

# Pouhiou vient écrire chez vous : 1 mois, 1 roman, 1 sac à dos !

Démarche originale (et sociale) de Pouhiou, membre émérite et hyperactif de Framasoft.

Il se propose en effet de venir écrire le tome 3 du *Cycle des NoéNautés* chez vous, durant tout le mois de novembre. Transformant du même coup votre maison en résidence d'artiste improvisée ☐

Vous en êtes ?



## J'irai écrire chez vous : 1 mois, 1 roman, 1 sac à dos.

J'ai déjà parlé sur mon blog du [NaNoWriMo](#). Chaque année en novembre, une foultitude d'internautes se lancent en chœur dans un défi dingue et personnel : écrire un roman. Chacun-e a pour but son histoire de 50 000 mots minimum entre le 1er et le 30 du mois. C'est d'ailleurs ce qui m'a inspiré [cette règle](#) d'un épisode par jour du lundi au vendredi pendant 4 mois...

## **Mon défi : écrire le livre III en novembre**

Je savais déjà que le livre III des NoéNautes allait bousculer les codes. Je ne vais pas l'écrire en direct. Il ne va pas paraître épisode par épisode, mais chapitre par chapitre. J'ai même envie qu'il paraisse au fur et à mesure que tu t'y intéresses (d'ailleurs si tu es dev php, on a besoin de ton aide pour créer un petit outil qui pourrait bien révolutionner les internetz. Nom de code : [Framajauge](#) !) J'ai su tout ça durant ces six derniers mois, mais je ne l'ai pas écrit : j'ai bossé. Un mi-temps « malheureusement » trop intéressant : il a capté mon temps de cerveau disponible.

## **Novembre 2013 : je me déconnecte de ma vie et je l'écris**

C'est Ploum qui a fini par m'y inciter. Cet auteur dont je découvre des facettes redoutables ([sa série Printeurs](#) alterne entre le cyber-punk délicieusement paranoïaque et l'anticipation déshumanisée trash et gore... un régal !) échange avec moi, en privé, sur l'intérêt de s'imposer des contraintes d'écriture. Puis sur son envie de faire un NaNoWriMo cette année. Vous pouvez d'ailleurs le soutenir tout au long de novembre dans sa démarche [en la découvrant ici](#) ! Bref : le mec m'a donné grave envie, alors en vilain copieur des internetz, je me suis dit : et pourquoi je m'y mettrais pas, moi aussi ?

## **Le libre est un échange, le livre est un échange.**

J'ai passé un mois d'octobre sur les routes des Villes en Biens Communs, à faire des conférences [sur la culture libre](#), à animer des [ateliers d'écriture collaborative](#). J'ai distribué des #Smartarded [rendus gratuits par mes lecteurs](#) dans nombre de villes et d'évènements. A Rennes j'ai [rencontré des libristes](#), puis [j'ai débattu](#) sur les cultures et les contes LGBT. A Toulouse j'ai expliqué ma démarche de Commoner, et nos besoins pour [mener à bien la Framajauge](#). A Bolbec j'ai débattu avec un auteur qui souhaite qu'[on ne touche pas à ses livres et qu'on les paie coûte que coûte](#). A Paris, j'ai assisté à [une](#)

[copyparty en bibliothèque](#) avant d'aller [signer des romans](#) dans la librairie de Bookynette...

## **J'ai eu envie de poursuivre ces rencontres, d'aller plus loin dans l'échange.**

Et pendant tout ce temps, cette idée de NaNoWriMo qui me trottait dans la tête... Jusqu'à ce que la connexion se fasse : et si j'allais écrire ce roman chez les gens ? Je le sais : me déconnecter de ma bulle, de ma colloc' avec mes potes, ma famille, mes habitudes, etc. – c'est un très bon moyen d'être efficace ! C'est comme ça que j'ai écrit tout Tocante, que je me suis lancé dans #Smartarded ou que j'ai achevé #MonOrchide... Sans compter qu'en vivant un mois chez les gens, ça amortirait les dépenses sur mes assedics de mi-temps de smicard... Ben oui : faire le choix de ne plus bosser pour écrire, c'est aussi faire le choix de l'indigence ^^ !

## **Résidence d'artiste improvisée : héberge un Pouhiou !**

Voilà comment m'est venue cette idée du « J'irai écrire chez vous ». Je vais donc partir un mois en sac à dos, un mois divisé en 10 lieux, à écrire un peu partout en France... En commençant par Paris, puisque je participerai (avec plein de membres de Framasoft et de SavoirsCom1) à la journée d'étude sur [le Domaine Public à l'Assemblée Nationale](#). De plus, il y aura un passage obligé par Toulouse, vu que le 22-23 novembre je fais une conférence et un atelier (et j'aiderai à tenir le stand Framasoft) au Capitole du Libre <http://2013.capitolelibre.org/programme.html>. Et on terminera à Lyon (avec là aussi un atelier d'écriture collaborative). Alors si tu veux héberger un Pouhiou, c'est simple... il te faut :

- Un canapé pour 3 nuits chez toi (j'ai déjà le sac de couchage)
- Une place à ta table (même que je mange plus d'animaux

morts, donc je suis super économe)

- Un peu de ton wifi (j'écris toujours sur une tablette, donc il me faut de bonnes ondes)
- Ne pas avoir peur de me laisser seul, parfois (j'aurai pas le temps de jouer avec des allumettes, je vais écrire ^^)
- Aller [t'inscrire sur le framadate](#) puis me contacter sur les réseaux (Pouhiou) ou par email chez [framsoft point org](#).

Et si tu veux participer autrement qu'en m'hébergeant, tu peux...

- Aller lire, télécharger et diffuser [les 2 premiers romans](#).
- Les promouvoir sur ton blog, ton forum, tes réseaux...
- Acheter les versions papier (même que je touche des sous dessus)  
<http://eventelibre.org/catalog/par-type-de-produit/livres>
- Flattr-er mes articles sur [noenaute.fr](#) (convertissez les gens à Flattr, ça marche !)
- Venir aider sur Framabook (surtout si connais l'édition, le graphisme, la diffusion ou les ebooks)
- Venir aider sur [la framajauge](#) (surtout si tu développes en php)

## **Suis mes aventures pendant la prochaine Campagne Framasoft**

Framasoft héberge mes sites web (et m'aide grandement techniquement) en plus d'éditer mes romans (je donne du grain à moudre à nombre de correcteurices et codeuses...) Framasoft défend nombre de projets du libre, dans le logiciel comme dans la culture, avec pour but de le rendre accessible à la « famille Michu ». Je suis très heureux d'aller battre la campagne pendant la campagne de financement de cette association (dont le top départ aura lieu en novembre

également), que j'aime et dont je suis un membre actif. Tu as remarqué que je n'ai pas fait d'appel aux dons pour cette aventure... Y'a pourtant un bouton de don paypal sur mon blog, mais si tu veux donner des sous, ce serait cool que tu les donnes à Framasoft.

## [Soutenir Framasoft](#)

Du coup, tu pourras suivre mes aventures de novembre sur le Framablog. J'y rendrai compte des rencontres et de mes avancées, sans aucun spoiler. Je tweeterai régulièrement le nombre de mots que j'ai atteint, et @Framasoft reprendra l'info... Parce que sincèrement, toute cette aventure, toutes ces rencontres, tous ces échanges et toutes ces histoires n'auraient pas été possibles si je n'avais pas rencontré une bande de grand malades qui se défoncent pour que de tels projets aient une chance d'être hébergés, édités, vus et reconnus. Et si tu veux me donner aussi à moi, vraiment : inscris-toi sur [flattr](#) et viens offrir une reconnaissance financière aux gens qui œuvrent sur le Net.

