Résistances et alternatives

Table des matières

Objectifs

- Interroger les impacts personnels du capitalisme de surveillance en construisant son modèle de menace
- Découvrir les différents types d'alternatives et retenir quelques exemples
- Passer à l'action à son échelle, à son rythme, selon ses propre modalités
- Être en capacité de se représenter des imaginaires alternatifs

Introduction

Le capitalisme de surveillance est un système économique et socio-technique intégré dans la plupart des aspects de la modernité occidentale.

Il implique les États, les industriels de la surveillance et les géants du numérique dans une relation symbiotique qui s'inscrit pleinement dans la tendance néolibérale :

- Croissance (consumérisme, création de nouveaux débouchés pour les industries en place, création de nouveaux marchés, accélération de l'extraction de ressources) ;
- Désinvestissement de l'État dans la vie économique (dérégulation des marchés, privatisation) ;
- Recentrage de l'État sur la gestion de l'ordre (surveillance et répression des résistances).

Cette tendance n'est pas totale et il existe nombre de nuances à apporter. Néanmoins, le capitalisme de surveillance a des impacts profonds qu'il est possible d'appréhender sous plusieurs prismes et échelles :

- Individuelle (santé mentale, vie privée, esprit critique, libre-arbitre...) ;
- Régionale (panoptique, discriminations raciales, statut de l'espace public...) ;
- Nationale (algorithmisation de la vie publique, suspicion généralisée, répression des militances, influences électorales...) ;
- Internationale (néo-colonialisme, pollution, guerres civiles, extractivisme, conditions de travail proches de l'esclavage...).

Ce module propose quelques pistes pour s'émanciper du capitalisme de surveillance selon différents points de vue et différentes échelles, forcément incomplètes et partielles.

I Agir en tant qu'individu

1. Réduire les risques

L'information, clé du pouvoir d'agir — Fondamental

« Travailler sur un chantier ou à un bureau ;

Partager des bijoux de piercing, des sextoys, ou sa brosse à dents ;

Se connecter à Internet ou utiliser des outils numériques ;

Monter dans une voiture ou faire du vélo…

Toutes ces pratiques comportent des risques… et on peut les réduire !

Comme le dit Act Up : « information = pouvoir ».

Boum, 2023[Boum, 2023], chap. 6. »

Risque et menace — Az Définition

« Le risque, c'est de s'abimer les mains en arrachant des ronces sans gants, la menace c'est le patron qui met au placard ses salariées syndiquées ;

Le risque, en conduisant ivre, c'est d'avoir un accident, la menace c'est de se faire retirer son permis de conduire ;

Le risque, quand on n'a pas fait de sauvegarde, c'est de perdre toutes ses données si un disque dur plante, la menace c'est que la police perquisitionne le lieu d'activité militante où il est stocké ;

Le risque c'est un bug dans un logiciel qui fait planter l'ordi, la menace c'est Cambridge Analytica qui utilise les données des comptes Facebook pour influencer les résultats des élections.

Boum, 2023[Boum, 2023], chap. 6. »

Modèle de menace — Az Définition

« Processus par lequel des menaces potentielles, telles que les vulnérabilités structurelles peuvent être identifiées, énumérées et classées par ordre de priorité - du point de vue de l'hypothétique agresseur.

Wikipédia[1] »

1. https://fr.wikipedia.org/wiki/Mod%C3%A8le_de_menace

Surface d'attaque

Az Définition

« Somme des différents points faibles (vecteurs d'attaque) par lesquels un utilisateur non autorisé pourrait s'introduire dans un environnement et en soutirer des données.

Wikipédia[2] »

L'intuition est mauvaise conseillère

⚠ Attention

Les idées qui viennent spontanément répondent rarement correctement aux questions qu'il faut se poser d'abord : **que veut-on protéger, et de qui ?**

Que veut-on protéger ?

Méthode

Le mot protection recouvre en réalité plusieurs besoins :

- **Confidentialité** : cacher des informations aux yeux indésirables ;
- **Intégrité** : conserver des informations en bon état, et éviter qu'elles ne soient modifiées sans qu'on s'en rende compte ;
- **Accessibilité** : faire en sorte que des informations restent accessibles aux personnes qui en ont besoin.

Ces besoins rentrant en conflit, il s'agit, pour chaque ensemble d'informations à protéger, de poser des priorités et trouver des compromis.

De qui veut-on se protéger ?

Méthode

« des parents intrusifs, des camarades de classe susceptibles de faire du harcèlement, des voleurs voulant récupérer des coordonnées bancaires, un ex-conjoint violent qui cherche des moyens de contrôle ou de chantage, des hiérarchies trop curieuses, la police chargée de mater un mouvement social, des fonctionnaires qui contrôlent les personnes migrantes[3], les GAFAM qui traquent et vendent les données personnelles, des services de renseignement mandatés pour ficher massivement une communauté ou un courant politique, *etc.*

Boum, 2023[Boum, 2023], chap. 7 »

La question centrale est les moyens dont disposent les adversaires :

- Moyens judiciaires : par exemple, la possibilité qu'une commission rogatoire autorise la police à saisir du matériel informatique, ou le fait qu'il peut être exigé de donner sa clé de chiffrement.
- Moyens techniques : avancées non rendues publiques sur le cassage de chiffrement, clusters de calculs, etc.

2. https://fr.wikipedia.org/wiki/Surface_d%27attaque
3. https://www.ritimo.org/10-menaces-contre-les-migrant-es-et-les-refugie-es - https://www.ritimo.org/10-menaces-contre-les-migrant-es-et-les-refugie-es

- Moyens politiques : par exemple, dans quelle mesure l'État français peut-il collaborer avec la NSA ?
- Relations de pouvoir : notamment dans le cas où l'acteur est capable de nuisance (un GAFAM fermant un compte, un patron menaçant de licenciement, etc).

Le risque zéro n'existe pas

⚠ Attention

Tout dispositif numérique relié à Internet est par essence, vulnérable. L'intégralité des couches (du matériel le plus bas-niveau aux logiciels installés sur un système d'exploitation) sont susceptibles de comporter des failles ou des portes dérobées.

Vulnérabilités connues

Exemple

- Au niveau des logiciels et des sytèmes d'exploitaiton : https://www.cvedetails.com/
- Au niveau des processeurs (CPU) : https://en.wikipedia.org/wiki/Transient_execution_CPU_vulnerability
- Au niveau du microcode des composants matériels (*firmware*) : https://www.csoonline.com/article/3480590/12-wide-impact-firmware-vulnerabilities-and-threats.html

La NSA implente des backdoors dans le matériel

Exemple

« L'agence implante ensuite des outils de surveillance clandestins, reconditionne [les routeurs] avec leur sceau d'origine et les expédie. La NSA obtient ainsi l'accès à l'ensemble des réseaux et à tous leurs utilisateurs. Le rapport observe avec jubilation que « *SIGINT tradecraft … is very hands-on (literally!)* » [jeu de mot intraduisible].

Une fois en fonctionnement, l'appareil vérolé se connecte à la NSA. Le rapport poursuit : « dans une infiltration récente, après plusieurs mois, un mouchard implanté par le biais d'une interception de la chaîne d'approvisionnement a contacté l'infrastructure de la NSA. Cette connexion nous a permis de prendre le contrôle de l'appareil et d'étudier le réseau. »

Greenwald, 2014[Greenwald, 2014] »

Quelle confiance accorder en un outil ?

Méthode

- Pourquoi cet outil a-t-il été développé ?
- Est-il libre ?
- Quel est son modèle économique ?
- À qui doit-il rendre des comptes ?

2. Quelques scénarios d'auto-défense

2.1. Introduction

Les scénarios d'auto-défense se concentrent uniquement sur l'individu et son pouvoir d'agir. Ils existent en raison de deux traditions principales :

- La pensée **libertarienne**, qui met l'accent sur les libertés individuelles ; ici le droit fondamental à la vie privée. C'est avec cette idée que les débats autour de la *privacy* naissent aux États-Unis dans les années 60 (*Masutti, 2020*[Masutti, 2020, p. 191-]).
- L'**anti-répression**, un ensemble de savoirs et pratiques diffusés dans les milieux militants pour se protéger d'un pouvoir (policier, judiciaire) considéré comme dangereux.

2.2. Se protéger des pisteurs

Situation de départ

Vous avez un Windows et un Android avec Google Chrome.

De quoi veut-on se protéger ? Fondamental

- Pistage sur le navigateur local (historique, frappe au clavier...) ;
- Pistage sur les sites web (via les cookies tiers...) ;
- Conditions Générales d'Utilisation (revente et utilisation des données...) ;
- Réquisitions judiciaires (n'importe quelle trace laissée).

Changer de navigateur Méthode

Il n'y a pas le choix : on ne peut pas se protéger d'un navigateur web muni d'outils de surveillances sans en changer.

Mozilla Firefox

Firefox est un logiciel libre qui ne collecte pas les données, et dont les données de compte sont chiffrées.

Bloquer les pisteurs

Méthode

uBlock Origin

uBlock Origin[4] est une extension (désormais bloquée par Chrome[5] dans sa version complète) qui implémente une large palette de techniques pour réduire le pistage.

> Conçu comme un bloqueur de publicités léger et efficace, uBlock Origin est réputé pour ses listes de filtres complètes et sa faible consommation de ressources. Contrairement à d'autres bloqueurs de publicités, qui ciblent principalement les éléments publicitaires visuels, uBlock Origin adopte une approche plus large, bloquant les requêtes au niveau du réseau vers les domaines publicitaires et de suivi connus. Cette stratégie proactive améliore non seulement le temps de chargement des pages, mais réduit également les menaces pour la vie privée associées aux méthodes de distribution et de suivi des publicités.
>
> *Madikeri et Madisetti, 2024*[Madikeri et Madisetti, 2024]

Bloquer les pisteurs sur Android

Complément

AdAway

4. https://ublockorigin.com/
5. https://www.lesnumeriques.com/appli-logiciel/chrome-interdit-ublock-origin-quelles-alternatives-pour-continuer-a-bloquer-les-publicites-n233769.html

AdAway utilise la fonctionnalité de VPN local introduite par Android 8 pour intercepter et bloquer toutes les requêtes vers des domaines de pisteurs. Un des effets de bord est généralement de supprimer la publicité de l'ensemble des applications.

Risques résiduels ⚠ Attention

- Pisteurs intégrés au système d'exploitation (MacOS, Android, Windows...) ;
- Données laissées « volontairement » sur des services ;
- Techniques plus sophistiquées (signaux résilients[6], fingerpriting[7]...).

2.3. Protéger ses communications

Situation de départ

Vous parlez avec vos potes sur Discord, vous envoyez des fichiers avec WeTransfer, vous travaillez sur Google Drive.

De quoi veut-on se protéger ? 💡 Fondamental

- Intrusions dans la vie privée (ciblée ou généralisée) ;
- Conditions Générales d'Utilisation (revente et utilisation des données...) ;
- Réquisitions judiciaires (n'importe quelle trace laissée).

Les communications traditionnelles sont en clair 💬 Remarque

Les mails et les SMS transitent « en clair », c'est-à-dire que n'importe quel intermédiaire peut les lire.

