Des routes et des ponts (9) – l'argent et l'open source

*Nadia Eghbal a déjà évoqué plusieurs fois les liens entre l'argent et l'*open source *(si vous avez manqué des épisodes). Elle y revient dans ce chapitre, en insistant sur les questions fondamentales que pose l'argent aux communautés* open source *ainsi qu'à leurs membres.*

Question de nature quasi-philosophique : l'open source *peut-il perdre son âme à cause de l'argent ? Question de gouvernance : qui va décider de l'utilisation des fonds ? Et pour finir question éthique et politique : jusqu'à où peut-on, doit-on accepter les requêtes des financeurs ?*

La relation compliquée de l'*open source* avec l'argent

Traduction Framalang : goudron, Penguin, serici, goofy, Rozmador, xi, Lumibd, teromene, xi, Diane, et 3 anonymes

L'argent est un sujet tabou dans les projets *open source*, et ce depuis les premiers jours du mouvement du logiciel libre qui émergea en réponse directe aux pratiques commerciales des logiciels propriétaires. Dans le contexte du mouvement du logiciel libre, l'aversion pour l'argent est tout à fait compréhensible. L'argent est ce qui permettait de commercialiser les logiciels dans les années 1980 et il a

fallu des décennies pour revenir sur cet état d'esprit et promouvoir les avantages liés à l'élaboration de logiciels qui soient libres d'utilisation, de distribution et de modification. Même si de nos jours, nous prenons les logiciels libres pour acquis, dans les années 1980, c'était une véritable contre-culture, un état d'esprit révolutionnaire.

Au sein même des communautés *open source*, il existe une croyance répandue selon laquelle l'argent est de nature à corrompre l'*open source*. Et en effet, le nombre de projets nés d'un « travail-passion » est assez incroyable. Aujourd'hui, le développement de logiciel est considéré comme un domaine lucratif, dont les écoles de programmation appâtent leurs futurs étudiants avec des promesses de premiers salaires en dollars à six chiffres. Par contraste, il y a quelque chose de pur et d'admirable dans le fait de créer un logiciel simplement pour le plaisir.

D'un point de vue plus pratique, les projets *open source* se créent traditionnellement autour d'un besoin réel et identifiable. Quelqu'un estime qu'un projet pourrait être mieux fait, décide de le *forker*, effectue des améliorations, puis les diffuse pour qu'on en fasse usage. Le pragmatisme est au cœur de la culture *open source*, comme le prouve sa scission stratégique avec le mouvement du logiciel libre à la fin des années 1990. Certains contributeurs *open source* craignent, peut-être avec raison, que l'argent n'introduise un développement « artificiel » du système, avec des développeurs qui lancent de nouveaux projets simplement pour acquérir des financements, plutôt que pour répondre à un besoin réel.

David Heinemeier Hansson (aussi connu sous le pseudo de DHH), qui a créé le *framework* populaire *Ruby on Rails*, mettait en garde en 2013 contre les mélanges entre *open source* et argent :

> *Si l'open source est une incroyable force pour la qualité et pour la communauté, c'est précisément parce qu'elle n'a pas*

> *été définie en termes de marché. Dans le cadre du marché, la plupart des projets open source n'auraient jamais eu leur chance.*
>
> *Prenez Ruby on Rails. […] C'est une réalisation colossale pour l'humanité ! Des milliers de gens, collaborant pendant une décennie entière pour produire une structure et un écosystème incroyablement aboutis, disponibles pour tous gratuitement. Prenez une seconde pour méditer sur l'ampleur de cette réussite. Pas seulement pour Rails, évidemment, mais pour de nombreux autres projets open source, encore plus grands, avec une filiation plus longue et encore plus de succès.*
>
> *C'est en considérant ce fantastique succès, dû aux règles de vie d'une communauté, que nous devrions être extraordinairement prudents avant de laisser les lois du marché corrompre l'écosystème.*

Structurellement, le meilleur atout de l'*open source* : son penchant pour la démocratie, est aussi sa faiblesse. Beaucoup de projets *open source* ne sont rien de plus qu'un dépôt numérique public où est stocké du code auquel un groupe de gens contribue régulièrement : l'équivalent d'une association officieuse sur un campus universitaire. Il n'y a pas de structure légale et il n'y a pas de propriétaire ou de chef clairement défini. Les « mainteneurs » ou les contributeurs principaux émergent souvent *de facto*, en fonction de qui a créé le projet, ou de qui y a investi beaucoup de temps ou d'efforts. Cependant, même dans ces cas-là, dans certains projets on répugne à introduire une hiérarchie favorisant clairement un contributeur par rapport à un autre.

