

Atelier CNIL Associations du libre et de l'open source

Partenariat pour un gouvernement ouvert

Septembre 2022

Cette synthèse de l'atelier organisé par la CNIL en mars 2022 reprend les échanges et les propositions faites par des associations de défense des droits et libertés, dont le contexte est précisé ci-dessous. Elle ne constitue pas un engagement de la CNIL mais vise à recenser les constats et pistes de travail faits par la société civile dans le cadre des ateliers tenus début mars 2022.

L'engagement de la CNIL dans le Partenariat pour un gouvernement ouvert

La CNIL s'est engagée le 17 décembre 2021, dans le cadre du Partenariat pour un gouvernement ouvert, à « *engager le dialogue avec la société civile sur les questions de protection des données, pour faire d'un droit individuel un sujet collectif* ».

Cet engagement, dont vous retrouvez le détail en annexe, est porté par le Laboratoire d'innovation numérique de la CNIL (LINC) et s'inscrit dans le prolongement des recommandations formulées dans le cahier Innovation et Prospective Scènes de la vie numérique, publié en avril 2021¹ : pour l'accompagnement au développement de « corps intermédiaires » de la donnée.

Dans ce cadre, le LINC a organisé en mars 2022 une série de trois ateliers thématiques avec des représentants de la société civile : associations de défense des droits et libertés, syndicats et représentants des travailleurs, collectifs et association du libre et de l'open source (FLOSS).

Contexte

Face à l'uniformisation des outils et services numériques proposés par les grandes plateformes selon des standards majoritairement étatsuniens, ou plus simplement pour limiter la prospection commerciale non désirée et la publicité invasive, les individus soucieux de la protection de leurs données peuvent avoir recours à des « tactiques » de contournement, plus ou moins sophistiquées.

En parallèle, la communauté technique de l'informatique occupe un rôle majeur dans l'évolution des techniques depuis 40 ans et revendique la mise à disposition d'outils ouverts et libres, au service de chacun. S'il est nécessaire d'outiller les individus afin qu'ils puissent numériser et automatiser ces contournements, la proposition de services alternatifs et le développement des communautés free/libre/open-source software (FLOSS) – rassemblant à la fois les logiciels libres et les logiciels à code source ouvert, qui malgré des cultures et des philosophies divergentes ont des modèles de développement logiciel similaires² – porteurs de projets et solutions vertueuses du point de vue de la protection des données est à encourager et à accompagner.

Cet atelier d'idéation a été l'occasion d'échanger sur ces différentes questions, notamment comment inciter et encourager le développement de nouvelles briques techniques qui jouent aujourd'hui le rôle de porte d'accès à des contenus ou des services (navigateurs, systèmes d'exploitation mobiles, réseaux sociaux) ; comment permettre à des solutions et standards protecteurs de la vie privée de passer à l'échelle afin de bénéficier des effets réseaux qui leur permettront de se développer ; comment organiser un dialogue régulier avec la CNIL.

Les associations représentées lors de cet atelier étaient : April, Debian France, Free Software Foundation Europe, Software Heritage, Tor / Nos Oignons, Framasoft. Des représentants de différents services de la CNIL prenaient part aux échanges. L'atelier était animé par le service du Laboratoire d'innovation numérique (LINC).

Moyens d'actions des associations et relations à la CNIL

Moyens d'action

Les modalités d'actions des associations sont diverses dans leur forme. Chaque association peut avoir recours à l'un ou l'autre de ces modes d'actions, souvent plusieurs, sur des échelons différents selon leur objectif et leur périmètre d'action. Ces types et modes d'actions, non exhaustifs, représentent le périmètre dans lequel les associations interviennent.

- **Promouvoir les logiciels libres**

L'ensemble des associations présentes a pour mission la promotion des logiciels libres, sous diverses formes et échelons. Elles peuvent agir globalement pour les logiciels libres (April, FSFE), mettre à disposition des outils (FramaSoft) pour promouvoir des solutions en particulier (Nos Oignons, Debian France), en France, dans l'espace francophone, en Europe.