Le plupart des communications sont chiffrées 💬 Remarque

Les données transférées via HTTPS (Discord, Google Drive) ne peuvent être lues que l'émetteur, l'intermédiaire et le destinataire.

Quelques communications sont chiffrées de bout en bout 💬 Remarque

Dans ce scénario, les seuls personnes en capacité d'accéder aux données sont l'émetteur et le destinataire.

6. https://www.pixeldetracking.com/fr/les-signaux-resilients-de-facebook-ou-comment-la-surveillance-sadapte
7. https://coveryourtracks.eff.org/

Le chiffrement de bout en bout est la seule solution robuste

Fondamental

Le chiffrement de bout en bout repose sur le fait que **vous et vous seul·e** possédez une **clé de déchiffrement** permettant de lire le contenu. Grâce à des techniques basées sur les mathématiques, cette clé est *a priori* incassable avec les moyens actuels et ne transite jamais sur le réseau.

Le chiffrement de bout en bout effraye les autorités

Complément

« Les mesures de confidentialité actuellement mises en place, telles que le chiffrement de bout en bout, empêcheront les entreprises technologiques de voir les infractions commises sur leurs plateformes. Elles empêcheront également les forces de l'ordre d'obtenir et d'utiliser ces preuves dans le cadre d'enquêtes visant à prévenir et à poursuivre les crimes les plus graves, tels que les abus sexuels sur mineurs, la traite des êtres humains, le trafic de drogue, les homicides, les crimes économiques et les actes terroristes.

Europol, 2024[Europol, 2024] »

« Le gouvernement australien a adopté un nouveau texte législatif qui permet aux organismes gouvernementaux chargés de l'application de la loi de forcer les entreprises à remettre les informations et les données des utilisateurs, même si elles sont protégées par la cryptographie. Si les entreprises n'ont pas le pouvoir d'intercepter les données cryptées pour les autorités, elles seront obligées de créer des outils permettant aux forces de l'ordre ou au gouvernement d'accéder aux données de leurs utilisateurs.

Bocetta, 2019[Bocetta, 2019] »

Comprendre le chiffrement

Complément

Découverte du chiffrement (cf. p.43), *Chiffrement symétrique* (cf. p.45), *Chiffrement asymétrique* (cf. p.48).

Les clés privées doivent rester privées

Attention

« iCloud utilise des méthodes de sécurité robustes, applique des politiques strictes pour protéger vos informations et est à la pointe du secteur en matière d'utilisation de technologies de sécurité préservant la confidentialité, telles que le chiffrement de bout en bout pour vos données. [...] Vos données iCloud sont chiffrées, **les clés de chiffrement sont sécurisées dans les centres de données Apple** afin que nous puissions vous aider à récupérer vos données.

Apple, 2025[Apple, 2025], je souligne. »

« Notez que MTProto prend en charge deux couches : **le chiffrement client-serveur utilisé** dans les discussions cloud Telegram et le chiffrement de bout en bout utilisé dans les discussions secrètes Telegram.

Telegram, 2025[Telegram, 2025], je souligne.

Dans ces deux exemples, des services faisant la promotion du chiffrement de bout en bout ne l'appliquent que dans des cas spécifiques ou bien gardent une copie de la clé privée, cassant de fait le chiffrement de bout en bout.

Pour les discussions instantanées

Méthode

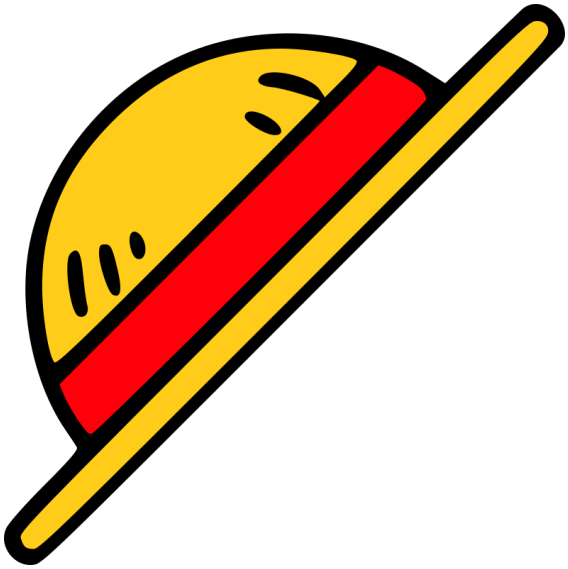
Signal

Signal est facile d'accès et a plusieurs avantages :

- Chiffrement de bout en bout même pour les conversations de groupe
- Chiffrement de l'émetteur et d'autres métadonnées

Pour le transfert de fichiers

Méthode

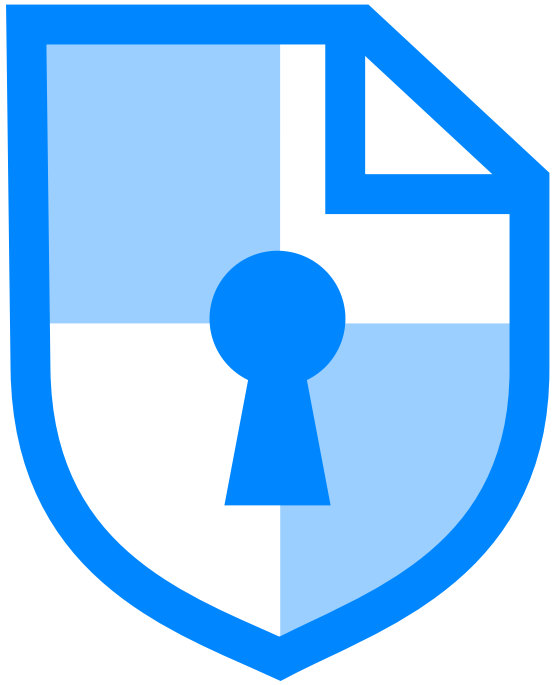


Lufi (« Let's Upload That File »), par exemple chez Picasoft → drop.picasoft.net[8]

8. https://drop.picasoft.net/

Pour une suite à la Google Drive

Méthode



« CryptPad fournit une suite bureautique complète avec tous les outils nécessaires à une collaboration productive. Les applications comprennent : Rich Text, Spreadsheets, Code/Markdown, Kanban, Slides, Whiteboard et Forms.

Toutes les données sur CryptPad sont cryptées dans le navigateur. Cela signifie qu'aucune donnée lisible ne quitte l'appareil de l'utilisateur. Même les administrateurs du service ne peuvent pas voir le contenu des documents ou les données des utilisateurs.

CryptPad est conçu pour permettre la collaboration grâce à des fonctionnalités telles que les disques durs d'équipe, le calendrier et le partage. Il synchronise les modifications apportées aux documents en temps réel. Comme toutes les données sont cryptées, le service et ses administrateurs n'ont aucun moyen de voir le contenu en cours d'édition et de stockage.

cryptpad.org[9] »

2.4. Sécuriser son système d'exploitation

Situation de départ

Vous avez Windows.

9. cryptpad.org - https://cryptpad.org/about/

De quoi veut-on se protéger ?

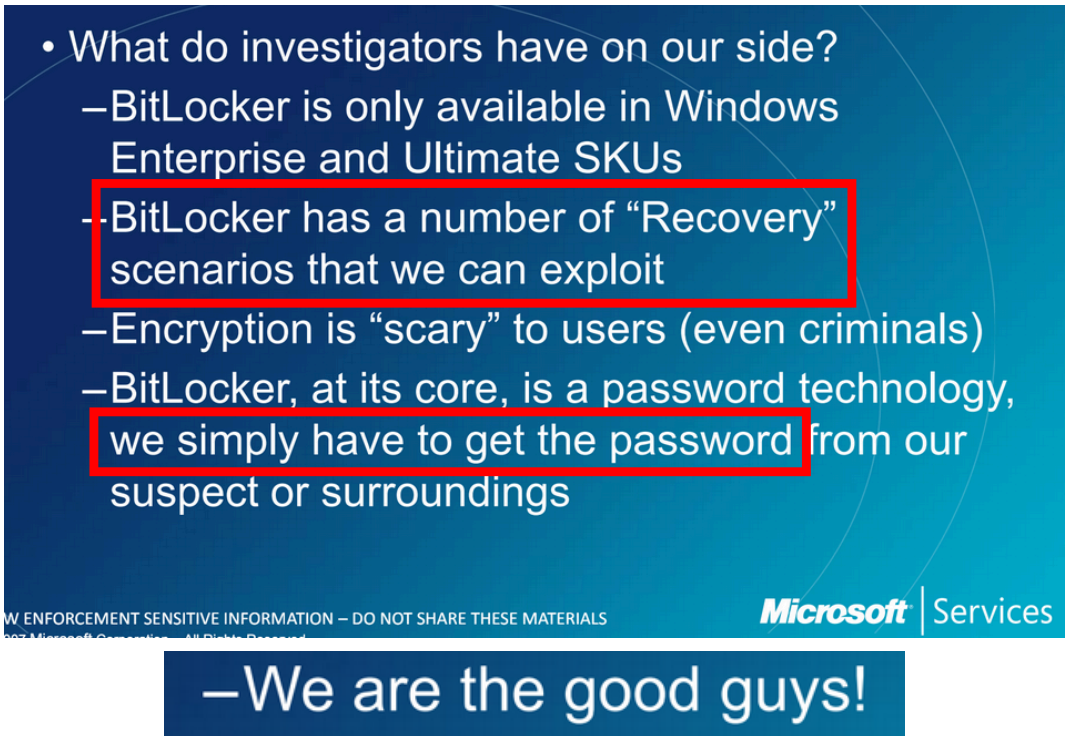
Fondamental

- Code fermé troué de failles ;
- Leak massif de données (télémétrie) ;
- Chiffrement du disque volontairement faible ;
- Longue histoire de collaboration.

Collaboration avec la NSA

Exemple

BitLocker, le logiciel de chiffrement de données de Windows, a été volontairement rendu vulnérable, notamment pour les besoins de la NSA (*Palisson, 2016*[Palisson, 2016]).



Utiliser un système d'exploitation libre

Méthode

Linux Mint, une distribution clé en main, moderne et sécurisée, approuvée par moi et par ma maman qui déteste l'informatique

Chiffrement de disque

Complément

La plupart des distributions Linux permettent de chiffrer le disque à l'installation avec une case à cocher. En d'autres termes, il est mathématiquement impossible pour quiconque de récupérer le contenu des données quand l'ordinateur est éteint, même en accédant au disque dur.

2.5. Se protéger des États

Ne pas confondre protéger droits et commettre des actes répréhensibles

Attention

- Protéger ses communications et son identité, particulièrement dans un contexte répressif, sont des droits fondamentaux ;
- Toutes les personnes qui utilisent ces technologies ne le font pas dans le but de contourner la loi ;
- Parfois, briser la loi est salutaire pour l'intérêt général : le cas des lanceur·ses d'alerte est un exemple classique ;
- Dans certains régimes autoritaires, briser la loi est nécessaire pour accéder à l'information et à l'expression.

Situation de départ

Vous naviguez sur Internet avec un navigateur libre, un système d'exploitation libre, les bonnes extensions, tout ce qui va bien.

De quoi veut-on se protéger ?