Allez hop, j'ai un sac à dos et un roman à préparer !

Au Plaisir,

Pouhiou.



---

# Quel niveau de surveillance la démocratie peut-elle endurer ? par Richard Stallman

« Le niveau de surveillance actuel dans nos sociétés est incompatible avec les droits de l'homme... »

C'est ce qu'affirme et expose [Richard Stallman](#) dans ce long article argumenté en proposant un certain nombre de mesures pour desserrer l'étau.

Sur la [photo](#) ci-dessous, on voit Stallman lors d'une conférence en Tunisie muni d'un étrange badge. Il l'a recouvert lui-même de papier aluminium pour ne pas être pisté lors de l'évènement !





# Quel niveau de surveillance la démocratie peut-elle supporter ?

par [Richard Stallman](#)

[URL d'origine du document \(sur GNU.org\)](#)

*Une première version de cet article a été publiée sur [Wired](#) en octobre 2013.*

*Licence : [Creative Commons BY-ND 3.0 US](#)*

*Traduction : aKa, zimadprof, Lamessen, Sylvain, Scailyna, Paul, Asta, Monsieur Tino, Marc, Thérèse, Amine Brikci-N, FF255, Achille, Slystone, Sky, Penguin et plusieurs anonymes*

*Révision : [trad-gnu@april.org](mailto:trad-gnu@april.org) – Version de la traduction : 14 août 2014*

Grâce aux révélations d'Edward Snowden, nous comprenons aujourd'hui que le niveau de surveillance dans nos sociétés est incompatible avec les droits de l'homme. Le harcèlement répété et les poursuites judiciaires que subissent les opposants, les sources et les journalistes (aux États-Unis et ailleurs) en sont la preuve. Nous devons réduire le niveau de surveillance, mais jusqu'où ? Où se situe exactement le *seuil tolérable de surveillance* que l'on doit faire en sorte de ne pas dépasser ? C'est le niveau au delà duquel la surveillance commence à interférer avec le fonctionnement de la démocratie : lorsque des lanceurs d'alerte comme Snowden sont susceptibles d'être attrapés.

Face à la culture du secret des gouvernements, nous, le peuple,<sup>1</sup> devons compter sur les lanceurs d'alerte pour [apprendre ce que l'État est en train de faire](#). De nos jours, cependant, la surveillance intimide les lanceurs d'alerte potentiels, et cela signifie qu'elle est trop intense. Pour retrouver notre contrôle démocratique sur l'État, nous devons réduire la surveillance jusqu'à un point où les lanceurs d'alerte se sentent en sécurité.

L'utilisation de logiciels libres, [comme je la préconise depuis trente ans](#), est la première étape dans la prise de contrôle de nos vies numériques – qui inclut la prévention de la surveillance. Nous ne pouvons faire confiance aux logiciels non libres ; la NSA [utilise](#) et même [crée](#) des failles de sécurité dans des logiciels non libres afin d'envahir nos ordinateurs et nos routeurs. Le logiciel libre nous donne le contrôle de nos propres ordinateurs, mais [cela ne protège pas notre vie privée dès l'instant où nous mettons les pieds sur Internet](#).

[Une législation bipartisane ayant pour but de « limiter les pouvoirs de surveillance sur le territoire national »](#) est en cours d'élaboration aux États-Unis mais elle le fait en limitant l'utilisation par le gouvernement de nos dossiers virtuels. Cela ne suffira pas à protéger les lanceurs d'alerte si « capturer le lanceur d'alerte » est un motif valable pour accéder à des données permettant de l'identifier. Nous devons aller plus loin encore.

## **Le niveau de surveillance à ne pas dépasser dans une démocratie**

Si les lanceurs d'alerte n'osent pas révéler les crimes, délits et mensonges, nous perdons le dernier lambeau de contrôle réel qui nous reste sur nos gouvernements et institutions. C'est pourquoi une surveillance qui permet à l'État de savoir qui a parlé à un journaliste va trop loin – au delà de ce que peut supporter la démocratie.

En 2011, un représentant anonyme du gouvernement américain a fait une déclaration inquiétante à des journalistes, à savoir que [les États-Unis n'assigneraient pas de reporter à comparaître parce que « nous savons avec qui vous parlez »](#). Parfois, pour avoir ces renseignements, [ils obtiennent les relevés téléphoniques de journalistes par injonction judiciaire](#), mais Snowden nous a montré qu'en réalité ils



adressent des injonctions en permanence [à Verizon](#) et [aux autres opérateurs](#), pour tous les relevés téléphoniques de chaque résident.

Il est nécessaire que les activités d'opposition ou dissidentes protègent leurs secrets des États qui cherchent à leur faire des coups tordus. L'ACLU<sup>2</sup> a démontré que le gouvernement des États-Unis [infiltrait systématiquement les groupes dissidents pacifiques](#) sous prétexte qu'il pouvait y avoir des terroristes parmi eux. La surveillance devient trop importante quand l'État peut trouver qui a parlé à une personne connue comme journaliste ou comme opposant.

## **L'information, une fois collectée, sera utilisée à de mauvaises fins**

Quand les gens reconnaissent que la surveillance généralisée atteint un niveau trop élevé, la première réponse est de proposer d'encadrer l'accès aux données accumulées. Cela semble sage, mais cela ne va pas corriger le problème, ne serait-ce que modestement, même en supposant que le gouvernement respecte la loi (la NSA a trompé la cour fédérale de la FISA,<sup>3</sup> et cette dernière a affirmé [être incapable, dans les faits, de lui demander des comptes](#)). Soupçonner un délit est un motif suffisant pour avoir accès aux données, donc une fois qu'un lanceur d'alerte est accusé d'« espionnage », trouver un « espion » fournira une excuse pour avoir accès à l'ensemble des informations.

Le personnel chargé de la surveillance d'État a l'habitude de détourner les données à des fins personnelles. Des agents de la NSA ont [utilisé les systèmes de surveillance américains pour suivre à la trace leurs petit\(e\)s ami\(e\)s](#) – passés, présents, ou espérés, selon une pratique nommée « LOVEINT ». La NSA affirme avoir détecté et puni cette pratique à plusieurs reprises ; nous ne savons pas combien d'autres cas n'ont pas été détectés. Mais ces événements ne devraient pas

nous surprendre, parce que les policiers [utilisent depuis longtemps leurs accès aux fichiers des permis de conduire pour pister des personnes séduisantes](#), une pratique connue sous les termes de « choper une plaque pour un rencard ».

Les données provenant de la surveillance seront toujours détournées de leur but, même si c'est interdit. Une fois que les données sont accumulées et que l'État a la possibilité d'y accéder, il peut en abuser de manière effroyable, comme le montrent des exemples pris [en Europe](#) et [aux États-Unis](#).

La surveillance totale, plus des lois assez floues, ouvrent la porte à une campagne de pêche à grande échelle, quelle que soit la cible choisie. Pour mettre le journalisme et la démocratie en sécurité, nous devons limiter l'accumulation des données qui sont facilement accessibles à l'État.