En avril 2008, Jeff Atwood, un développeur .NET bien connu et dont nous avons déjà parlé, a annoncé qu'il donnait 5 000 $ au projet *open source* : *ScrewTurn Wiki*. *ScrewTurn Wiki* est un projet de wiki développé par Dario Solara, un autre

développeur .NET, et maintenu par des volontaires. Atwood a dit à Dario que le don était « sans condition » : Solara pouvait utiliser l'argent de la manière qu'il jugerait la plus utile au projet.
Plusieurs mois plus tard, Atwood demanda à Solara comment il avait décidé de dépenser l'argent. Solara lui répondit que l'argent de la donation était « *encore intact. Ce n'est pas facile de l'utiliser… Que suggères-tu* ? » Atwood a écrit que cette réponse l'avait « terriblement déçu ».

La nature décentralisée du monde *open source* en a fait ce qu'il est : des logiciels produits de façon participative, que n'importe qui peut élaborer, partager, et améliorer. Mais quand vient le moment de discuter des besoins organisationnels, ou de la viabilité, il peut être difficile de prendre des décisions faisant autorité.

Ces transitions vers une viabilité à long terme peuvent êtres interminables et douloureuses. Un des exemples les plus connus est le *noyau Linux*, un projet *open source* utilisé dans de nombreux systèmes d'exploitation à travers le monde, parmi lesquels Android et Chrome OS. Il a été créé en 1991 par Linus Torvalds, un étudiant en informatique .
Au fur et à mesure que le noyau Linux gagnait en popularité, Linus rechignait à discuter de l'organisation du développement du projet, préférant tout gérer tout seul. L'inquiétude et aussi la colère à l'égard de Torvalds grandirent chez les développeurs du projet, déclenchant de « vraies grosses disputes » selon Torvalds. Le conflit a atteint son apogée en 2002, on évoqua même un possible schisme.

Torvalds attribua ces conflits internes à un manque d'organisation, plutôt qu'à un quelconque problème technique :

> *Nous avons eu de vraies grosses disputes aux alentours de 2002, quand j'appliquais des correctifs à droite à gauche, et que les choses ne fonctionnaient vraiment pas. C'était très douloureux pour tout le monde, et également beaucoup pour*

> *moi. Personne n'aime vraiment les critiques, et il y avait beaucoup de critiques virulentes, et comme ce n'était pas un problème strictement technique, on ne pouvait pas juste montrer un correctif et dire : « Hé, regardez, ce patch améliore les performances de 15% » ou quoique ce soit de ce genre. Il n'y avait pas de solution technique. La solution a été d'utiliser de meilleurs outils, et d'avoir une organisation du travail qui nous permette de mieux distribuer les tâches.*

La Fondation Linux a été créée en 2007 pour aider à protéger et à maintenir Linux et ses projets associés. Torvalds ne pilote pas la Fondation Linux lui-même, il a préféré recevoir un salaire régulier en tant que « Compagnon Linux », et travailler sur ses projets en tant qu'ingénieur.

Malgré le fait que le logiciel *open source* soit admirablement ancré dans une culture du volontariat et de la collaboration relativement peu touchée par des motivations extérieures, la réalité est que notre économie et notre société, depuis les sociétés multimillionnaires jusqu'aux sites web gouvernementaux, dépendent de l'*open source*.

Dans l'ensemble, c'est probablement une évolution positive pour la société. Cela signifie que les logiciels ne sont plus limités à un développement privé et propriétaire, comme cela a été le cas pendant des dizaines d'années. Le fait que le gouvernement des États-Unis, ou un réseau social possédant des milliards d'utilisateurs, intègrent des logiciels construits par une communauté, annonce un futur optimiste pour la démocratie.

