu'aux États-Unis en fait un acteur de plus en plus incontournable dans l'écosystème mondial. Cela a été démontré par la relocalisation d'Eclipse en Belgique et de RISC-V en Suisse, et la création de la branche « Europe » de la fondation Linux.

Enfin, la vision européenne doit s'articuler avec les positions diplomatiques de l'UE. Il existe certainement des pistes de coopération avec les États-Unis et d'autres pays dans les domaines où convergent à la fois les priorités des États et les intérêts des communautés *open source*, tels que l'inventaire et la maintenance des composants OS critiques. À l'inverse, la Chine est parfois qualifiée de possible « alliée objective » de l'UE dans certains domaines de l'*open source*, comme les processeurs[277]. Si la Chine partage l'objectif européen d'une plus grande autonomie face aux solutions propriétaires des *Big Tech*, le virage pris par le gouvernement chinois ne peut en faire un allié politique de l'ambition européenne. En revanche, il existe une réelle opportunité pour l'Europe de tendre la main à des partenaires, non seulement les États-Unis mais aussi l'Inde et le Brésil, qui pourraient adhérer à et aider à promouvoir cette vision visant à préserver les communs numériques et un internet ouvert, interopérable, respectueux des libertés et centré sur l'humain.

277. Entretien, DG CONNECT, septembre 2022.

27 rue de la Procession 75740 Paris cedex 15 – France

Ifri.org