## **Une protection solide de la vie privée doit être technique**

L'Electronic Frontier Foundation et d'autres structures proposent un ensemble de principes juridiques destinés à [prévenir les abus de la surveillance de masse](#). Ces principes prévoient, et c'est un point crucial, une protection juridique explicite pour les lanceurs d'alerte. Par conséquent, ils seraient adéquats pour protéger les libertés démocratiques s'ils étaient adoptés dans leur intégralité et qu'on les faisait respecter sans la moindre exception, à tout jamais.

Toutefois, ces protections juridiques sont précaires : comme nous l'ont montré les récents événements, ils peuvent être abrogés (comme dans la loi dite *FISA Amendments Act*), suspendus ou [ignorés](#).

Pendant ce temps, les démagogues fourniront les excuses habituelles pour justifier une surveillance totale ; toute attaque terroriste, y compris une attaque faisant un nombre réduit de victimes, leur donnera cette opportunité.

Si la limitation de l'accès aux données est écartée, ce sera comme si elle n'avait jamais existé. Des dossiers remontant à des années seront du jour au lendemain exposés aux abus de l'État et de ses agents et, s'ils ont été rassemblés par des entreprises, seront également exposés aux magouilles privées de ces dernières. Si par contre nous arrêtons de fichier tout le monde, ces dossiers n'existeraient pas et il n'y aurait pas moyen de les analyser de manière rétroactive. Tout nouveau régime non libéral aurait à mettre en place de nouvelles méthodes de surveillance, et recueillerait des données à partir de ce moment-là seulement. Quant à suspendre cette loi ou ne pas l'appliquer momentanément, cela n'aurait presque aucun sens.

## **En premier lieu, ne soyez pas imprudent**

Pour conserver une vie privée, il ne faut pas la jeter aux orties : le premier concerné par la protection de votre vie privée, c'est vous. Évitez de vous identifier sur les sites web, contactez-les avec Tor, et utilisez des navigateurs qui bloquent les stratagèmes dont ils se servent pour suivre les visiteurs à la trace. Utilisez GPG (le gardien de la vie privée) pour chiffrer le contenu de vos courriels. Payez en liquide.

Gardez vos données personnelles ; ne les stockez pas sur le serveur « si pratique » d'une entreprise. Il n'y a pas de risque, cependant, à confier la sauvegarde de vos données à un service commercial, pourvu qu'avant de les envoyer au serveur vous les chiffriez avec un logiciel libre sur votre propre ordinateur (y compris les noms de fichiers).

Par souci de votre vie privée, vous devez éviter les logiciels non libres car ils donnent à d'autres la maîtrise de votre informatique, et que par conséquent [ils vous espionnent probablement](#). N'utilisez pas de [service se substituant au logiciel](#) : outre que cela donne à d'autres la maîtrise de votre informatique, cela vous oblige à fournir toutes les

données pertinentes au serveur.

Protégez aussi la vie privée de vos amis et connaissances. [Ne divulguez pas leurs informations personnelles](#), sauf la manière de les contacter, et ne donnez jamais à aucun site l'ensemble de votre répertoire téléphonique ou des adresses de courriel de vos correspondants. Ne dites rien sur vos amis à une société comme Facebook qu'ils ne souhaiteraient pas voir publier dans le journal. Mieux, n'utilisez pas du tout Facebook. Rejetez les systèmes de communication qui obligent les utilisateurs à donner leur vrai nom, même si vous êtes disposé à donner le vôtre, car cela pousserait d'autres personnes à abandonner leurs droits à une vie privée.

La protection individuelle est essentielle, mais les mesures de protection individuelle les plus rigoureuses sont encore insuffisantes pour protéger votre vie privée sur des systèmes, ou contre des systèmes, qui ne vous appartiennent pas. Lors de nos communications avec d'autres ou de nos déplacements à travers la ville, notre vie privée dépend des pratiques de la société. Nous pouvons éviter certains des systèmes qui surveillent nos communications et nos mouvements, mais pas tous. Il est évident que la meilleure solution est d'obliger ces systèmes à cesser de surveiller les gens qui sont pas légitimement suspects.

## **Nous devons intégrer à chaque système le respect de la vie privée**

Si nous ne voulons pas d'une société de surveillance totale, nous devons envisager la surveillance comme une sorte de pollution de la société et limiter l'impact de chaque nouveau système numérique sur la surveillance, de la même manière que nous limitons l'impact des objets manufacturés sur l'environnement.

Par exemple, les compteurs électriques « intelligents » sont paramétrés pour envoyer régulièrement aux distributeurs

d'énergie des données concernant la consommation de chaque client, ainsi qu'une comparaison avec la consommation de l'ensemble des usagers. Cette implémentation repose sur une surveillance généralisée mais ce n'est nullement nécessaire. Un fournisseur d'énergie pourrait aisément calculer la consommation moyenne d'un quartier résidentiel en divisant la consommation totale par le nombre d'abonnés, et l'envoyer sur les compteurs. Chaque client pourrait ainsi comparer sa consommation avec la consommation moyenne de ses voisins au cours de la période de son choix. Mêmes avantages, sans la surveillance !

Il nous faut intégrer le respect de la vie privée à tous nos systèmes numériques, dès leur conception.

## **Remède à la collecte de données : les garder dispersées**

Pour rendre la surveillance possible sans porter atteinte à la vie privée, l'un des moyens est de conserver les données de manière dispersée et d'en rendre la consultation malaisée. Les caméras de sécurité d'antan n'étaient pas une menace pour la vie privée. Les enregistrements étaient conservés sur place, et cela pendant quelques semaines tout au plus. Leur consultation ne se faisait pas à grande échelle du fait de la difficulté d'y avoir accès. On les consultait uniquement sur les lieux où un délit avait été signalé. Il aurait été impossible de rassembler physiquement des millions de bandes par jour, puis de les visionner ou de les copier.

Aujourd'hui, les caméras de sécurité se sont transformées en caméras de surveillance ; elles sont reliées à Internet et leurs enregistrements peuvent être regroupés dans un centre de données [*data center*] et conservés *ad vitam aeternam*. C'est déjà dangereux, mais le pire est à venir. Avec les progrès de la reconnaissance faciale, le jour n'est peut-être pas loin où les journalistes « suspects » pourront être pistés sans

interruption dans la rue afin de surveiller qui sont leurs interlocuteurs.

Les caméras et appareils photo connectés à Internet sont souvent eux-mêmes mal protégés, de sorte que [n'importe qui pourrait regarder ce qu'ils voient par leur objectif](#). Pour rétablir le respect de la vie privée, nous devons interdire l'emploi d'appareils photo connectés dans les lieux ouverts au public, sauf lorsque ce sont les gens qui les transportent. Tout le monde doit avoir le droit de mettre en ligne des photos et des enregistrements vidéo une fois de temps en temps, mais on doit limiter l'accumulation systématique de ces données.

## **Remède à la surveillance du commerce sur Internet**

La collecte de données provient essentiellement des activités numériques personnelles des gens. D'ordinaire, ces sont d'abord les entreprises qui recueillent ces données. Mais lorsqu'il est question de menaces pour la vie privée et la démocratie, que la surveillance soit exercée directement par l'État ou déléguée à une entreprise est indifférent, car les données rassemblées par les entreprises sont systématiquement mises à la disposition de l'État.