¹ [Cahier IP n°8, Scènes de la vie numérique \(PDF, 5,1 Mo\), cnil.fr](#)

² « [Free/Libre Open Source Software](#) », [wikipedia.org](#)

- **Dialoguer avec les développeurs de logiciels libres**

Les associations peuvent dialoguer avec les communautés de développeurs afin de mettre en forme les logiciels, pour qu'ils soient utilisés par le plus grand nombre. (Debian France)

- **Mettre à disposition des logiciels libres**

Les associations peuvent héberger et mettre à disposition des solutions et des services en ligne libres (Framasoft).

- **Conservation des logiciels libres**

Un projet est mené visant à construire une archive universelle de tous les codes sources disponibles, afin de rendre plus transparente la façon dont les outils sont construits. (Software Archive).

- **Actions de sensibilisation du grand public**

Les associations dans leur ensemble peuvent agir par la sensibilisation du grand public aux enjeux du numérique et au logiciel libre, par l'affichage dans les médiathèques, par la participation à des colloques et conférences, par l'organisation d'ateliers.

Elles s'appuient pour cela sur des groupes locaux (April par exemple).

- **Actions de plaidoyer**

Les associations agissent par des actions de plaidoyer afin d'obtenir des décisions politiques, juridiques et réglementaires favorables au développement du logiciel libre (April), comme centre de compétences pour les politiciens, juristes et journalistes (FSFE), ou auprès des acteurs de la science ouverte (Software Archive).

- **Agir sur la protection des données des solutions**

Les associations peuvent agir sur la protection de la vie privée en configurant les logiciels par défaut pour qu'ils soient *privacy-friendly* (favorables au respect vie privée), par la minimisation des données (Debian France, Framasoft), parce que leur solution est par nature protectrice de la vie privée (Tor/Nos Oignons).

Les associations agissent également sur la promotion de la défense de la vie privée au travers de très nombreuses interventions (Framasoft).

Perceptions et relations à la CNIL

Les associations, dans leur ensemble, ont assez peu, voire pas de relations à la CNIL – ou alors de manière très ponctuelle – mais seraient intéressées pour les développer, de différentes manières.

- **Volonté de trouver des ressources**

Les associations engagées dans des actions de développement ou d'accompagnement du développement seraient preneuses de directives et/ou de checklists sur les questions de données personnelles. (Debian France)

- **La protection des données n'est pas toujours le cœur de métier du libre**

Si certaines solutions du libre sont par nature protectrice des données, à l'image de Tor, la protection des données n'est pas le « cœur de métier » du libre. Mais les associations sont convaincues que le logiciel libre doit être un des éléments indispensables pour renverser les paradigmes actuels. (April)

- **Volonté de faire remonter des informations du terrain**

Les associations pourraient contribuer et faire remonter à la CNIL des retours du terrain, « en particulier des personnes qui n'y connaissent rien », pour que ce soit pris en compte.

- **Volonté de disposer d'outils**

Les associations attendent de la CNIL qu'elle propose plus d'outils pour les développeurs, au-delà du guide développeur.

En tant qu'hébergeur de services, savoir quels sont les données traitées par les logiciels est lourd et compliqué, les associations auraient besoin d'un langage pour décrire les données traitées. (Frama)

- **Souhait que la CNIL participe de la promotion des logiciels libres (par tous les participants)**

Atelier

Quels sont les leviers pour encourager le développement de briques techniques respectueuses des libertés ?

Les participants à l'atelier constatent que les alternatives existent mais qu'il manque différents leviers qui doivent permettre de les développer et les maintenir, tant techniquement que financièrement. Bien souvent les développeurs vont travailler dans l'urgence et aller au plus vite, vers des solutions clés en main. Ils sont pris entre plusieurs feux et notamment celui du marketing qui les poussent à aller vers solutions moins respectueuses des droits des personnes (à l'image de ce que le LINC avait constaté pour les designers en 2018, dans le cadre d'une étude réalisée à la sortie du cahier *La forme des choix*³).