De plus, de nombreux projets fonctionnent très bien de manière communautaire lorsqu'ils sont d'une des deux tailles extrêmes possibles, c'est-à-dire soit des petits projets qui ne demandent pas de maintenance significative (comme dans l'exemple de Arash Payan et Appirater), soit de très gros

projets qui reçoivent un soutien important de la part d'entreprises (comme Linux).

Cependant, beaucoup de projets sont coincés quelque part entre les deux : assez grands pour avoir besoin d'une maintenance significative, mais pas d'une taille suffisante pour que des entreprises déclarent leur offrir un soutien. Ces projets sont ceux dont l'histoire passe inaperçue, ceux dont on ne parle pas. Des deux côtés, on dit aux développeurs de ces projets « moyens » qu'ils sont le problème : du côté des « petits projets », on pense qu'ils devraient simplement mieux s'organiser et du côté des « gros projets », on pense que si leur projet était « assez bon », il aurait déjà reçu l'attention des soutiens institutionnels.

Il existe aussi des intérêts politiques autour de la question du soutien financier qui rendent encore plus difficile la prospection d'une source de financement fiable. On peut imaginer qu'une entreprise seule ne souhaite pas sponsoriser le développement d'un travail qui pourrait également bénéficier à son concurrent, qui lui n'aurait rien payé. Un mécène privé peut exiger des privilèges spécifiques qui menacent la neutralité d'un projet. Par exemple, dans les projets en lien avec la sécurité, le fait d'exiger d'être le seul à qui sont révélées les potentielles failles (c'est-à-dire payer pour être le seul à connaître les failles de sécurité plutôt que de les rendre publiques) est un type de requête controversé. Des gouvernements peuvent également avoir des raisons politiques pour financer le développement d'un projet en particulier, ou pour demander des faveurs spéciales comme une « *backdoor* » (une porte dérobée, c'est-à-dire un accès secret qui permet d'outrepasser les authentifications de sécurité), même si le projet est utilisé dans le monde entier.

Les récents démêlés légaux entre le FBI et Apple sont un bon révélateur des tensions qui existent entre technologie et gouvernement, au-delà même des projets *open source*.
Le FBI a, de manière répétée, et à l'aide d'assignations en

justice, demandé l'aide d'Apple pour déverrouiller des téléphones afin d'aider à résoudre des enquêtes criminelles. Apple a toujours refusé ces requêtes. En février 2016, le FBI a demandé l'aide d'Apple pour déverrouiller le téléphone d'un des tireurs d'une attaque terroriste récente à San Bernardino, en Californie. Apple a également refusé de les aider, et a publié une lettre sur son site, déclarant :

> *Tout en croyant que les intentions du FBI sont bonnes, nous pensons qu'il serait mauvais pour le gouvernement de nous forcer à ajouter une « backdoor » dans nos produits. Et finalement, nous avons peur que cette demande mette en danger les libertés que notre gouvernement est censé protéger.*

En mars 2016, le FBI a trouvé une tierce partie pour l'aider à déverrouiller l'iPhone et a laissé tomber l'affaire.

Une des plus grandes forces de l'*open source* est que le code est considéré comme un bien public, et beaucoup de projets prennent la gestion de ces projets au sérieux. Il est important à titre personnel, pour beaucoup de développeurs de projets, que personne ne puisse prendre seul le contrôle d'une chose que le public utilise et dont il bénéficie. Toutefois, cet engagement à rester neutre a un prix, puisque beaucoup de ressources disponibles pour les développeurs de nos jours (comme les capitaux-risques ou les donations d'entreprises) attendent en contrepartie d'influer sur le projet ou des retours sur investissement.

Le logiciel *open source* est créé et utilisé de nos jours à une vitesse jamais vue auparavant. Beaucoup de projets *open source* sont en train d'expérimenter la difficile transition d'une création désintéressée à une infrastructure publique essentielle.
Ces dépendances toujours plus nombreuses signifient que nous avons pour responsabilité partagée de garantir à ces projets

le soutien dont ils ont besoin.

Crédits pour les 2 images Eelke (CC BY 2.0)

Les géants du Web nous veulent du bien

Lourdement mises en cause pour avoir laissé les agences gouvernementales accéder aux données de leurs clients, les grandes entreprises du Web ont vite senti qu'elles risquaient gros à passer aux yeux du monde entier pour des complices de l'espionnage de masse. Elles ont donc défendu leur position avec une belle énergie en clamant leur bonne foi : elles auraient été les victimes non consentantes des intrusions de la NSA.