Depuis PRISM, [la NSA a un accès direct aux bases de données de nombreuses grandes sociétés d'Internet](#). AT&T conserve tous les relevés téléphoniques depuis 1987 et [les met à la disposition de la DEA](#) sur demande, pour ses recherches. Aux États-Unis, l'État fédéral ne possède pas ces données au sens strict, mais en pratique c'est tout comme.

Mettre le journalisme et la démocratie en sécurité exige, par conséquent, une réduction de la collecte des données privées, par toute organisation quelle qu'elle soit et pas uniquement par l'État. Nous devons repenser entièrement les systèmes numériques, de telle manière qu'ils n'accumulent pas de

données sur leurs utilisateurs. S'ils ont besoin de détenir des données numériques sur nos transactions, ils ne doivent être autorisés à les garder que pour une période dépassant de peu le strict minimum nécessaire au traitement de ces transactions.

Une des raisons du niveau actuel de surveillance sur Internet est que le financement des sites repose sur la publicité ciblée, par le biais du pistage des actions et des choix de l'utilisateur. C'est ainsi que d'une pratique simplement gênante, la publicité que nous pouvons apprendre à éviter, nous basculons, en connaissance de cause ou non, dans un système de surveillance qui nous fait du tort. Les achats sur Internet se doublent toujours d'un pistage des utilisateurs. Et nous savons tous que les « politiques relatives à la vie privée » sont davantage un prétexte pour violer celle-ci qu'un engagement à la respecter.

Nous pourrions remédier à ces deux problèmes en adoptant un système de paiement anonyme – anonyme pour l'émetteur du paiement, s'entend (permettre au bénéficiaire d'échapper à l'impôt n'est pas notre objectif). [Bitcoin n'est pas anonyme](#), bien que des efforts soient faits pour développer des moyens de payer anonymement avec des bitcoins. Cependant, la technologie de la [monnaie électronique remonte aux années 80](#) ; tout ce dont nous avons besoin, ce sont d'accords adaptés pour la marche des affaires et que l'État n'y fasse pas obstruction.

Le recueil de données personnelles par les sites comporte un autre danger, celui que des « casseurs de sécurité » s'introduisent, prennent les données et les utilisent à de mauvaises fins, y compris celles qui concernent les cartes de crédit. Un système de paiement anonyme éliminerait ce danger : une faille de sécurité du site ne peut pas vous nuire si le site ne sait rien de vous.



## Remède à la surveillance des déplacements

Nous devons convertir la collecte numérique de péage en paiement anonyme (par l'utilisation de monnaie électronique, par exemple). Les systèmes de reconnaissance de plaques minéralogiques reconnaissent toutes les plaques, et [les données peuvent être gardées indéfiniment](#) ; la loi doit exiger que seules les plaques qui sont sur une liste de véhicules recherchés par la justice soient identifiées et enregistrées. Une solution alternative moins sûre serait d'enregistrer tous les véhicules localement mais seulement pendant quelques jours, et de ne pas rendre les données disponibles sur Internet ; l'accès aux données doit être limité à la recherche d'une série de plaques minéralogiques faisant l'objet d'une décision de justice.

The U.S. "no-fly" list must be abolished because it is [punishment without trial](#).

Il est acceptable d'établir une liste de personnes pour qui la fouille corporelle et celle des bagages seront particulièrement minutieuses, et l'on peut traiter les passagers anonymes des vols intérieurs comme s'ils étaient sur cette liste. Il est acceptable également d'interdire aux personnes n'ayant pas la citoyenneté américaine d'embarquer sur des vols à destination des États-Unis si elles n'ont pas la permission d'y rentrer. Cela devrait suffire à toutes les fins légitimes.

Beaucoup de systèmes de transport en commun utilisent un genre de carte intelligente ou de puce RFID pour les paiements. Ces systèmes amassent des données personnelles : si une seule fois vous faites l'erreur de payer autrement qu'en liquide, ils associent définitivement la carte avec votre nom. De plus, ils enregistrent tous les voyages associés avec chaque carte. L'un dans l'autre, cela équivaut à un système de surveillance à grande échelle. Il faut diminuer cette collecte de données.

Les services de navigation font de la surveillance : l'ordinateur de l'utilisateur renseigne le service cartographique sur la localisation de l'utilisateur et l'endroit où il veut aller ; ensuite le serveur détermine l'itinéraire et le renvoie à l'ordinateur, qui l'affiche. Il est probable qu'actuellement le serveur enregistre les données de localisation puisque rien n'est prévu pour l'en empêcher. Cette surveillance n'est pas nécessaire en soi, et une refonte complète du système pourrait l'éviter : des logiciels libres installés côté utilisateur pourraient télécharger les données cartographiques des régions concernées (si elles ne l'ont pas déjà été), calculer l'itinéraire et l'afficher, sans jamais dire à qui que ce soit l'endroit où l'utilisateur veut aller.

Les systèmes de location de vélos et autres peuvent être conçus pour que l'identité du client ne soit connue que de la station de location. Au moment de la location, celle-ci informera toutes les stations du réseau qu'un vélo donné est « sorti » ; de cette façon, quand l'utilisateur le rendra, généralement à une station différente, cette station-là saura où et quand il a été loué. Elle informera à son tour toutes les stations du fait que ce vélo a été rendu, et va calculer en même temps la facture de l'utilisateur et l'envoyer au siège social après une attente arbitraire de plusieurs minutes, en faisant un détour par plusieurs stations. Ainsi le siège social ne pourra pas savoir précisément de quelle station la facture provient. Ceci fait, la station de retour effacera toutes les données de la transaction. Si le vélo restait « sorti » trop longtemps, la station d'origine pourrait en informer le siège social et, dans ce cas, lui envoyer immédiatement l'identité du client.

## **Remède aux dossiers sur les communications**

Les fournisseurs de services Internet et les compagnies de téléphone enregistrent une masse de données sur les contacts

de leurs utilisateurs (navigation, appels téléphoniques, etc.) Dans le cas du téléphone mobile, [ils enregistrent en outre la position géographique de l'utilisateur](#). Ces données sont conservées sur de longues périodes : plus de trente ans dans le cas d'AT&T. Bientôt, [ils enregistreront même les mouvements corporels de l'utilisateur](#). Et il s'avère que [la NSA collecte les coordonnées géographiques des téléphones mobiles](#), en masse.

Les communications non surveillées sont impossibles là où le système crée de tels dossiers. Leur création doit donc être illégale, ainsi que leur archivage. Il ne faut pas que les fournisseurs de services Internet et les compagnies de téléphone soient autorisés à garder cette information très longtemps, sauf décision judiciaire leur enjoignant de surveiller une personne ou un groupe en particulier.

Cette solution n'est pas entièrement satisfaisante, car cela n'empêchera pas concrètement le gouvernement de collecter toute l'information à la source – ce que fait [le gouvernement américain avec certaines compagnies de téléphone](#), voire avec toutes. Il nous faudrait faire confiance à l'interdiction par la loi. Cependant, ce serait déjà mieux que la situation actuelle où la loi applicable (le PATRIOT Act) n'interdit pas clairement cette pratique. De plus, si un jour le gouvernement recommençait effectivement à faire cette sorte de surveillance, il n'obtiendrait pas les données sur les appels téléphoniques passés avant cette date.