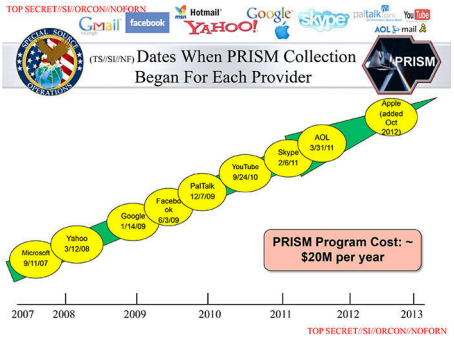
Fondamental

Un État qui a accès à toute la chaîne de transmission de l'information :

- Les FAI
- Les serveurs web
- Éventuellement, des pisteurs sur l'ordinateur local

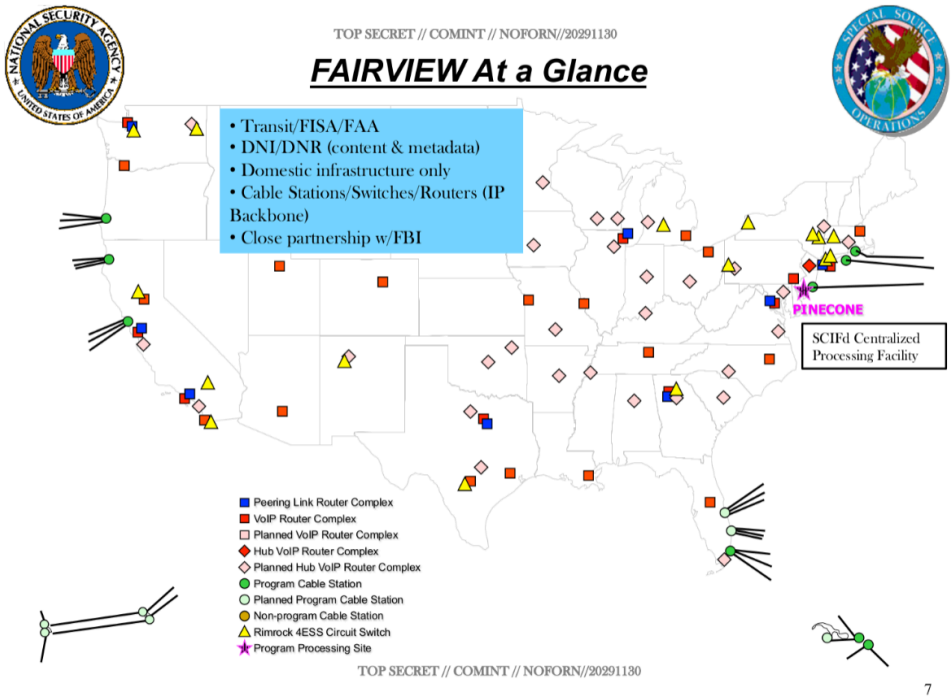
PRISM et les FAI américains

Exemple



Selon Edward Snowden, liste des entreprises utilisées par PRISM et l'année où la collecte d'information a commencé

> « Les documents montrent que AT&T a permis à la NSA d'avoir accès à des milliards de mails échangés sur le territoire américain, parmi lesquels ceux du siège des Nations unies à New York, dont AT&T est le fournisseur d'accès internet. [...] ATT a commencé en 2011 à fournir quotidiennement à la NSA plus d'un milliard de relevés de téléphones portables. »

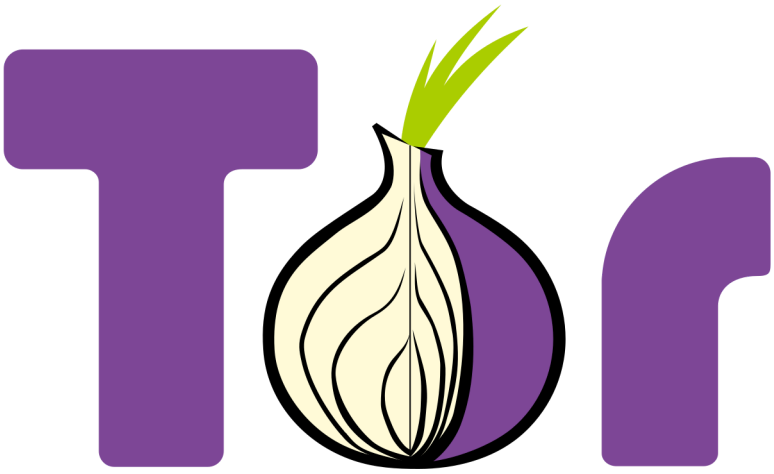


SSO Corporate Partner Access briefing slides

> « [AT&T] transmet à la seconde des données sur les appels téléphoniques, les courriels et d'autres communications dans Internet, si elles sont menées par des citoyens étrangers et qu'elles passent par des câbles de communications ou des stations-relais d'importance situés en sol américain. [...] il s'agit d'une société « très collaborative » (*highly collaborative*) qui fait montre d'un « extrême empressement d'aider » (*extreme willingness to help*).
>
> Wikipédia[10] »

Anonymiser sa navigation

Méthode



Logo de Tor (The Onion Router)

- Réseau d'environ 8000 machines (« noeuds ») opérés par des bénévoles, des associations...
- Associé à une version modifée de Firefox...
- Pour un observateur, il est impossible de savoir qui a visité quoi.
- Tor se rajoute par dessus les autres mesures (HTTPS, chiffrement du contenu...)
- Il existe aussi des « services cachés » (`.onion`) accessibles uniquement via Tor.

Ne laisser aucune trace sur sa machine

Méthode

10. https://fr.wikipedia.org/wiki/Fairview_(programme)

> « Un outil de communication recommandé par des extrémistes sur des forums extrémistes
>
> NSA *(code source XKeyScore)* »

Notamment utilisé durant les *leaks* de l'affaire Snowden.

- Système autonome sur une clé USB ;
- Effacement complet des traces après utilisation ;
- Logiciels soigneusement audités ;
- Toutes les connexions passent par Tor.

Conclusion

Quand bien même ces solutions **techniques** pourraient parvenir à leurs fins, elles s'inscrivent nécessairement dans un jeu du chat de la souris et ne peuvent pas, à elles seules, constituer une porte de sortie du capitalisme de surveillance.

II Quelques pistes collectives

1. Introduction

Les solutions techniques évoquées précédemment, si elles ne sont pas suffisantes, peuvent être des briques permettant de construire des alternatives. Dans la mesure où elles sont déjà libres et parfois même mathématiquement résistantes à toute forme de surveillance, il reste alors à examiner les aspects sociaux, politiques, juridiques.

2. Élevons des chatons

Contexte

Framasoft est une association d'éducation populaire au numérique, connue pour proposer de nombreux services web alternatifs à ceux des géants du numérique (libres, sans pistage, etc). Le nombre d'utilisateur·ices augmente chaque année, mais pour autant...

> « Framasoft est, et souhaite rester, une association à taille humaine, un groupe de passionné·es qui expérimentent pour tenter de changer le monde (un octet à la fois). Il y a 9 salarié·es, dans une association qui compte une trentaine de membres depuis plusieurs années. [...] nous tenons à notre modèle associatif, nous ne voulons pas croître en mode « la start up qui veut se faire plus grosse que Google ». »

En bref, Framasoft ne veut pas être le GAFAM du libre, car ça ne reste pas tous les problèmes et en particulier ceux à la centralisation.

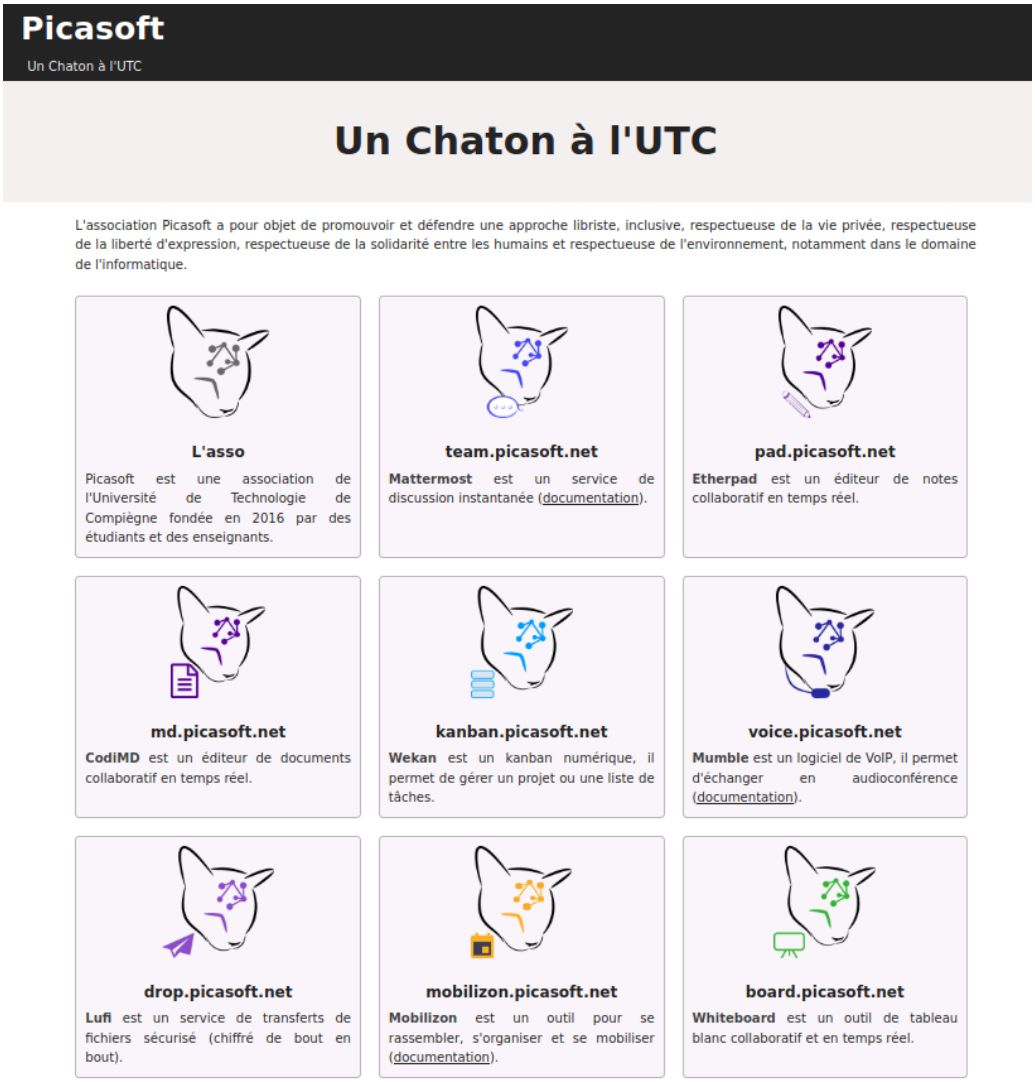
CHATONS Az Définition

Collectif des Hébergeurs Alternatifs Transparents Ouverts Neutres et Solidaires.

Tous les chatons ont en commun de proposer des services à leur utilisateur·ices, mais la typologie est large.