Pourtant le logiciel libre a gagné dans les briques inférieures du développement (bases de données, langage, protocoles, bibliothèques, etc.) et de l'installation (serveurs web, systèmes d'exploitation), tous les développeurs travaillent sur du libre aujourd'hui, mais il reste beaucoup à faire sur la partie applications finales, qui souvent tournent sur des solutions propriétaires.

Idées de projets et pistes d'actions

Les participants proposent une série de leviers et de pistes d'action pour encourager le développement de briques « vertueuses » :

- **Promouvoir les briques existantes**

Les associations proposent une série de pistes à étudier pour la promotion des briques, à mettre en place par les régulateurs, les développeurs, les formateurs.

- **À destination des développeurs :**

- Permettre à ces briques d'atteindre un niveau de qualité équivalente à celles des GAFAM en termes de design UX, pour encourager leur utilisation.
- Sensibiliser les développeurs au risque de « dépendance aux gros » qui peut parfois jouer des tours (par exemple lorsqu'un service gratuit devient subitement payant ou dont les tarifs évoluent, à l'exemple de Google Maps), et au bénéfice du libre (gain sur le long terme, accumulation des connaissances, etc.)
- Permettre à ces briques de gagner en visibilité en engageant des actions de promotion, par exemple par la CNIL.
- Sensibiliser à l'importance de la documentation du code afin de permettre la réutilisation par les développeurs.
- Investir dans la maintenance des outils libres, plus compliqué que le seul prototypage.

- **À destination des utilisateurs :**

- Encourager clairement à l'utilisation, faire la promotion des solutions respectueuses de la vie privée (plus largement que ce qui est fait aujourd'hui) ;

- **Mettre en place des hubs régionaux de la CNIL**

Les associations encouragent à la création d'un réseau de la CNIL en France, et plus seulement à Paris, afin de toucher tous les publics de développeurs.

- **Aller vers de la certification (et/ou récompenses/reconnaisances)**

Les associations proposent une série de moyens qui pourraient être étudiés par la CNIL et, plus largement, les autorités de protection pour la certification de certaines briques et certains services.

- **Aller vers la certification de certaines briques** et/ou technologies afin de provoquer des effets leviers, et générer des modèles économiques.
- **Organiser des concours pour élire le « logiciel de l'année »** dans un concours de développeur.

³ [Cahier IP n°6, La forme des choix \(PDF, 1.4 Mo\), linc.cnil.fr](#)

- **Agir sur les systèmes d'exploitation et les navigateurs** : promouvoir des solutions protectrices de la vie privée intégrées aux navigateurs.
- **Proposer des formats de paywall standardisés** pour promouvoir des modèles économiques différents.

- **Activer le levier juridique / sanction**

L'application de la loi (et les sanctions) sont des leviers pour le développement de ces briques, à l'exemple de la décision sur Google Analytics, dans un contexte où les développeurs sont soumis aux contraintes du marketing.

- **Encourager le financement et/ou le développement de nouveaux modèles économiques**

Les participants poussent à la recherche par les communautés FLOSS de nouveaux modèles économiques, dont certains pourraient être encouragés par les autorités et gouvernements.

- S'inspirer des modèles développés dans la presse (La Presse Libre) comme le fonds de dotation (non lucratif) ou le fonds de pérennité (lucratif)
- Sortir des logiques de *charity business* (financement et mercantilisation d'œuvres caritatives) pour accompagner le développement de modèles économiques.
- Encourager des nouveaux modèles d'entreprises pour des modèles pérennes et vertueux.
- Financer la recherche par des appels à projets.

- **Rôle de l'État facilitateur / acteur**

Les participants poussent à des actions de l'État pour organiser et favoriser l'offre de services libres au grand public comme aux développeurs.