Pour garder confidentielle l'identité des personnes avec qui vous échangez par courriel, une solution simple mais partielle est d'utiliser un service situé dans un pays qui ne risquera jamais de coopérer avec votre gouvernement, et qui chiffre ses communications avec les autres services de courriels. Toutefois, Ladar Levison (propriétaire du service de courriel Lavabit que la surveillance américaine a cherché à corrompre complètement) a une idée plus sophistiquée : établir un système de chiffrement par lequel votre service de courriel

saurait seulement que vous avez envoyé un message à un utilisateur de mon service de courriel, et mon service de courriel saurait seulement que j'ai reçu un message d'un utilisateur de votre service de courriel, mais il serait difficile de déterminer que c'était moi le destinataire.

## **Mais un minimum de surveillance est nécessaire.**

Pour que l'État puisse identifier les auteurs de crimes ou délits, il doit avoir la capacité d'enquêter sur un délit déterminé, commis ou en préparation, sur ordonnance du tribunal. À l'ère d'Internet, il est naturel d'étendre la possibilité d'écoute des conversations téléphoniques aux connexions Internet. On peut, certes, facilement abuser de cette possibilité pour des raisons politiques, mais elle n'en est pas moins nécessaire. Fort heureusement, elle ne permettrait pas d'identifier les lanceurs d'alerte après les faits, si (comme je le recommande) nous empêchons les systèmes numériques d'accumuler d'énormes dossiers avant les faits.

Les personnes ayant des pouvoirs particuliers accordés par l'État, comme les policiers, abandonnent leur droit à la vie privée et doivent être surveillés (en fait, les policiers américains utilisent dans leur propre jargon le terme [testilying](#)<sup>4</sup> au lieu de [perjury](#)<sup>5</sup> puisqu'ils le font si souvent, en particulier dans le cadre de la comparution de manifestants et de [photographes](#)). Une ville de Californie qui a imposé à la police le port permanent d'une caméra a vu [l'usage de la force diminuer de près de 60 %](#). L'ACLU y est favorable.

[Les entreprises ne sont pas des personnes et ne peuvent se prévaloir des droits de l'homme](#). Il est légitime d'exiger d'elles qu'elles rendent public le détail des opérations susceptibles de présenter un risque chimique, biologique, nucléaire, financier, informatique (par exemple les [DRM](#)) ou politique (par exemple le lobbyisme) pour la société, à un

niveau suffisant pour assurer le bien-être public. Le danger de ces opérations (pensez à BP et à la marée noire dans le Golfe du Mexique, à la fusion du cœur des réacteurs nucléaires de Fukushima ou à la crise financière de 2008) dépasse de loin celui du terrorisme.

Cependant, le journalisme doit être protégé contre la surveillance, même s'il est réalisé dans un cadre commercial.

---

La technologie numérique a entraîné un accroissement énorme du niveau de surveillance de nos déplacements, de nos actions et de nos communications. Ce niveau est bien supérieur à ce que nous avons connu dans les années 90, [bien supérieur à ce qu'ont connu les gens habitant derrière le rideau de fer](#) dans les années 80, et il resterait encore bien supérieur si l'utilisation de ces masses de données par l'État était mieux encadrée par la loi.

A moins de croire que nos pays libres ont jusqu'à présent souffert d'un grave déficit de surveillance, et qu'il leur faut être sous surveillance plus que ne le furent jadis l'Union soviétique et l'Allemagne de l'Est, ils nous faut inverser cette progression. Cela requiert de mettre fin à l'accumulation en masse de données sur la population.

## Notes :

---

### Notes de traduction

1. Allusion probable à la Constitution de 1787, symbole de la démocratie américaine, qui débute par ces mots : *We, the people of the United States* (Nous, le peuple des États-Unis). [?](#)
2. Union américaine pour les libertés civiles. [?](#)
3. Loi sur la surveillance du renseignement étranger ; elle

a mis en place une juridiction spéciale, la FISC, chargée de juger les présumés agents de renseignement étrangers sur le sol américain. ?

4. *Testilying* : contraction de *testify*, faire une déposition devant un tribunal, et *lying*, acte de mentir.

?

5. *Perjury* : faux témoignage. ?

---

## Le chiffrement, maintenant (la récap')

Voici la dernière livraison de notre traduction par épisodes de Encryption Works. Vous trouverez ci-dessous les quelques lignes qui concluent l'ouvrage original ainsi que des liens vers le miniguide de 30 pages en français qui réunit les épisodes en un seul document.

### Une chance de s'en sortir

Protéger sa vie privée à l'ère de la surveillance omniprésente de la NSA est incroyablement complexe. L'effort d'acquisition des concepts à maîtriser, représente une sacrée courbe d'apprentissage, plus ou moins facilitée par l'utilisation des logiciels déjà disponibles. Mais même avec un accès direct à toutes les données transitant à la vitesse de la lumière par les fibres optiques, formant l'épine dorsale d'Internet, même avec la coopération des principales entreprises des États-Unis (qu'il est extrêmement difficile pour les gens de boycotter), le plus grand, le plus puissant et le meilleur système de surveillance que l'humanité ait jamais connu ne pourra pas battre les mathématiques. Le défi pour le nouveau mouvement cypherpunk est de rendre la sécurité et le chiffrement

vérifiés de bout à bout accessibles à tout le monde et activés par défaut.

## L'ensemble du guide en une seule fois

Cliquez sur le lien avec le bouton droit, puis « Enregistrer la cible du lien sous... »

- [Le chiffrement, maintenant – ODT \(367 Ko\)](#)
- [Le chiffrement, maintenant – PDF \(872 Ko\)](#)

## Pour aller plus loin, appel à contributions

Ce guide n'a pas la prétention de proposer une couverture exhaustive d'une question aussi épineuse. C'est pourquoi, si vous souhaitez contribuer à proposer un guide plus complet, nous vous invitons à apporter votre pierre à ce projet : [Votre sécurité sur Internet, notions de base](#) (un gros ouvrage de plus de 400 pages). Le travail est actuellement en cours sur la plateforme Flossmanuals francophone sur laquelle il faut donc s'inscrire pour pouvoir modifier/traduire le texte. Quelques points importants :

- Le premier jet de traduction a déjà été réalisé (notamment pour plusieurs chapitres par des étudiants de l'INRIA de Rouen encadrés par leur enseignant).
- Nous avons besoin :
  - de contributeurs capables de proposer des images d'illustration (captures d'écran) avec des textes inclus *en français*
  - de relecteurs spécialisés et compétents sur les problèmes techniques de sécurité, car outre la bonne conformité des termes employés, ils devront réviser



voire refondre certains chapitres qui ne seraient plus tout à fait à jour, particulièrement en fonction des dernières révélations sur les capacités de nuisance de la NSA.

- Ceux qui estimeront qu'il manque des informations voire un chapitre etc. pourront tout à fait ajouter ce qu'ils estiment nécessaire sur la plateforme.

– à bientôt !

---

## Le CERN publie des photos sous licence Creative Commons By-Sa

Bonne nouvelle, le [CERN](#) nous annonce la mise en ligne d'un [fond photographique](#) sous « licence Creative Commons ».

Et pas n'importe laquelle des licences Creative Commons, la libre copyleft [CC By-SA](#) (pour plus de précisions sur la question des licences, vous pouvez lire [La « politique » Framabook et les licences libres](#)). On notera au passage qu'ils abandonnent leur propre licence *maison*.