Picasoft, un chaton à l'UTC

Exemple



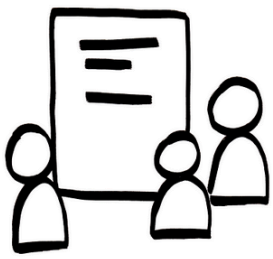
Deuxfleurs, un chaton pointu sur les systèmes distribués lowtechisés

Exemple

Deuxfleurs

Infini, un chaton qui propose une suite complète pour les particuliers, assos, entreprises...

Exemple



HÉBERGEUR LIBRE, ASSOCIATIF, SOLIDAIRE,
NON MARCHAND, MILITANT

La Contre-Voie, un chaton d'éducation populaire et d'accompagnement à la transition

Exemple

Zaclys, un chaton entreprise qui fournit quantité de services pour particuliers ou professionnels

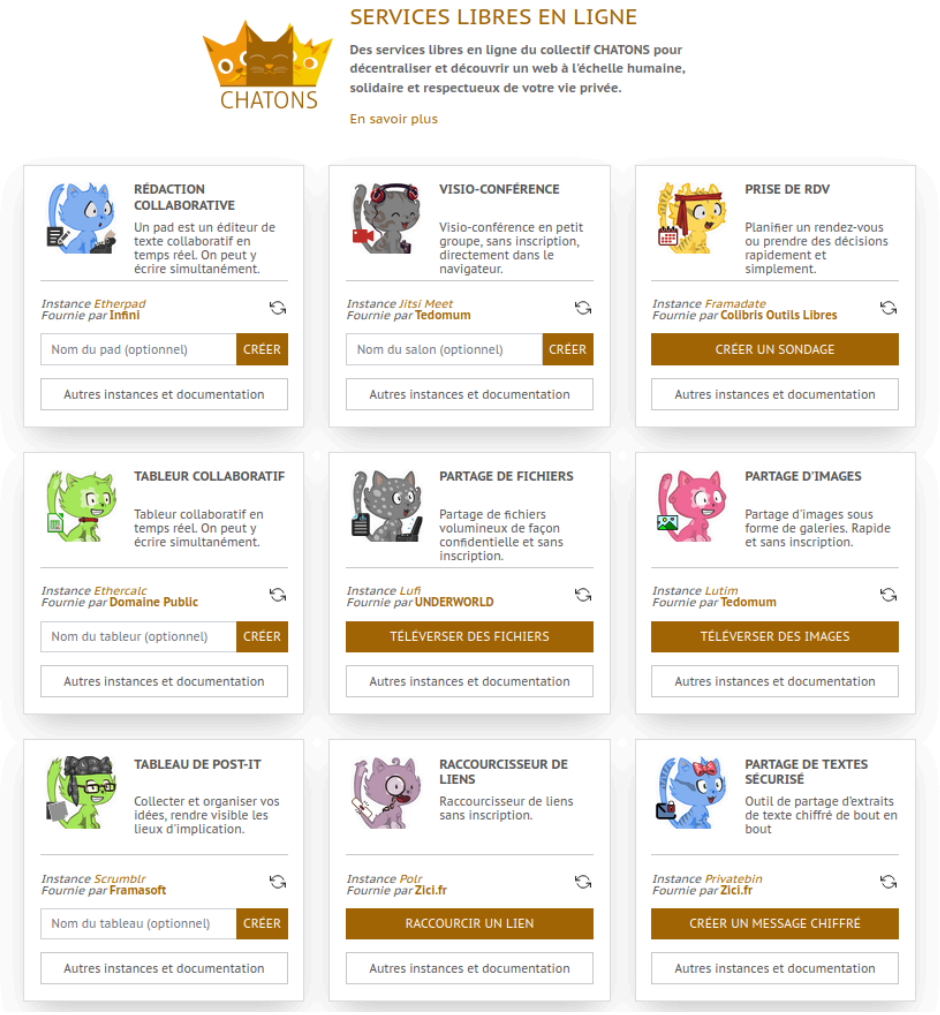
Exemple

La décentralisation promeut la résilience

Fondamental

Pendant le confinement au printemps 2020, l'enseignement à distance explose. Les outils centralisés ne parviennent pas à monter en charge rapidement. Le collectif crée entraide.chatons.org[11], qui distribue la charge en renvoyant à chaque fois à un chaton différent.

11. https://entraide.chatons.org/fr/



Archipélisation

Fondamental

Archipélisation

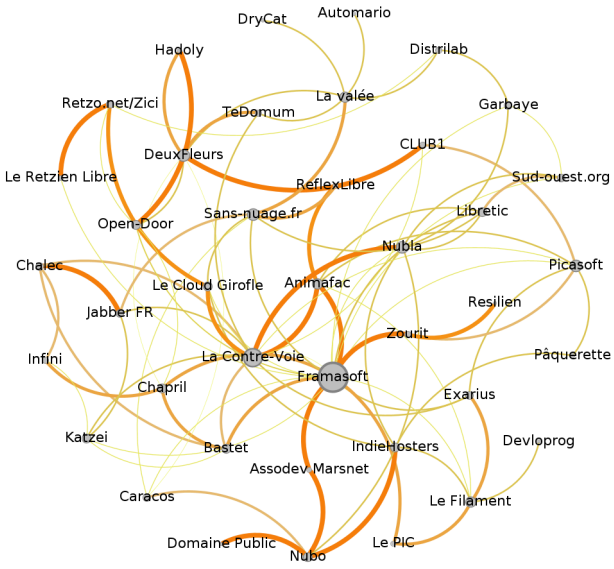
Chacun·e son identité sa culture, sa raison d'être, ses objectifs, ses moyens.
Mais on se retrouve sur des **valeurs ou des stratégies communes**.
On fait le choix de **coopérer**, même ponctuellement.

> « J'appelle créolisation la rencontre, l'interférence, le choc, les harmonies et les dysharmonies entre les cultures. » Par ces mots, Édouard Glissant [écrivain, poète, philosophe martiniquais] fait de la « créolisation » une décontinentalisation, qu'il nomme archipélisation, et qu'il corrèle à ce qu'il appelle le « tout-monde ». Le monde entier, pour lui, se créolise et s'archipélise. [...] L'objectif n'est donc plus de construire un mouvement unique, monolithique, mais bien d'envisager l'avancée des luttes sous forme de coopérations entre ces différents îlots, sans essayer de se convaincre de tous faire la même chose.
>
> *Framasoft, 2019*[Framasoft, 2019]

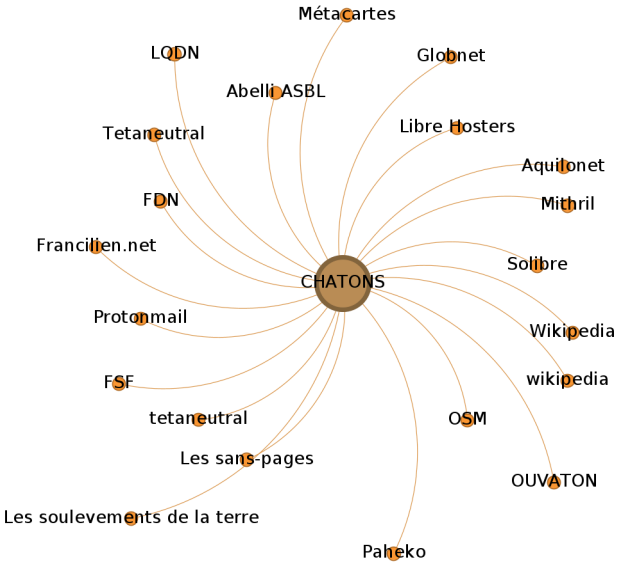
Les chatons tissent des liens

Exemple

On a vu qu'il n'était pas souhaitable de créer une méga-structure centralisée comme alternative crédible aux modèles actuels. Pour autant, une structure isolée aura peu de pouvoir d'agir. Une possibilité est de promouvoir les liens dans et hors du collectif, de sorte à pouvoir, par exemple, coordonner des actions.

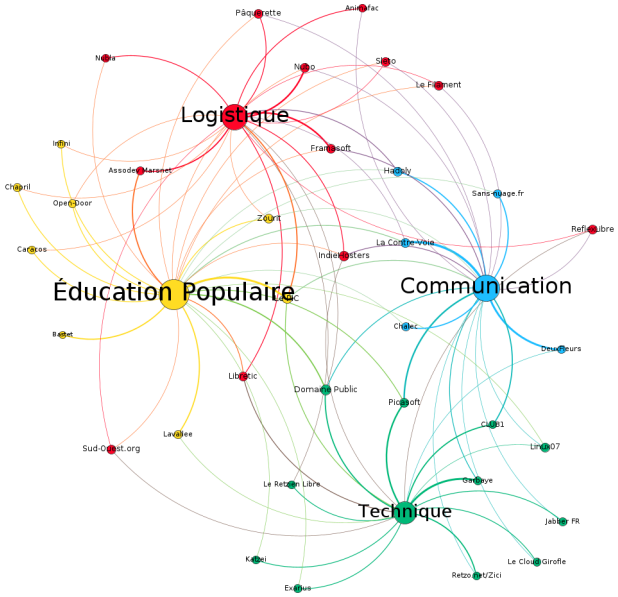


Visualisation en graphe des liens entre les membres ayant participé à la recherche



Visualisation en graphe des liens entre le collectif et des structures extérieures

Une idée est aussi de posséder et de mutualiser une variété de compétences.



Visualisation en graphe des grandes compétences liées aux structures du collectif CHATONS

3. Des médias sociaux décentralisés

3.1. Introduction

Les médias sociaux sont parmi les services pour lesquels il est le plus difficile de penser à une alternative, car c'est précisément la présence de nombreuses personnes au même endroit qui fait l'intérêt du service. Pour autant, il existe des façons décentralisées de construire les médias sociaux sans se couper du monde.

3.2. Introduction au Fediverse

Le Fediverse

Az Définition

Le Fediverse est un ensemble de médias sociaux administrés de façon autonome et connectés entre eux.

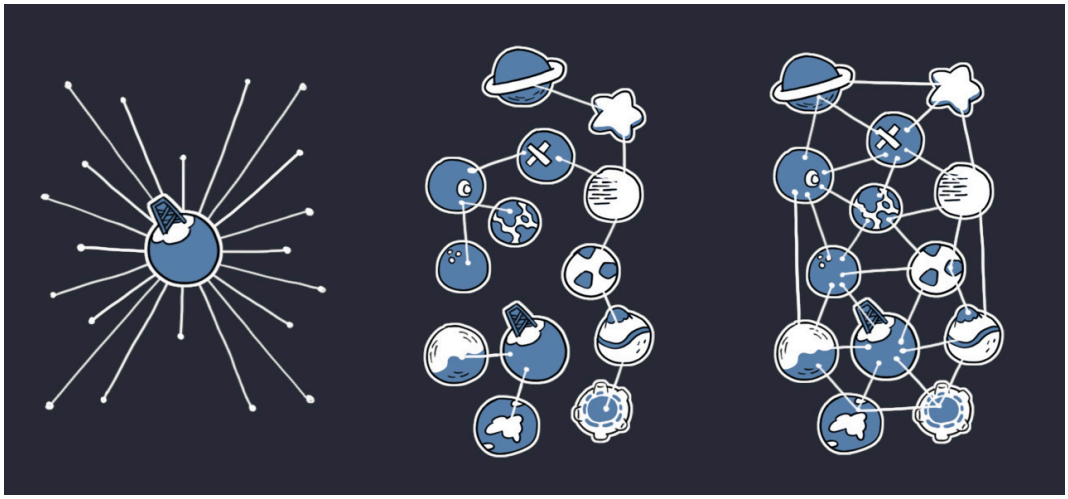
Logo du Fediverse

Trois briques fondamentales des **médias sociaux alternatifs, libres, décentralisés et fédérés** :

1. Des **instances de logiciels libres** qui communiquent avec des **protocoles standards ouverts** ;
2. La **décentralisation** ;
3. La **fédération**.