- Proposer un service public des solutions libres avec une infrastructure dédiées et des solutions en SAAS (sans pour autant tout centraliser). Offrir des outils centralisés tout en permettant la décentralisation.
- Mettre en place des aides de l'État aux logiciels libres (au-delà de la promotion).
- Actionner le levier de la commande publique pour développer le libre et l'open source.
- Développer ces actions à l'échelon européen
- Sortir d'une stricte logique d'utilisation des logiciels libres, et développer une politique active de contribution (en l'incluant dans les cahiers des charges des marchés publics ou en s'appuyant sur des compétences internes (que les agents publics soient membres, en tant qu'agent, des communautés, ou par exemple en envisageant de libérer du temps de travail des agents concernées sur le principe de la décharge).
- Soutenir les initiatives vertueuses des agents publics (par exemple avec <https://apps.education.fr/>, développé pendant le confinement pour proposer au corps enseignant des services libres, hébergés par le ministère).

- **Accentuer l'aspect formation**

La formation des développeurs est un des points importants à mettre en œuvre pour une meilleur prise en compte de la protection des données par ces derniers, mais aussi par leurs organisations.

- Travailler à la formation des formateurs : l'éthique et le droit ne sont pas enseignés dans les écoles de code. La protection des données résulte souvent d'intérêts individuels, mais n'est pas un sujet porté par les organisations/écoles. La formation donne le pouvoir de refuser (dès lors que l'on sait ce qui est légal, ce qui ne l'est pas, notamment).
- Introduire des cours de culture numériques dans les écoles de code
- La CNIL pourrait publier un Mooc des développeurs (en plus du guide développeur)

Comment permettre à des solutions et standards protecteurs de la vie privée de passer à l'échelle afin de bénéficier des effets réseaux

Les participants à l'atelier constatent que le passage à l'échelle de solutions et de standards protecteurs de la vie privée se heurte à des enjeux organisationnels, d'informations et d'interopérabilité. En premier lieu, l'usage massif de solutions propriétaires au sein des organisations (écoles, entreprises, administrations, etc.) crée un chemin de dépendance, dont il est difficile de dévier. Par ailleurs, les individus ou les organisations devant faire des choix d'une solution ne disposent pas toujours d'une information claire sur le degré protecteur des services qui leur sont proposés. Enfin, le changement vers une solution plus protectrice doit être facilité par une interopérabilité permise par l'élaboration de normes et de standards. Les solutions plus protectrices doivent enfin apporter un niveau de services (design, fonctionnalités, stabilité, etc.) au moins équivalent aux autres pour que les individus se tournent vers elles.

Idées de projets et pistes d'actions

- **Proposer des modèles de fédération et des bases éthiques⁴**
 - Promouvoir les modèles décentralisés et fédérés qui permettent des adaptations avec par exemple la création d'instances selon les besoins, plutôt qu'une seule base centrale.
 - Promouvoir une approche systémique et éviter de penser seulement en alternative par le changement d'un logiciel propriétaire pour du libre.
- **Travailler à des solutions sécurisées, *by design, by default* (dès la conception et par défaut)**
 - Encourager au paramétrage « protecteur » par défaut des fonctionnalités d'un service, d'une application ou d'un logiciel afin que l'utilisateur doivent faire un effort pour avoir des paramètres moins protecteurs.
 - Ex. Signal Secure by default.
 - Ex. Debian et la minimisation des logs.
 - Promouvoir et contribuer à l'interopérabilité par une plus forte représentation des institutions publiques dans les groupes de normalisation (ex. W3C, IETF).
- **Promouvoir le levier du design afin de rendre les logiciels attractifs et *privacy by design***
 - Par exemple en accompagnant un logiciel très utilisé pour faire en sorte qu'il soit *privacy-friendly* (favorable au respect de la vie privée) : les gens sont passés à Signal parce que c'est une application (pas de problème d'interface).
 - Intégrer une approche UX et un design orienté « préservation de la vie privée » dans le développement afin de mettre en capacité les développeurs (par exemple par la minimisation de la charge cognitive afin d'éviter les erreurs, etc.).
 - Le monde du logiciel libre ne doit pas comprendre que des développeurs, mais également des (UX) designers.
 - La protection des données n'est qu'un facteur ; il faut avant tout que le logiciel fonctionne bien.
- **Développer la commande publique**
 - Par l'effet symbolique de mise en visibilité par l'usage des acteurs publics.
 - Ex. Mobilizon pour l'agenda des événements des collectivités territoriales.
 - Par le levier juridique : imposer aux acteurs publics un usage prioritaire des logiciels libres⁵ et faire respecter la réglementation déjà existante (ex. du référentiel général d'interopérabilité – RGI).
 - Faire évoluer la culture des agents publics pour les amener vers les logiciels libres pour contrer l'inertie sur les logiciels utilisés (due aux coûts d'entrée et de changement).
 - Investir dans le développement de nouvelles fonctionnalités et/ou mettre en commun les développements (et leurs financements) si plusieurs acteurs publics souhaitent la même fonctionnalité.