Dans cette recherche d'une crédibilité essentielle pour leur survie économique – car à chaque utilisateur perdu c'est la monétisation d'un profil qui disparaît, elles multiplient les déclarations hostiles aux pressions, de plus en plus fortes aux USA, pour limiter voire interdire le chiffrement de haut niveau, comme pour leur imposer des portes dérobées. C'est ce que nous pouvons voir dans cette compilation réunie par l'EFF.

> L'*Electronic Frontier Foundation* est une organisation non gouvernementale qui mène depuis vingt-cinq ans un combat sur de multiples fronts pour les libertés numériques, comme le fait La Quadrature du Net, qui est un peu son équivalent pour la France et l'Europe.

À lire cette suite d'extraits choisis, on hésite un peu à donner pleine absolution à toutes ces entreprises à but parfaitement lucratif. Ces déclarations sont-elles sincères, et surtout sont-elles concrètement suivies d'effets ? Sciemment ou non, elles ont laissé l'espionnage s'installer au cœur de leur activité, et même au cœur d'un système d'exploitation hégémonique. Aujourd'hui elles voudraient préserver le chiffrement comme outil indispensable aux transactions économiques, soit. Mais on sait bien que par ailleurs elles n'ont guère de scrupules à faire commerce de nos données privées. Ce que ces entreprises états-uniennes redoutent surtout c'est que l'administration Obama (elle-même sous la pression des agences d'espionnage) « tue le business ».
Quoi qu'il en soit, l'EFF trouve en elles des alliées inattendues puissantes pour faire pression sur le plan politique : l'enjeu est de taille et peut justifier une aussi paradoxale alliance de circonstance. En effet, le chiffrement fort, attaqué par de nombreux gouvernements dans le monde sous prétexte de sécurité, demeure un rempart qui protège nos libertés numériques.

Où en sont les grandes entreprises du numérique sur la question du chiffrement ?

Une comparaison des positions affichées par 21 des plus importantes entreprises du numérique

Article original sur le site de l'EFF : Where Do Major Tech Companies Stand on Encryption?
Traduction Framalang : Luke, Obny, goofy, KoS, Niilos, McGregor

En ce moment même une bataille décisive fait rage autour du chiffrement.

Les services de police essaient d'imposer des « portes dérobées » (*backdoors*) pour accéder à nos données et nos communications sensibles, tandis que les groupes de défense des libertés individuelles répliquent par une campagne intitulée SaveCrypto. Quant au président Obama, il s'efforce de trouver un compromis, en évitant de donner à ces demandes la force d'une loi, mais en continuant de façon informelle à faire pression sur les entreprises pour qu'elles fournissent un accès sans chiffrement aux données qu'elles récoltent.

Où en sont donc les entreprises du numérique sur ce front ?

Elles sont les seules à être à la fois en position de connaître et de résister aux pressions officieuses exercées par le gouvernement pour qu'elles donnent accès aux données de leurs utilisateurs. Nous leur offrons sur un plateau de gigantesques quantités de données sensibles tout en leur faisant confiance pour qu'elles les gardent en sécurité. Quelles sont les entreprises qui souhaitent afficher publiquement leur opposition aux portes dérobées ?

Nous avons rassemblé les politiques publiques des 21 plus

importantes entreprises du numérique pour que vous puissiez les comparer. Certaines des déclarations proviennent de notre rapport annuel *Who has your back* et quelques-unes de blogs et de rapports sur la transparence issus des entreprises..