Décentralisation

Rappel



Réseaux centralisé, décentralisé (modèle du Fediverse) et distribué.

Les médias sociaux du Fediverse

Exemple

- Mastodon[12] / Pleroma[13] : des services de microblogging, alternatives à Twitter ;
- PeerTube[14] : un service de partage de vidéos, alternative à Youtube ;

12. https://joinmastodon.org
13. https://pleroma.social
14. https://joinpeertube.org/instances#instances-list

- Pixelfed[15] : un service de partage de photos, alternative à Instagram ;
- Mobilizon[16] : un service d'organisation d'événements, alternative aux groupes et événements Facebook ;
- Plume[17] / WriteFreely[18] : des moteurs de blogs ;
- Funkwhale[19] : un service de partages audios ;
- Lemmy[20] : un service de forums de discussion équivalents à Reddit ou HackerNews ;

Quelques chiffres d'utilisation (au 7 avril 2023)

- le Fediverse regroupe **~23 000 instances** (dont **~12 000 instances Mastodon**),
- sur lesquelles sont répartis **~9,3 millions d'utilisateurs** (dont **~7,1 millions d'utilisateurs de Mastodon**,
- parmi lesquels on compte **~1,3 millions d'utilisateurs actifs**).

fediverse.observer/stats.

Par où commencer — Complément

- Une porte d'entrée possible, avec la liste des médias sociaux, des protocoles et des statistiques du Fediverse : the-federation.info[21]
- D'autres portails généraux sur le Fediverse : fediverse.party[22], fedidb.org[23], instances.social , fediverse.observer
- Des listes d'instances à rejoindre : joinmastodon.org/servers , instances.joinpeertube.org[24] , instances.joinmobilizon.org ...

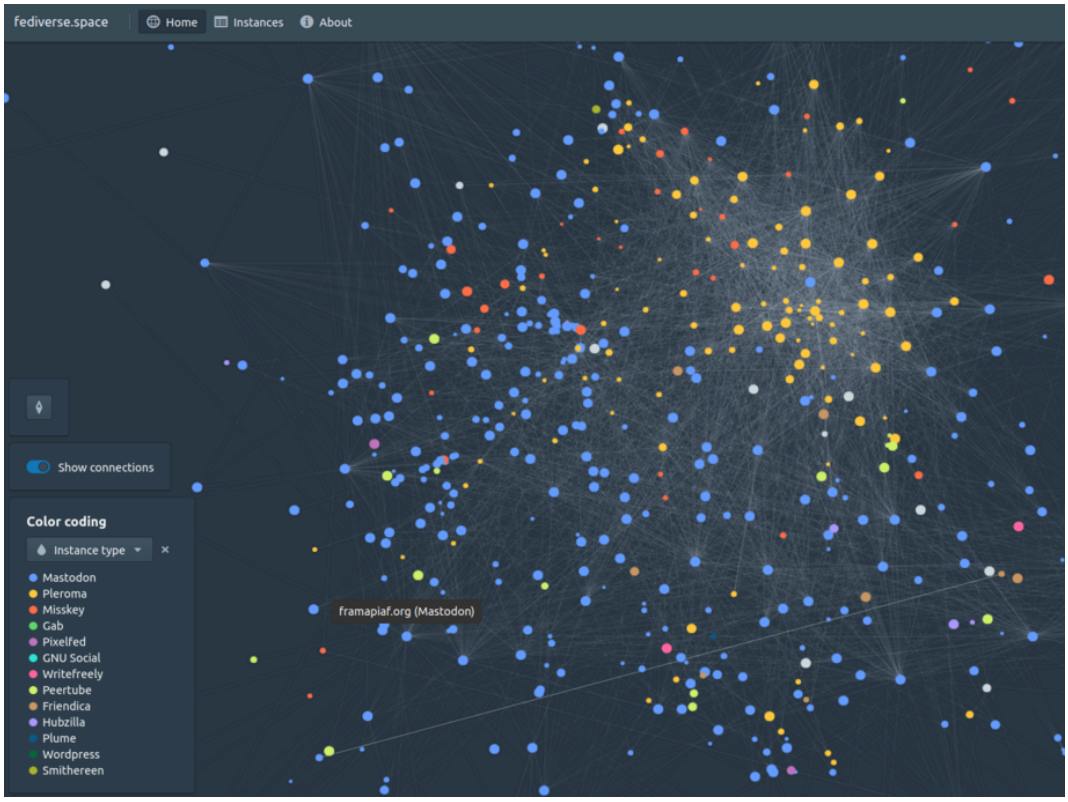
3.3. L'instance à la base du Fediverse

Instance — Az Définition

En effet, il n'y a pas qu'un seul Mastodon dans le Fediverse, mais des milliers de copies de Mastodon. Chaque copie est le résultat d'une installation du logiciel Mastodon sur un **serveur** (un ordinateur qui sert un ou plusieurs sites ou services web auxquels on accède lorsque l'on navigue sur le web).

On appelle ces copies de médias sociaux des **instances**.

15. https://pixelfed.org
16. https://joinmobilizon.org
17. https://joinplu.me/
18. https://writefreely.org/
19. https://funkwhale.audio/
20. https://join.lemmy.ml/
21. https://the-federation.info/
22. https://fediverse.party/en/portal/servers/
23. https://fedidb.org/software
24. https://instances.joinpeertube.org/



Carte interactive du Fediverse sur fediverse.space

Les serveurs du Fediverse

Remarque

On peut dire que :

```
le Fediverse =
  le média social Mastodon
+ le média social Peertube
+ le média social Mobilizon
+ ...
```

?

Les instances du Fediverse

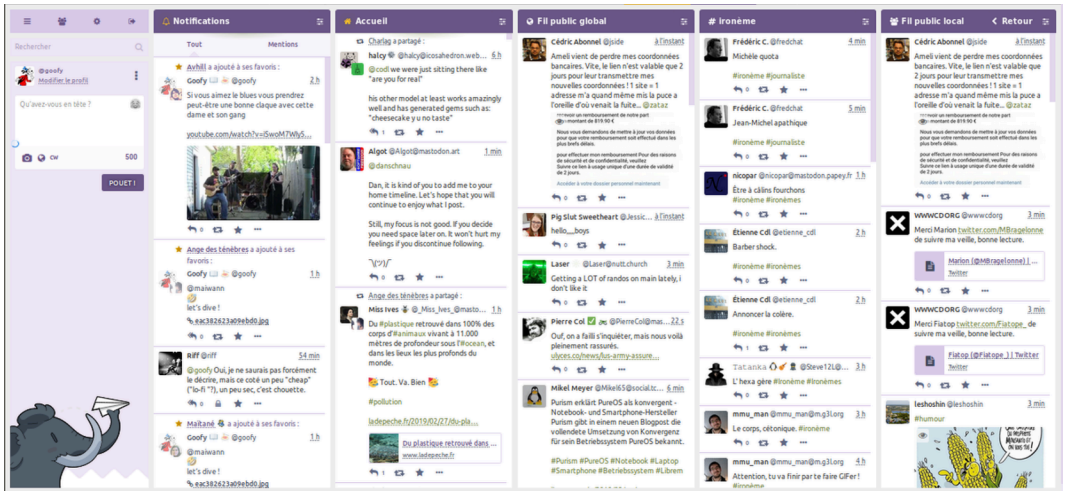
Remarque

On peut aussi (et c'est même plus précis) dire que :

```
le Fediverse =
  le serveur de l'instance du média social Mastodon de Framasoft
+ le serveur de l'instance du média social Mastodon de La Quadrature Du Net
+ le serveur de l'instance du média social Mastodon de ...
+ le serveur de l'instance du média social Peertube de Framasoft
+ le serveur de l'instance du média social Peertube de ...
+ le serveur de l'instance du média social ...
+ ...
```

L'instance Mastodon de Framasoft : https://framapiaf.org/framapiaf.org

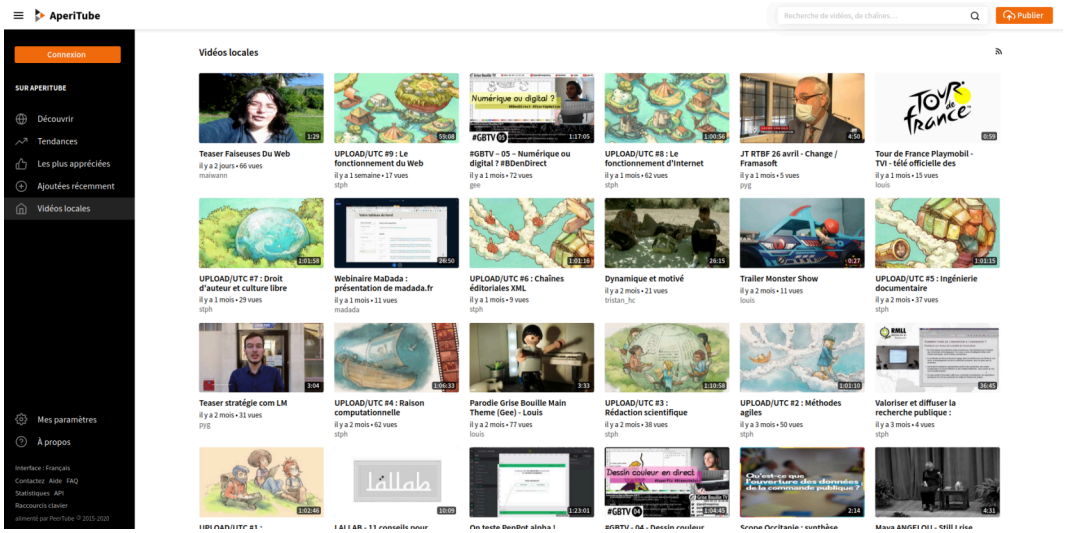
Exemple



Capture d'écran de Framapiaf

L'instance Peertube AperiTube : https://aperi.tube/aperi.tube

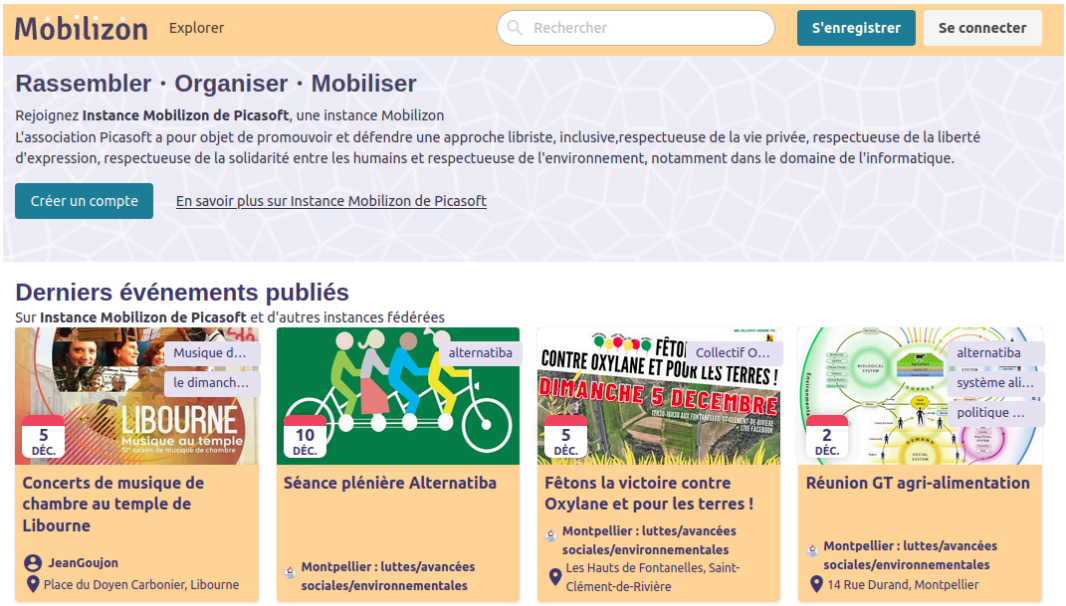
Exemple



Capture d'écran d'Aperi.tube

L'instance Mobilizon de Picasoft : https://mobilizon.picasoft.net/mobilizon.picasoft.net