C'est Wikipédia et tous ceux qui souhaitent pouvoir librement réutiliser des images du CERN qui vont être contents, c'est-à-dire nous tous ☐



## Le CERN publie des photos sous licence Creative Commons

[CERN releases photos under a Creative Commons licence](#)

*Tim Smith – 17 octobre 2013 – CERN (Traduction : Penguin, Rémy, Monsieur Tino, Floréal, Ag3m)*

Les licences définissent le cadre et les conditions d'utilisation d'une œuvre. Bien souvent, dans la vie courante, on est confronté à des licences limitant les usages que l'on peut faire de ces œuvres, empêchant la copie ou le partage de celles-ci. Mais tout une famille de licences libres vise et encourage l'utilisation et le partage, sous réserve de reconnaître l'origine de l'œuvre et d'avoir un comportement identique en retour (c'est à dire partager l'oeuvre modifiée sous la même licence).

Depuis ses débuts, le CERN utilise le web pour partager ouvertement des éléments multimédia. Pour indiquer clairement que nous voulions permettre aux gens d'utiliser nos photos et vidéos, nous avons créé une licence média libre novatrice. Elle incluait des clauses qui répondaient aux exigences d'une organisation intergouvernementale, et assurait la cohérence

avec notre convention initiale en tant qu'organisation scientifique pacifique.

Avec la croissance du web, les éléments multimédia ont proliféré autour du globe, tout comme les licences. Le web-citoyen moyen, allergique au jargon juridique dont ces licences sont faites, a souvent été désorienté ou dans l'ignorance des détails de chaque condition particulière d'utilisation. Des licences libres standardisées, comme la licence Creative Commons, ont gagné en popularité grâce à l'effet boule-de-neige, à force d'être utilisées systématiquement et généralement comprises. Avec l'expansion de licences standardisées, la licence du CERN s'est retrouvée isolée contre notre volonté, et les médias populaires d'aujourd'hui n'incluent pas nos ressources multimédia, car ils ne considèrent pas que notre licence est compatible.

Ainsi, encouragés et soutenus par nos équipes de sensibilisation pour cette expérience, nous avons rendu disponible sous une licence Creative Commons [une première collection de photos](#). Nous avons choisi la licence CC-BY-SA, pour nous assurer que le crédit des photos serait bien attribué au CERN ("BY") et que les versions modifiées puissent être partagées librement ("Share Alike"). Grâce à ce changement modeste mais significatif, nous espérons que nos photos et vidéos seront désormais disponibles dans plus d'endroits, utilisés par une communauté plus large et ré-utilisés avec plus de confiance par davantage de personnes.

Ce changement a déjà permis que les photos de nos récents Directeurs Généraux soient pour la première fois utilisés systématiquement sur les pages Wikipédia, et que des schémas de la découverte de Higgs provenant de [ATLAS](#) et [CMS](#) soient inclus sur la page du [boson de Higgs](#) ! Nous avons l'intention d'étendre cette première petite collection avec de plus en plus de contenus provenant de nos vastes archives.

Les vents du changement ont commencé à souffler, et nous

espérons faire que bientôt les licences standardisées soient la norme au CERN.

*Crédit photo : [CERN](#) (Licence Creative Commons By-Sa)*

---

# Opérateur du logiciel libre pour les métiers du livre (Villes en Biens Communs)

Dans le cadre de notre participation à Villes en Biens Communs nous ajoutons [un double événement](#) lié aux métiers du livre et organisé par Chloé Girard, membre de Framasoft, le 23 octobre à Paris et le 24 octobre à Lyon.

- [Site officiel](#)
- [Paris 23 octobre](#)
- [Lyon 24 octobre](#)
- Twitter : [@OperateurLL](#)
- [« Inscription »](#) aux réunions (maximum 30 personnes) sur Framadate

Présentation

# La Forge

Outils numériques pour les métiers du livre

Votre département R&D externalisé

Cette rencontre consiste en un après-midi de consultation et de travail avec les professionnels des métiers du livre (éditeurs, libraires, bibliothécaires, documentalistes, distributeurs...), des sociétés de service en logiciel libre et des acteurs engagés dans la mutualisation des expertises informatiques

<http://www.editionforge.org>

Quand ?  
Où ?

À Paris, le 23 octobre 2013, 14:00 hrs., au  
Labo de l'Édition, 2, rue Saint-Médard, 75005 Paris

À Lyon, le 24 octobre 2013, 14:00 hrs., à  
Enssib, 17/21 boulevard du 11 novembre 1918,  
69623 Villeurbanne

Déroulement :

- Présentation de La Forge
- Présentation de projets
- Consultation autour de la gouvernance de la structure
- Discussion ouverte avec le public sur les besoins logiciels identifiés.
- Dépôt logiciel de la Forge
- Projets publiés au Bureau d'étude
- Jouer le jeu et reverser ses développements sous licences libres ?
- Témoignages d'acteurs métier

Soutiens

éditeurs  
des origines  
contemporains

enssib

LABO DE L'ÉDITION  
Labo de l'édition

## Présentation de La Forge par Chloé Girard

Quelques années après avoir commencé à [réfléchir](#) à la transposition du modèle de l'[Adullact](#) vers les métiers du livre, l'[Enssib](#), où je suis maître de conférences associé en édition numérique, a accepté de soutenir ce « projet de recherche ». J'organise donc deux réunions de présentation et de travail, l'une à Paris, l'autre à Lyon, afin de pousser la modélisation de cette Forge.

Il s'agit d'une structure accompagnant les éditeurs, libraires, diffuseurs, dans la mutualisation des fonds, la réalisation et la maintenance de logiciels métier communs et, par extension, experts, pérennes et évolutifs. Elle est gouvernée par et pour les professionnels du livre et constitue une interface « chargée de projet » côté « clients » avec les entreprises de service informatique.

De nombreux éditeurs expriment des besoins communs (de la gestion d'entreprise à la diffusion en passant par la fabrication) ou spécifiques (selon le genre éditorial par exemple, ou le modèle économique). Or aucun ou presque n'a de « département informatique » et beaucoup investissent des fonds, subventionnés ou non, sans prendre la mesure de la complexité de ces outils et de leur maintenance.

Ces deux réunions ont donc pour objectif de présenter le fonctionnement d'une telle, de réfléchir à sa gouvernance (très probablement associative), à son économie (mutualisation), et au logiciel libre (quelques a priori perdurent...).

De nombreux écueils se profilent dans ce contexte de petites entreprises privées, aux finances souvent fragiles. Du côté des développeurs (qui sont parfois les éditeurs eux-mêmes), la libération du code est souvent perçue comme l'abandon d'une potentielle manne financière, souvent en réalité plus coûteuse que rentable. Les acteurs métier espèrent aussi souvent, et nous les comprenons, se « débarrasser » de ces encombrantes questions techniques en choisissant des services en ligne, sans se soucier de la pérennité de ces services, de l'outil ou de l'entreprise qui les sous-tend.

En réponse la forge peut offrir par exemple de développer du côté « clients » les outils sur lesquels baser ce type de services de façon à ce qu'en cas de sortie d'une plateforme tout éditeur ou libraire puisse retrouver le même outil libre et le déployer, ou le voir déployer, ailleurs : expertise,

qualité, indépendance et pérennité !

J'invite donc chacun à venir exprimer ses besoins en logiciels ou extensions métier, à discuter des tenants et aboutissants d'un tel projet et à y verser des logiciels développés en interne et complexes à maintenir seul.

Nous espérons au cours de ces deux réunions pouvoir identifier un besoin phare à lancer comme projet pilote.