Voyez plutôt vous-même :

Adobe

> *Adobe n'a aménagé de « porte dérobée » pour aucun gouvernement – ni étranger ni américain – dans ses produits et ses services. Toutes les demandes du gouvernement pour obtenir des données de nos utilisateurs doivent passer par la grande porte (c'est-à-dire en menant suivant une procédure légale valide auprès du département juridique approprié d'Adobe). Adobe s'oppose vigoureusement à toute législation aux USA ou à l'étranger qui affaiblirait de quelque manière que ce soit la sécurité de nos produits ou la protection de la vie privée de nos utilisateurs.*

Amazon

> *Alors que nous reconnaissons qu'il est légitime et nécessaire pour les autorités de mener des enquêtes sur le crime et les activités terroristes, qu'il est nécessaire de coopérer avec les autorités quand elles respectent le cadre légal pour mener de telles investigations, nous sommes opposés à une législation qui interdirait les technologies de sécurité et de chiffrement ou les soumettrait à une demande d'autorisation, cela aurait pour effet d'affaiblir la sécurité des produits, systèmes et services qu'utilisent nos clients, qu'ils soient des particuliers ou des entreprises.*

Apple

> *De plus, Apple n'a jamais travaillé avec quelque agence gouvernementale de quelque pays que ce soit pour créer des « portes dérobées » dans nos produits ou services. Nous*

> *n'avons non plus jamais permis à un quelconque gouvernement d'accéder à nos serveurs. Et nous ne le ferons jamais.*

L'entreprise Apple mérite d'être saluée pour sa prise de position encore plus ferme contre les portes dérobées sur son nouveau site consacré au respect de la vie privée qui explique la politique de l'entreprise. Cette nouvelle déclaration indique :

> *Le chiffrement sécurise des milliers de milliards de transactions en ligne chaque jour. Que ce soit en passant commande ou en payant, vous utilisez du chiffrement. Vos données sont transformées en un texte indéchiffrable qui ne peut être lu que si on dispose de la bonne clé. Depuis plus de dix ans nous protégeons vos données avec SSL et TLS [liens ici] dans Safari, FileVault pour Mac, et le chiffrement qui existe par défaut dans iOS. Nous refusons également d'ajouter des portes dérobées au moindre de nos produits parce qu'elles sapent les protections que nous avons mises au point. Et nous ne pouvons déverrouiller votre appareil pour personne parce que vous seul en avez la clé, votre unique mot de passe. Nous sommes résolus à utiliser un chiffrement fort parce que vous devez avoir la certitude que les données que contient votre appareil et les informations que vous partagez avec d'autres sont protégées.*

Comcast

> *Comcast ne soutient pas la création de portes dérobées extra-légales ou l'insertion délibérée de failles de sécurité, dans les logiciels open source ou autres, pour faciliter la surveillance sans procédure légale appropriée.*

Dropbox

> *Les gouvernements ne devraient jamais installer de portes dérobées dans les services en ligne ou compromettre les*

infrastructures pour obtenir des données personnelles. Nous continuerons à travailler pour protéger nos systèmes et pour changer les lois afin d'établir clairement que ce type d'activité est illégal.

Nous constatons également que partout dans le monde, des administrations essaient de limiter les mesures de sécurité comme le chiffrement sans pour autant faire de progrès sur le renforcement de la protection légale que méritent les gens. Il en résulte les gouvernements demandent actuellement des informations sur une toute petite partie de nos clients, mais cherchent de plus en plus à perturber l'équilibre entre vie privée et sécurité publique d'une manière qui concerne tout le monde.
Comme nous le disions précédemment, les autorités ont parfois besoin d'accéder aux données privées pour protéger les citoyens. Cependant, cet accès devrait être réglementé par la loi et non en réclamant des « portes dérobées » ou en affaiblissant la sécurité de nos produits et services utilisés par des millions de clients respectueux de la loi. Ceci devrait concerner chacun d'entre nous.

Pinterest

Pinterest s'oppose aux portes dérobées contraintes et soutient les réformes visant à limiter les demandes de surveillance de masse.

Slack

La transparence est une valeur clé pour nous et une caractéristique importante de Slack lui-même. C'est cet engagement pour la transparence qui amène mon dernier point – Slack s'oppose aux portes dérobées des pouvoirs publics de toutes sortes, mais particulièrement aux exigences des gouvernements qui pourraient compromettre la sécurité des données.