⁴ Sur le modèle de l'initiative CHATONS, le Collectif des Hébergeurs Alternatifs, Transparents, Ouverts, Neutres et Solidaires

⁵ Voir l'initiative <https://publiccode.eu/>

- **Pousser des actions d'éducation et d'information**
 - **Auprès des publics :**
 - Mener des actions de pédagogie auprès des citoyens, par la communication et l'éducation.
 - Création de documentations et de ressources sur les alternatives.
 - **Auprès des développeurs :**
 - Informer les développeurs des données collectées et pour quels usages, quand on récupère du code, par exemple en mettant un fichier GDPR.txt dans la racine des sites (à l'exemple du projet lancé par Framasoft : <https://gdpr-txt.org/>).
 - Sensibiliser au risque du *cargo culting* : on parle de culte du cargo en informatique lorsqu'un programmeur emprunte un bout de code (le copier-coller) sans le comprendre et espère qu'il fera la chose attendue dans un tout autre contexte.
- **Engager des actions d'audit et de transparence pour développer la confiance**
 - **Mettre en avant les solutions utilisées par la CNIL** qui sont respectueuses de la protection des données, à l'image de Matomo comme alternative à Google Analytics.
 - **Mettre en place des *privacy score* (score de protection des données) pour les applications ou services**
 - Par exemple avec un classement des applications mobiles.
 - Faire du *machine learning* (apprentissage automatique) pour détecter les mauvais acteurs.
 - Ce type d'action devra aller avec l'explicitation des critères de choix pour permettre de comparer les applications ou services.
 - **Financer un audit tiers des logiciels libres sur leur conformité en matière de données personnelles**, sur le même modèle que l'audit financé par le gouvernement US sur la sécurité des logiciels libres.
 - **Pour éviter l'écueil du versioning, développer des outils permettant d'automatiser les audits**, sur le modèle de Exodus Privacy.

Quelles seraient les conditions d'un dialogue régulier entre la CNIL et la société civile (associations) ?

Les représentants des communautés FLOSS sont ouverts à créer les conditions de dialogue sur des formats ouverts et variés, en s'appuyant notamment sur des réseaux existants (ou en cours de création comme les Blue Hats), ou en ouvrant des canaux asynchrones avec la CNIL.

Idées de projets et pistes d'actions

- **Se rattacher à des réseaux existants :**
 - **Se rattacher au réseau Blue Hats** en cours de constitution par le pôle du logiciel libre de Etalab, auquel le LINC a été convié.
- **Créer un espace de discussion dédié au développement :**
 - **Avoir un Community Manager Tech** à la CNIL
 - **Ouvrir un canal de discussion asynchrone** sur un support dédié, liste de discussion ou autre (les communautés du libre sont souvent bénévoles)
 - **Créer un « bureau du logiciel libre »** : une personne référente qui officierait en tant que canal dédié et privilégié.
- **Créer un événement annuel « Privacy Code »**
 - Un **forum d'échange** sur le libre et la protection des données
 - Une « **non-conférence** » où les participants font le programme
 - Une **nouvelle itération de ce genre d'atelier PGO** pour maintenir le contact
 - **S'inspirer des** Open Tech Fund <https://www.opentech.fund/> (qui font également du financement), des événements de partage et de facilitation.