Déroulement :

- présentation de l'Opérateur du logiciel libre pour les métiers du livre, une association à vocation d'expert informatique coté « clients » : recension de logiciels, appels à projets, rédaction de cahiers des charges, mutualisation des fonds, suivi de projet, mise en production, assistance ;
- présentation de projets : outils de gestion d'entreprise (droits d'auteur, abonnements revues, facturation, workflow de fabrication), outils de fabrication (édition de ePUB, passage ePUB to Web, mise en page PDF en ligne, annotation, lien POD), diffusion (gestion et publication de métadonnées, mesure d'usages, gestion des URL, protocoles de gestion d'accès, connexion aux réseaux sociaux, flux de catalogage, alertes, outils de librairie...) ;
- consultation autour de la gouvernance de la structure : offrir une souplesse d'adhésion et de retrait des entreprises au gré de l'ouverture et de l'aboutissement d'un projet ;
- les besoins logiciels identifiés : exprimez vos propres besoins ;
- dépôt logiciel de la Forge : être informé et avoir accès en amont aux outils existants ;
- reverser ses propres développements sous licences libres ?
- le financement des projets.



---

# Geektionnerd : TAFTA

Pour rappel, demain, samedi 19 octobre, Gee sera à Paris pour une [libre séance de dédicaces](#).

## TAFTA

Transatlantic Free Trade Area, projet de traité consistant entre autres à nous faire avaler ce que nous avons rejeté avec ACTA (renforcement de la propriété intellectuelle, répression, etc.).

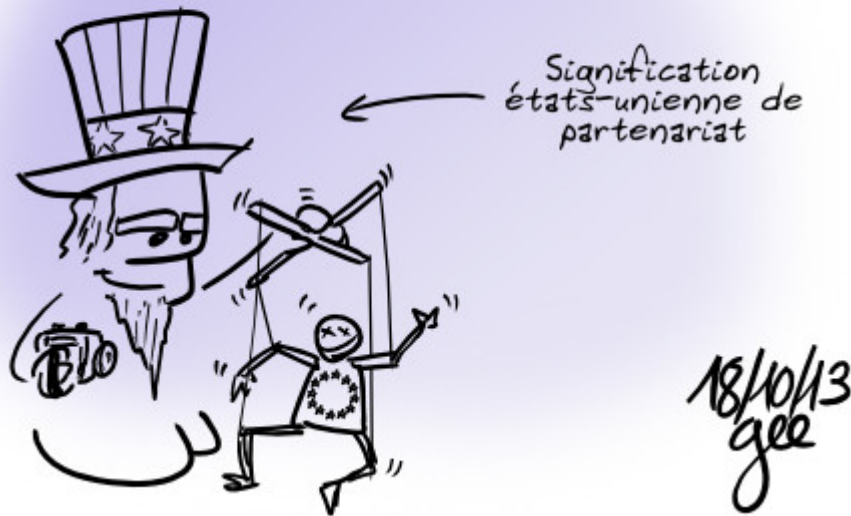
Nous souhaitons juste « une harmonisation progressive des réglementations... »



...et de la reconnaissance mutuelle des règles et normes en vigueur\* ».

\* Extrait d'un communiqué de presse du Parlement Européen

On l'appelle également TTIP, Transatlantic Trade and Investment Partnership : ce serait donc un partenariat entre l'Union Européenne et les États-Unis.



Source :

- [Zone de libre-échange transatlantique – Wikipédia](#)
- [TAFTA](#)
- [Un “marché transatlantique libre d’entraves” à l’horizon 2015](#)

Crédit : [Simon Gee Giraudot](#) (Creative Commons By-Sa)

---

## Quand l'open source investit dans la diversité, tout le monde y gagne

Le groupe d'utilisateurs [Python](#) de Boston est passé en 2 ans de presque rien à 15% de femmes.

Ce qui est intéressant ici c'est qu'il semblerait qu'on se

soit moins focalisé sur les femmes que sur les débutant(e)s, avec pour conséquence une croissance du nombre de femmes.



## Quand l'open source investit dans la diversité, tout le monde y gagne

[When open source invests in diversity, everyone wins](#)

*Lynn Root – 15 octobre 2013 – OpenSource.com*

*(Traduction : lyn, SonicWars, aKa, Théotix, Cryptie, Moosh + anonymes)*

Jessica McKellar est une entrepreneuse, une ingénieure logiciel et une développeuse open source. Elle aide à l'organisation du groupe d'utilisateurs Python à Boston et joue un rôle important dans la sensibilisation de la diversité en favorisant l'arrivée d'encore plus de débutants et de femmes. La participation a augmenté de 0-2% à 15% et le groupe d'utilisateurs a connu la même progression pendant les 2 dernières années.

Ce sont de tels résultats qui ont convaincu Jessica que quand des communautés open source s'investissent dans la diversité, cela profite à tout le monde. Depuis la création de cours pour

débutants, des ateliers de niveau intermédiaire et des marathons open source, le groupe de Boston a vu sa taille plus que quintupler en passant de 700 membres à plus de 4000. C'est maintenant le groupe d'utilisateurs le plus important du monde. Ce type de croissance est quelque chose à laquelle toutes les communautés open source devraient aspirer.

Plus d'informations sur [Jessica McKellar](#) dans cette interview.

**Depuis combien de temps participez-vous à la communauté open source ? Avez-vous eu un mentor quand vous avez commencé ?**

Ma toute première contribution à un projet open source était sur la documentation du projet [Twisted](#) en 2009 (Twisted est un moteur réseau événementiel écrit en Python). Je suis restée impliquée dans le projet depuis, je suis désormais une contributrice principale et j'ai même eu le plaisir d'écrire un livre sur Twisted.

Contribuer à Twisted a été une première expérience fantastique : la communauté disposait d'une documentation à l'usage des nouveaux contributeurs, et a été à la fois une aide et un soutien patient lorsque j'ai satonné dans mes premières utilisations des processus et des outils. Je ne dirais pas que j'ai eu un mentor en particulier, mais j'ai bénéficié de l'aide collective de la communauté Twisted et du feedback patient des reviewers sur mes premiers tickets.

**Comment voyez-vous l'évolution des logiciels libres depuis que vous avez rejoint la communauté ?**

Il y a eu une formidable progression vers la diversité elle-même et sa sensibilisation, en particulier vers les débutants et tout ce qui s'y rapporte. L'augmentation de l'adoption de codes de conduite dans les conférences techniques, le [programme GNOME de sensibilisation auprès des femmes](#), le programme de sensibilisation et d'éducation de la [fondation Python](#) ainsi que les événements [PyCon's Young Coders](#) sont quelques exemples du très beau travail que la communauté open

source accomplit pour devenir un environnement accueillant et favorable.

**Vous êtes profondément impliquée dans la communauté Python. Pourquoi Python ? Quelle était votre première expérience avec ce langage ?**

J'ai utilisé Python pour la première fois à l'école (j'étais au MIT au moment du changement dans le tronc commun Informatique de Scheme vers Python) et je l'ai utilisé dans chacun des emplois que j'ai pu avoir. C'est aussi mon langage par défaut pour la plupart de mes projets parallèles. En plus d'être un langage qui, à mon avis, est un bonheur pour développer, je me suis investie dans la communauté Python encouragée par son engagement dans un environnement favorable et accueillant pour tous.