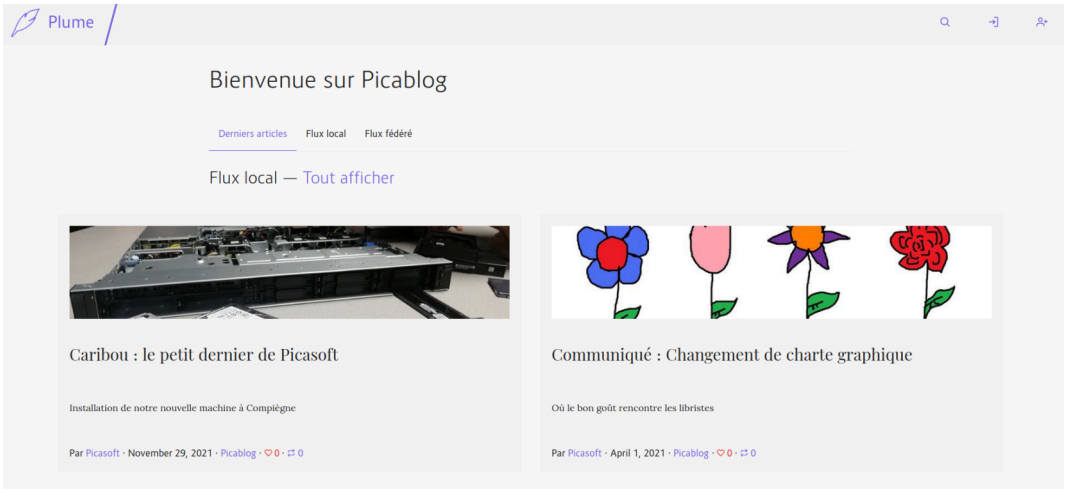
Exemple



Capture d'écran de l'instance Mobilizon de Picasoft

L'instance Plume de Picasoft : https://blog.picasoft.net/blog.picasoft.net

Exemple



Capture d'écran du Picablog

Choisir une instance pour entrer dans le Fediverse

Méthode

1. **Selon son (ou ses) activité(s) favorite(s)** : le microblogging, le partage de vidéos, de photos, de billets de blog...
2. **Selon les valeurs et les règles** que l'on souhaite respecter, et **le type de modération** qui nous convient.

instances.social

Exemple

Le site instances.social[25] propose des listes d'instances correspondant à certains **critères** : langue parlée, taille de l'instance, type de modération. Il est aussi possible d'effectuer une recherche par mots clés.

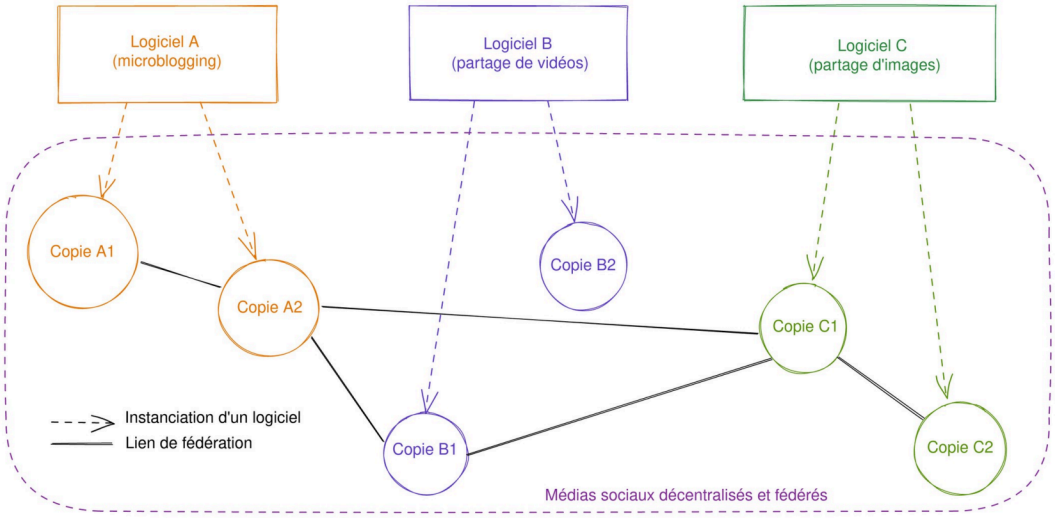
3.4. Le Fediverse en questions

Comment est-il possible d'avoir des milliers d'instances d'un média social ?

Complément

Les médias sociaux du Fediverse, comme Mastodon, sont tous des **logiciels libres**. Ils peuvent donc être installés sur un serveur par toute personne souhaitant mettre en place son propre média social, et ayant quelques compétences techniques (ou faisant appel à quelqu'un qui les a).

En installant le logiciel de média social Mastodon sur un serveur, on créé **une copie** de ce logiciel qui, une fois accessible sur le web, sera **une nouvelle instance** du média social Mastodon. Il est aussi possible de configurer, de personnaliser l'apparence et de modifier l'interface ou des fonctions du média social que l'on installe, parce que les médias sociaux du Fediverse sont sous licence libre.



Instanciation et fédération des logiciels du Fediverse

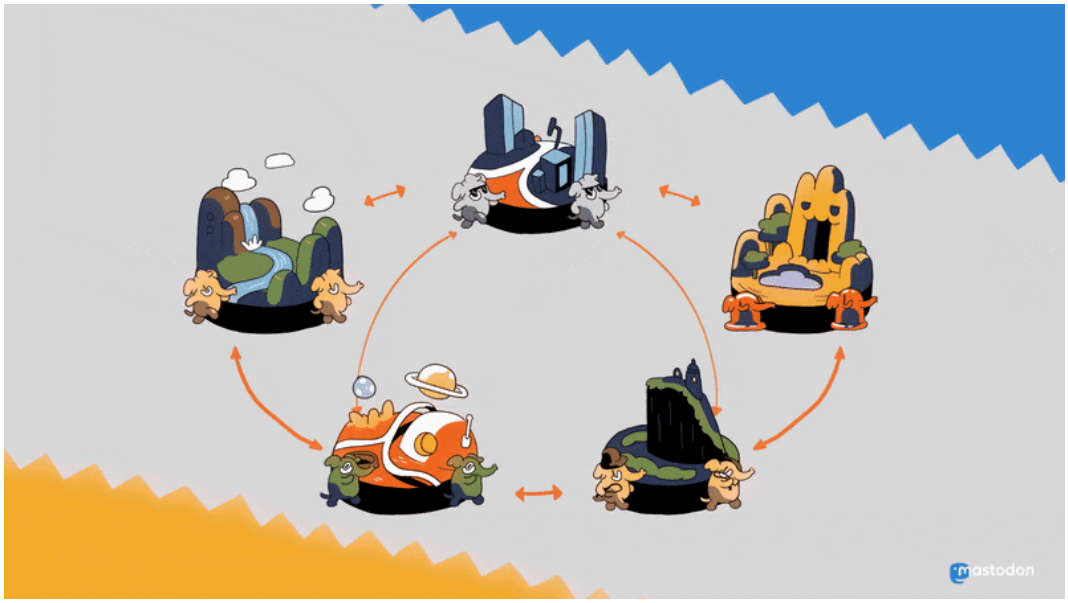
Quel est l'intérêt d'avoir plusieurs instances d'un même média social ?

Complément

Plusieurs instances de média social connectées entre elles forment **un réseau décentralisé**. Une des propriétés de ce type de réseau est de ne pas être contrôlable par un seul acteur : l'administrateur·ice d'une instance du Fediverse ne peut pas prendre le contrôle de l'ensemble du Fediverse. Ainsi, chaque instance peut exister sans dépendre des autres instances, ni techniquement, ni politiquement.

Cela donne la possibilité de faire cohabiter plusieurs communautés, différentes cultures et modes de communication en laissant à chacun un espace où vivre selon les règles qui lui conviennent, tout en maintenant des liens entre ces multiples espaces.

25. https://instances.social/



Interactions dans le Fediverse

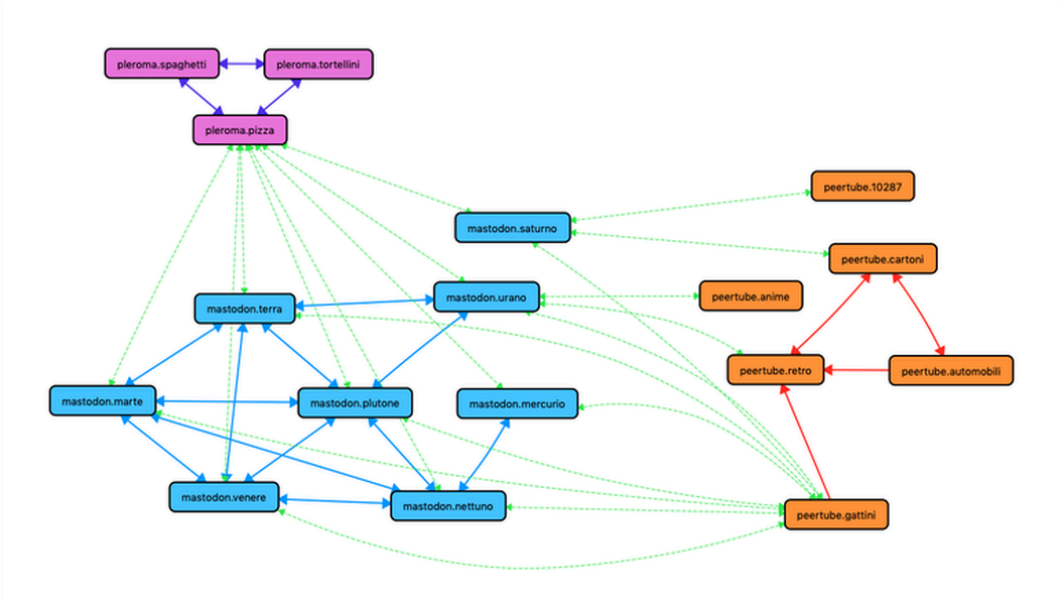
Qui administre les instances de médias sociaux du Fediverse ?