Snapchat

> *La confidentialité et la sécurité sont des valeurs essentielles chez Snapshat, et nous nous opposons fermement à toute initiative qui viendrait affaiblir la sécurité de nos systèmes. Nous nous engageons à gérer vos données de manière sécurisée et mettrons à jour ce rapport tous les six mois.*

Sonic

> *Enfin, nous déclarons publiquement notre position concernant l'inclusion forcée de portes dérobées, failles de sécurité volontaires ou divulgation de clés de chiffrement. Sonic ne soutient pas ces pratiques.*

Tumblr

> *Sécurité : nous croyons qu'aucun gouvernement ne devrait installer de portes dérobées dans les protocoles de sécurité du web, ou encore compromettre l'infrastructure d'internet. Nous combattrons les lois qui permettraient cela, et nous travaillerons à sécuriser les données de nos utilisateurs contre de telles intrusions.*

Wickr

> *Nous croyons au chiffrement robuste et généralisé et exhortons le gouvernement des États-Unis à adopter des normes de chiffrement fort pour assurer l'intégrité de l'information des particuliers, des entreprises et des organismes gouvernementaux à travers le monde.*

WordPress

> *Certains gouvernements ont récemment cherché à affaiblir le chiffrement, au nom de l'application de la loi. Nous sommes en désaccord avec ces suggestions et ne croyons pas qu'il*

> *soit possible d'inclure une quelconque faille de sécurité délibérée ou autres portes dérobées dans les technologies de chiffrement, même pour le « seul » bénéfice des services de sécurité. Comme l'a dit un sage, « il n'existe pas de faille technologique qui puisse être utilisée uniquement par des personnes bienveillantes respectueuses de la loi ». Nous sommes entièrement d'accord.*

Yahoo

> *Nous avons chiffré beaucoup de nos principaux produits et services pour les protéger de l'espionnage des gouvernements et autres acteurs. Ceci inclut le chiffrement du trafic entre les centres de données de Yahoo ; l'utilisation de HTTPS par défaut sur Yahoo Mail et la page d'accueil de Yahoo ; et l'implémentation de règles de bonne pratique en matière de sécurité, y compris le support de TLS 1.2, de la Confidentialité persistante et d'une clé RSA 2048 bits pour la plupart de nos services tels que la page d'accueil, la messagerie et les magazines numériques. Nous avons également mis en place une extension de chiffrement de bout en bout (e2e) pour Yahoo Mail, disponible sur GitHub. Notre but est de fournir une solution de chiffrement e2e intuitive à tous nos utilisateurs d'ici la fin 2015. Nous sommes engagés sur la sécurité de cette solution et nous opposons aux demandes de l'affaiblir délibérément ainsi que tout autre système de chiffrement.*

Credo Mobile, Facebook, Google, LinkedIn, Twitter, WhatsApp, et la Wikimedia Foundation ont tous signé une lettre proposée par l'Open Technology Institute (OTI) qui s'oppose à l'affaiblissement volontaire des mesures de sécurité :

> *Nous vous exhortons à rejeter toute proposition poussant les entreprises américaines à affaiblir délibérément la sécurité de leurs produits… Que vous les appeliez portes avant ou portes dérobées, le fait d'introduire délibérément des*

vulnérabilités à usage gouvernemental dans des produits sécurisés à l'intention du gouvernement rendra ces produits moins sécurisés face à d'autres attaquants. Tous les experts en sécurité qui se sont exprimés sur cette question sont d'accord, y compris ceux du gouvernement.

Que pouvons-nous en conclure ? Il existe une très forte opposition des entreprises technologiques aux portes dérobées imposées.

La semaine dernière, l'EFF, accompagnée d'une coalition formée d'entreprises technologiques et de groupes de défense des libertés, a lancé SaveCrypto.org, une pétition en ligne où les parties concernées peuvent faire savoir au président Obama que l'administration devrait se prononcer en faveur d'un chiffrement fort. Alors qu'Obama a clarifié sa position initiale, il a aussi promis de répondre à toute pétition qui recueillerait plus de 100 000 signatures. Cela signifie qu'il est encore temps pour de l'influencer.

Dans une ère de piratage omniprésent et de violation des données sensibles, il est temps pour le président Obama d'écouter les utilisateurs d'Internet et les entreprises qui se battent pour la sécurité des utilisateurs et leur vie privée.

Vous pouvez ajouter votre voix à la pétition ci-dessous.
https://savecrypto.org/


Vous pouvez nous faire confiance
Nous attachons la plus haute importance
à votre vie privée
de liberté
ma vie privée de quoi ?
ah ok