**Vous et Asheesh Laroia avez fait une [belle présentation](#) lors de la PyCon 2012 à propos du groupe d'utilisateur de Boston Python augmentant son champ d'action. Pouvez-vous décrire ce que vous avez fait ?**

Ces 2 dernières années, le [Boston Python](#) a lancé une liste d'événements récurrents qui se concentrent sur les moyens d'amener plus de femmes dans les communautés Python locales. La première étape de la liste est de faire un week-end workshop pour les personnes programmant pour la première fois, ce que nous avons fait huit fois pour plus de 400 femmes.

Dans ce projet nos objectifs sont :

- D'attirer plus de femmes dans la communauté de programmation locale, avec un objectif chiffré de 15% de femmes dans tous les événements du groupe d'utilisateurs Python de Boston ;
- De mettre en avant de bons exemples de femmes programmeurs ;
- De développer des ressources à destination des autres groupe de programmation, pour qu'ils puissent organiser

leurs propres événements en faveur de la diversité.

Avant de lancer ces workshops, il y avait entre 0 à 2% de femmes à un événement standard du groupe d'utilisateurs Python de Boston. Depuis la participation des femmes à ce type d'événement a atteint, voire dépassé, les 15%. Ces manifestations rassemblent de 80 à 120 personnes : le nombre de femmes présentes a donc littéralement bondi, à la fois en pourcentage et en valeur absolue. Encore plus impressionnant, ces résultats se maintiennent depuis maintenant 2 ans !

Le grand secret de cette initiative est que même si vous vous concentrez sur un groupe particulier de personnes sous-représentées, tout le monde en bénéficie. Lancer ces workshops introductifs nous a forcé à apprendre comment aider les débutants. Nous avons commencé un projet de suivi mensuel *Project Night* de ces workshops, pour donner aux débutants et intermédiaires plus d'opportunités d'apprendre et de pratiquer le langage avec un mentor présent. Nous avons développé des cursus et des projets pratiques qui ont été utilisés partout dans le monde. Nous avons lancé des workshops pour les niveaux intermédiaires et des marathons open source. À travers tout cela, le groupe d'utilisateurs a quintuplé, passant de 700 à plus de 4000 membres, en faisant de notre groupe le plus grand groupe d'utilisateurs de Python au monde.

Pour résumer, quand vous investissez dans la diversité, tout le monde y gagne.

Crédit photo : [Jessica McKellar](#)

---

# Histoire d'une photo : le phare de Battery Point #Wikipedia

Voici une histoire toute simple mais qui raconte peut-être quelques chose de notre époque.

Lorsque KoS a demandé à son auteur l'autorisation de traduction voici quelle a été [sa réponse](#) :

Last week, someone contacted me via email and asked politely if I was ok with him translating one of my latest blog posts into French. I replied that the content of my blog was under a CC-BY SA 3.0 license, which allows the free re-use of the material for any purpose. A few days later, this person sent me the French version of my text that he had created with three other free knowledge enthusiasts. I'm still blown away by so much kindness and I'm deeply grateful for the work of the four people that I still don't know who they are. Alors, "KoS, lamessen, Paul Scailyna and goofy" – merci beaucoup pour la traduction, vous êtes extraordinaire !





## Histoire d'une photo : le phare de Battery Point

### [Story Behind The Shot: Battery Point Lighthouse](#)

*Frank Schulenburg – 28 septembre 2013 – Site personnel  
(Traduction : KoS, lamessen, Paul Scailyna et goofy)*

« Alors, vous avez fait tout le chemin depuis San Francisco hier juste pour prendre une photo du phare ? »

« Oui, je suis photographe pour Wikipédia ».

Je suis assis à côté de Rick, conducteur de taxi à Crescent City, à six heures de voiture de là où je vis. Rick me conduit à l'aéroport, où je pourrai louer une voiture suite à un accident que j'ai eu la nuit dernière. Il me regarde et rigole. « Combien ils vous paient ? »

« Rien, je fais ça bénévolement. »

Rick me regarde. Il est stupéfait. « Mais ils remboursent au



moins l'essence et l'hôtel. »

« Non, je paye tout de ma poche. »

« Pour prendre une photo de notre phare ? »

Visiblement Rick pense que je suis fou. « Oui, le phare. Nous n'avons pas de bonne photo du phare de Battery Point. »

Rick rigole encore, secoue la tête et sourit, « La prochaine fois, appelez-moi, je vous prendrai toutes les photos que vous voulez ».

Je n'avais pas envie de me lancer dans une discussion sur la difficulté de prendre vraiment une bonne photo d'un bâtiment. Combien de tentatives il me faut pour obtenir la bonne exposition, la bonne composition. Je n'ai pas non plus abordé [« Wiki Loves Monuments »](#), la compétition annuelle pour laquelle je prenais le phare en photo. Mais la réaction de Rick m'a fait réfléchir. C'était la troisième personne à qui je racontais mon histoire depuis mon arrivée à Crescent City, cette petite ville voisine de la frontière de l'Oregon. Et toutes les personnes avec qui j'avais parlé avaient eu la même réaction. Ils ont tous pensé que j'étais fou. Ou du moins étrange.

[Crescent City](#) est située sur la côte pacifique, dans la partie nord-ouest supérieure de la Californie. La pêche, le bois et le tourisme sont les principales sources de revenus. D'après Wikipédia, le revenu moyen par habitant en 2003 était de 13 000 dollars et près de 34 % des familles vivaient en dessous du seuil de pauvreté.

Est-ce bizarre de conduire près de 500 kilomètres pour prendre une photo d'un phare ? Peut-être. Du moins du point de vue de quelqu'un vivant à Crescent City. La plupart des gens avec qui j'ai discuté connaissaient Wikipédia. Cependant, aucun d'entre eux ne savait que les articles sont rédigés par des bénévoles. Pareil pour les photos. Certains pensaient que j'étais un

photographe professionnel. À chaque fois que je disais « C'est une bonne chose de donner aux autres l'accès à une information libre », les gens acquiesçaient. Mais on voyait bien que le bénévolat n'est pas quelque chose de très répandu dans cette partie de la Californie.

Je suis rentré chez moi le même jour que celui où j'avais parlé avec Rick. J'ai beaucoup pensé aux gens que j'avais rencontrés. Et à leur réaction face à mon histoire.

Oui, c'est une bénédiction de pouvoir faire des choses qu'on aime pendant son temps libre. Ce mois-ci, des bénévoles du monde entier ont participé à « Wiki Loves Monuments », la plus grande compétition photo du monde. Ils y investissent leur savoir-faire, leur temps libre et parfois leur propre argent pour documenter le patrimoine culturel de plus de 50 pays. Au moment où je vous parle, [plus de 250 000 images](#) ont été déposées sur Wikimedia Commons, le dépôt de médias de Wikipédia. C'est un énorme succès ! Chapeau à ceux qui mettent en ligne mais aussi aux nombreux volontaires qui ont fait un super boulot dans l'organisation de ce concours. J'ai adoré, même si mon voyage à Crescent City s'est terminé de façon inattendue. J'aurais aimé prendre plus de photos de phares et passer le mot sur Wikipédia à des dizaines de milliers de bénévoles.

Heureusement, j'ai eu quelques photos acceptables du phare de Battery Point. Et je suis sûr que je vais y retourner. Il y a encore de nombreux phares le long de la côte de Californie et de l'Oregon qui n'ont pas une bonne photo sur Wikipédia...

*Crédit photo : [Frank Schulenburg](#) (Creative Commons By-Sa)*