⊕ Complément

Des particuliers, des associations, des entreprises et des institutions administrent de façon autonome une ou plusieurs instances dans le Fediverse. Personne ne contrôle tout le Fediverse !

Comment les médias sociaux du Fediverse communiquent-ils entre eux ?

⊕ Complément



Fediverse connections

Les médias sociaux du Fediverse utilisent **des protocoles de communication communs**. Concrètement, cela signifie que pour échanger une information (comme un message ou un commentaire), deux médias sociaux doivent adopter un format commun pour transmettre cette information. Ainsi, deux médias sociaux différents peuvent « se comprendre », car ils suivent les mêmes règles de communication.

Le protocole principal du Fediverse est ActivityPub. Ce protocole définit par exemple comment doit être formaté un commentaire pour pouvoir être transmis entre deux instances du Fediverse. En utilisant le protocole ActivityPub, deux instances Mastodon peuvent ainsi permettre à leurs utilisateurs respectifs d'interagir comme s'ils partageaient un seul et même espace de communication.

4. Pour celles et ceux qui voudraient du « pareil »

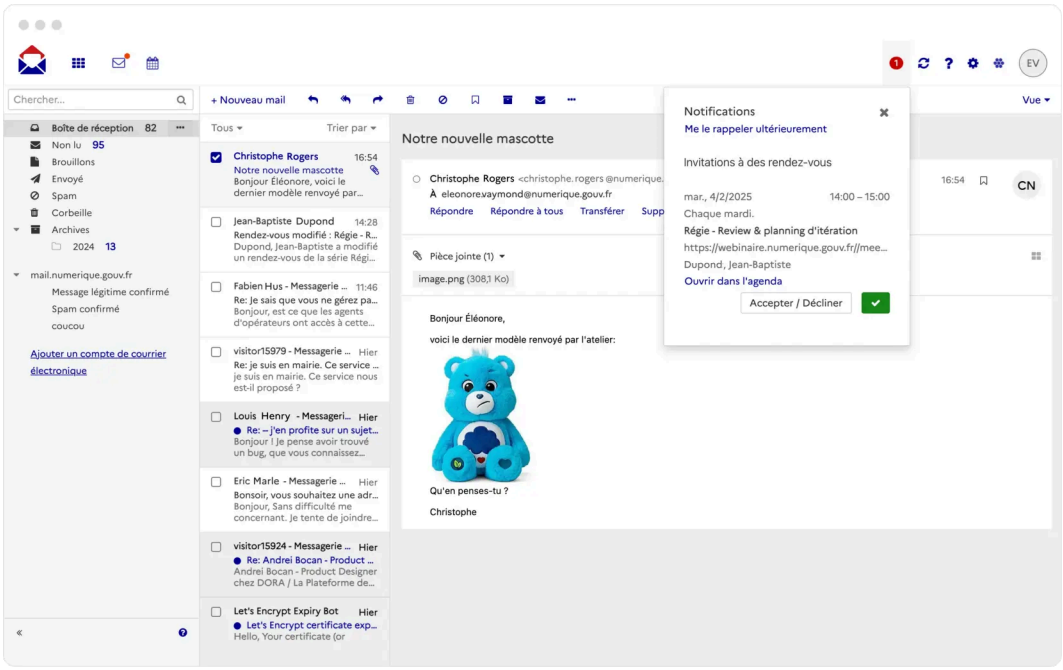
La suite numérique

Le gouvernement français a encadré le développement d'une suite collaborative libre. En 2025, elle est composée de :

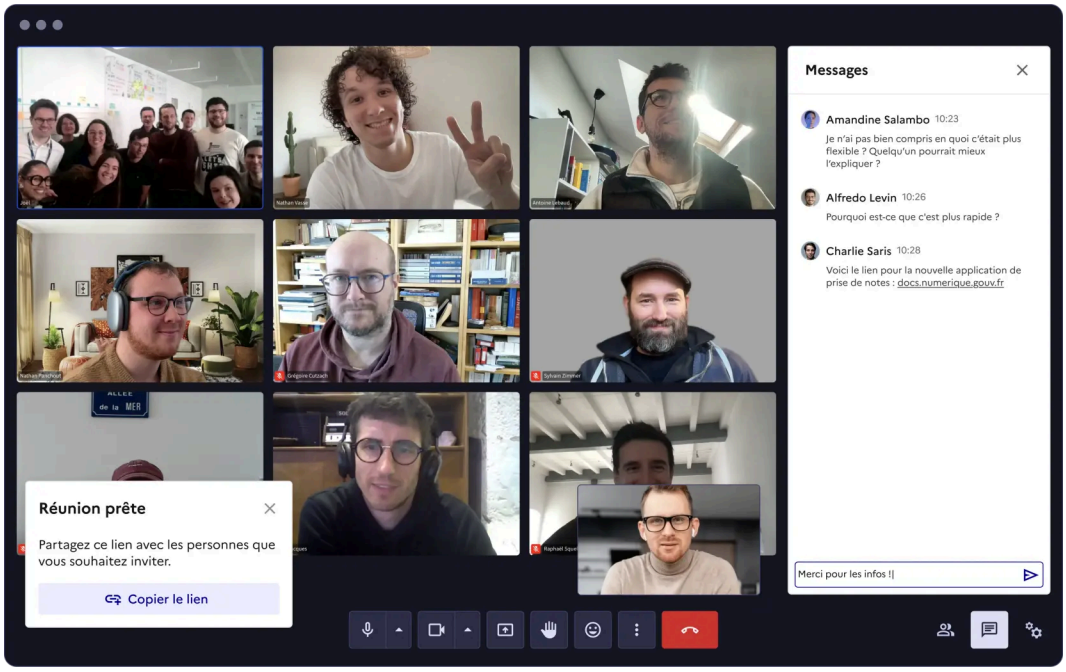
- Messagerie chiffrée de bout en bout (à la Slack) ;
- Transfert de fichiers (à la WeTransfer) ;
- Tableur collaboratif (à la Sheets) ;
- Éditeur collaboratifs (à la Docs) ;
- Visioconférence (à la Zoom) ;
- Messagerie mail (à la Gmail).

Une esthétique conforme aux standards industriels Remarque

La suite, bien que composée de logiciels séparés, adopte une charte graphique cohérente et une interface « moderne ». Les grands moyens sont déployés pour imiter les outils existants, ce qui constitue à la fois un avantage pour les personnes qui ne sont pas prêtes à changer leurs habitudes, et un inconvénient du point de vue des infrastructures nécessaires.



Interface de Messagerie, l'application de gestion de mails des agents de l'État français



Interface de Visio, l'application de visioconférence des agents de l'État français

CHATONS

Remarque

Les outils de la suite numérique peuvent être appropriés par des chatons ou apparentés, car ce sont des logiciels libres.

III Réparer nos imaginaires

1. Introduction

Les récits socio-techniques dominants ont façonné, colonisé nos imaginaires de sorte qu'il est souvent très difficile de penser hors de ce cadre. Pourtant, si le capitalisme de surveillance représente un modèle à dépasser, il est indispensable d'imaginer un autre futur sans utiliser ses outils techniques et rhétoriques. Cette section présente quelques pistes.

2. L'émancipation dans un monde capitaliste

Réparer les règles, c'est légitimer le système — Fondamental

> « Dénoncer les pratiques des entreprises ou pointer les manquements des réglementations revient en réalité à une forme d'acceptation, tout comme celle qui nous a fait accepter le capitalisme parce qu'il a créé le consumérisme et que les réglementations n'ont jamais eu d'autre effet que de tenter de freiner ses excès, uniquement.
>
> *Masutti, 2020*[Masutti, 2020], p. 406 »

Capitalisme et automatisation : suite ou fin ? — Remarque

Pour Bernard Stiegler, l'économie capitaliste est le fruit d'un mouvement d'automatisation, qui a d'abord permis de gagner en productivité et de redistribuer une partie des gains pour stimuler la consommation, d'où est né le consumérisme.

L'automatisation a des effets concrets (*prolétarisation*) : les savoirs-faire incorporés se perdent dans les machines et se réduisent à des automatismes.

L'automatisation s'accélère aujourd'hui, en particulier avec l'explosion des systèmes à base de *machine learning* : le secteur tertiaire est lui aussi touché.

L'automatisation ne s'arrête pas au travail : le marketing, via les pratiques de surveillance, tend à déterminer de plus en plus les choix des consommateurs, les privant ainsi de liberté.

Stiegler spécule qu'à un moment (reste à savoir lequel...), l'automatisation aura atteint de telles limites qu'elle ne permettra plus de redistribution : le capitalisme s'effondrera.

Il n'y a pas de frontière entre dedans et dehors — Attention

Ce qui est difficile, c'est que les choses ne sont pas binaires. Stiegler semble suggérer que le consumérisme et les technologies du capitalisme annihilent la production de connaissances et le libre-arbitre. Pourtant, même sur Facebook on voit des mouvements s'organiser, réfléchir et produire des connaissances. C'est précisément ce que suggérait Fogg en parlant de captologie : « ma mère peut créer un groupe sur Facebook et influencer des centaines, des milliers, voire des millions de personnes » (*Fogg, 2012*[Fogg, 2012]).

L'utopie est déjà là

Remarque

La gestion communautaire et auto-organisée de ressources (eau, terres, logiciel, encyclopédie...) n'est pas nouvelle. Elinor Ostrom, prix Nobel d'économie en 2009, montre avec des exemples s'étendant sur plus de mille ans comment des individus parviennent à s'auto-organiser pour gérer des Communs, hors des solutions préconisées par la science économique de l'époque (l'état fort ou la privatisation). Elle donne tort à une longue lignée de philosophes et d'économistes (voir « tragédie des communs ») (*Ostrom, 1990*[Ostrom, 1990]).

Prérequis techniques

Méthode

Masutti propose trois conditions pour limiter radicalement les pratiques du capitalisme de surveillance :

- Chiffrement de bout en bout ;
- Neutralité du net ;
- Fédération généralisés.

« Code is law »

Fondamental

> Les institutions publiques s'adaptent là où les pratiques le mènent, *par la force des choses*. Le refus, lui, ne peut-être qu'idéologique.
>
> *Masutti, 2020*[Masutti, 2020], p. 422

> Dans une lutte contre le capitalisme de surveillance, il ne peut y avoir de salut dans la revendication individuelle mais dans la construction d'alternatives de réappropriation collectives des connaissances, des technologies et, plus généralement, des communs, fondées sur le partage et la solidarité. Autrement dit, la lutte contre le capitalisme de surveillance ne peut être décrorrélée d'une lutte économique et sociale.
>
> *Masutti, 2020*[Masutti, 2020], p. 435

Incarner, c'est la meilleure manière de transmettre

Fondamental

Les alternatives les plus transformatrices sont celles structurées autour de collectifs dont le fonctionnement interne représente un imaginaire désirable. La sociologue Marianne Maeckelbergh parle de *préfiguration*. Avec les mots du géographe Simon Springer, dans un article à charge contre le néolibéralisme :

> Préfigurer, c'est rejeter le centrisme, la hiérarchie et l'autorité associés à la politique représentative, en soulignant la pratique incarnée des relations horizontales et des formes organisationnelles qui s'efforcent de refléter la société future que nous recherchons. [...] Préfigurer c'est embrasser la convivialité et la joie qui émanent d'être rassemblés comme égaux radicaux ; non pas comme des soldats au front ni comme le prolétariat sur la voie de la promesse transcendantale et vide de l'utopie ou du « non lieu », mais comme

l'immanence enracinée de l'ici et maintenant, de la fabrique d'un nouveau monde « dans la coquille du vieux », du travail constant et de la réaffirmation que tout cela implique.

Springer, 2016[Springer, 2016]

3. L'émancipation dans un monde post-capitaliste

3.1. Introduction

Le capitalisme industriel est probablement une parenthèse de l'Histoire

Rappel

Le numérique a un impact sur les ressources, la biodiversité et les écosystèmes (voir *Mesures d'impacts environementaux : les PEF* (cf. p.53)). Plus généralement, la croissance ne peut vraisemblablement pas durer (voir *Mécanismes et limites de la croissance exponentielle* (cf. p.54)). En d'autres termes, que nous le souhaitions ou non, un autre modèle s'imposera.

Décoloniser les imaginaires

Méthode

La critique du capitalisme, a fortiori de surveillance, est un processus *négatif*. Pour construire des alternatives (*positif*), il faut être capable d'imaginer des futurs souhaitables, ou de « décoloniser les imaginaires » (*Latouche, 2011*[Latouche, 2011]). Plusieurs approches sont possibles :

- Étudier l'histoire et l'anthropologie, pour déconstruire les récits dominants et prendre connaissance d'autres modèles ayant existé ;
- Transformer son rapport au monde (au temps, au vivant, aux liens sociaux, au travail) ;
- Lire des fictions proposant des dynamiques (sociales, économiques, politiques...) radicalement différentes.

3.2. Récits dominants et imaginaires

Les mythes structurent le réel

Fondamental

Notre société repose sur un ensemble de mythes fondateurs, largement acceptés, qui naturalisent des constructions sociales alors considérées comme indéboulonnables.

> Maurice Gaudelier, qui a côtoyé les Baruya de Nouvelle-Guinée, montre ainsi que leurs mythes fondateurs font apparaître les enjeux associés au pouvoir : pouvoir de gouverner les personnes, de contrôler l'accès aux dieux et aux moyens de destruction (armes), de productions (outils), d'échange (monnaie, biens précieux) et aux conditions de subsistance. La mythologie façonne le social et donne une cohésion à un univers qui peut sembler, aux yeux d'un observateur extérieur, profondément irrationnel.

Carnino, 2015[Carnino, 2015], p. 258

Mythbusters

Exemple

Dans un ouvrage faisant la synthèse des travaux en archéologie et en anthropologie, Graeber et Wengrow montrent que la plupart des mythes fondateurs de notre civilisation sont erronés.

> Il est désormais acquis que les sociétés humaines préagricoles ne se résumaient pas à de petits clans égalitaires. Au contraire, le monde des chasseurs-cueilleurs avant l'apparition de l'agriculture était un monde d'expérimentations sociales audacieuses, beaucoup plus proche d'un carnaval des formes politiques que des mornes abstractions suggérées par la théorie évolutionniste. L'agriculture, elle, n'a pas entraîné l'avènement de la propriété privée, pas plus qu'elle n'a marqué une étape irréversible dans la marche vers l'inégalité. En réalité, dans bien des communautés où l'on commençait à cultiver la terre, les hiérarchies sociales étaient pour ainsi dire inexistantes. Quant aux toutes premières villes, loin d'avoir gravé dans le marbre les différences de classe, elles étaient étonnamment nombreuses à fonctionner selon des principes résolument égalitaires, sans faire appel à de quelconques despotes, politiciens-guerriers bourrés d'ambition ou même petits chefs autoritaires.
>
> *Graeber et Wengrow, 2021*[Graeber et Wengrow, 2021]

Revenir au troc

Exemple

> [L'histoire de la monnaie] est devenue, aux yeux de la plupart des gens, du simple bon sens. Nous l'enseignons aux enfants dans les manuels scolaires et les musées. Tout le monde la connaît. « Autrefois, on faisait du troc. C'était difficile. Donc on a inventé la monnaie. Et plus tard il y a eu le développement de la banque et du crédit. » Tout cela constitue une progression parfaitement simple et directe, un processus d'affinement et d'abstraction croissants qui a porté l'humanité, logiquement et inexorablement, du troc préhistorique des défenses de mammouth aux marchés boursiers, fonds spéculatifs et dérivés titrisés. [Pourtant], « aucun exemple d'économie de troc n'a jamais été décrit, sans parler d'en faire émerger la monnaie ; toute la recherche ethnographique existante suggère qu'il n'y en a jamais eu ».
>
> *Graeber, 2013*[Graeber, 2013]

Science, progrès, félicité

Exemple

Carnino montre que l'apparition de « la » science est contemporaine et ne s'inscrit pas du tout dans l'histoire linéaire d'un progrès technique continu et abstrait visant à résoudre les problèmes de l'humanité.

> À la lueur des avancées récentes de l'histoire sociale et culturelle des sciences, il n'est aujourd'hui guère possible de continuer à penser la science comme un univers étanche et clos, qui flotterait au-dessus ou au-delà du social. Non seulement la science n'apparaît jamais concrètement comme une pure entremise

de connaissances qui serait parfois infléchie ou détournée par des biais extérieurs, mais même la science la plus « pure », celle qui trône au panthéon du savoir rationnel, alimente ses réflexions grâce à la religion, l'industrie, la politique, l'économie et la technique (p. 11) »

La figure de l'inventeur martyre se popularise. Dans « L'inventeur » (1867), le journaliste et économiste Yves Guyot écrit :

« L'invention détruira l'effort et donnera la satisfaction ; les intérêts opposés deviendront harmoniques ; à l'utilité onéreuse succédera l'utilité gratuite. C'est la machine qui détruira l'esclavage, ce sera elle qui détruira le prolétariat. Là est la loi du progrès. (p. 217) »

À la fin de ce processus de naturalisation, « toute résistance apparaît désormais comme une crispation futile engendrée par l'aveuglement obscurantiste de privilégiés jaloux de leurs prérogatives » (p. 220).

La « science » - pour autant que l'on ait correctement défini le terme - est tellement puissante qu'elle est exclue du débat public et constitue la fin de l'Histoire.

« Ainsi, l'industrialisation du monde, fondée par et sur la science, se trouve désormais exclue, en droit, des choix démocratiques. Découlant par principe du progrès des connaissances humaines, l'industrie est naturalisée au point d'être soustraite à la discussion politique (p. 261) »

« Véritable clef de voûte et pierre d'angle, la science - dont les définitions, nécessairement floues, varient - constitue dès lors l'horizon terminal de l'univers contemporain ; la divinité donnait un sens à la finitude de l'existence et du monde ; la science garantit désormais la cohérence du progrès perpétuel et de l'univers infini - et engendre l'illusion d'une croissance *illimitée* possible et souhaitable (p. 264) »

3.3. Rapports au monde

En finir avec l'opposition entre humains et nature

Exemple

« L'Occident moderne possède en conséquence un héritage *dualiste*, une manière de penser le monde en termes binaires, opposés, exclusifs et hiérarchisés : les « humains » et la « nature ». [...] Comment alors dire qui nous sommes, pour repenser notre relation au monde ? Voici la carte d'identité que je propose : nous sommes des vivants parmi les vivants, façonnés et irrigués de vie chaque jour par les dynamiques du vivant. [...] Nous ne sommes plus une espèce solitaire confrontée au reste du monde empaqueté en « nature » : nous ne sommes plus face à face, mais côte à côte avec le reste du vivant, face au dérobement de notre monde commun. [...] il s'agit de retrouver confiance dans les puissances du vivant : ses puissances de régénération et de résilience, sa capacité à *faire* notre monde. Retrouver confiance dans le fait que nous ne sommes pas *seuls* à veiller à l'habitabilité de ce monde. [...] Le message secret des sciences écologiques tient à cet égard en une phrase : l'habitat de chaque vivant n'est jamais un décor inanimé, c'est le tissage des autres habitants. Il n'y a pas de monde physique sur lequel nous habitons : nous vivons dans la respiration des végétaux, dans la pollinisation des abeilles, comme les grenouilles asiatiques habitent dans les empreintes-mondes laissées par les éléphants.

Morizot, 2020[Morizot, 2020]

Une connaissance incarnée qui relie

Exemple

« L'un des grands enjeux d'une culture du vivant est ainsi, à mon sens, de mettre en lumière, et d'inventer des *formes de connaissances qui relient*. [...] Cette manière de connaître a été en réalité incroyablement mise en oeuvre au XIXe siècle, en Angleterre et aux États-Unis, par une lignée de femmes écrivaines et naturalistes. [...] Autodidactes, n'ayant pas le droit de cité dans l'académie, étudiant ainsi le vivant chaque jour depuis chez elles, dans les jardins ou les alentours, ces femmes ont inventé un style d'attention au vivant particulièrement singulier : un style d'attention non moderne, où la connaissance du vivant a pour ambition explicite de faire entrer en relation avec lui. [...] Ne pas connaître le nom des plantes autour de nous, c'est s'exposer à éprouver ce même sentiment de n'être pas à sa place, de ne pas appartenir, d'avoir le sentiment d'être seul alors même que l'on est entouré. L'origine du sentiment de solitude cosmique des Modernes n'est peut-être pas une lucidité métaphysique supérieure [...] : c'est simplement qu'on hérite d'une socialisation culturelle telle qu'on ne connaît personne à la fête du vivant.

Zhong, 2020[Zhong, 2020]

3.4. La fiction comme antidote

Utopie

Az Définition

« Mot forgé par l'écrivain anglais Thomas More[26], titre de son livre *L'Utopie*[27], du grec οὐ-τόπος / *ou-tópos*, « en aucun lieu ». Représentation d'une société idéale, opposée aux sociétés réelles imparfaites.

Wikipédia[28]

Eutopie

Az Définition

Littéralement « lieu du bon ». Relativement ignoré ou confondu jusqu'alors, le mot gagne une signification particulière depuis les années 1960.

« Je propose de voir dans l'eutopie un « virtuel positif possible », c'est-à-dire une construction utopique « réaliste », mimétique, qui donne la sensation de vraisemblance et de plausibilité, et dans l'utopie (dans le sens restreint) un « virtuel positif impossible », une construction utopique « fantastique », métaphysique, qui fait le saut dans l'incroyable, dans l'extraordinaire.

Braga, 2006[Braga, 2006]

26. https://fr.wikipedia.org/wiki/Thomas_More
27. https://fr.wikipedia.org/wiki/L%27Utopie
28. https://fr.wikipedia.org/wiki/Utopie

Solarpunk

Az Définition

« Le solarpunk propose une vision optimiste d'un avenir durable, interconnecté avec la nature et la communauté, à la lumière des préoccupations des luttes intersectionnelles du début du XXIe siècle, non seulement au sujet de l'environnement, à l'égard du changement climatique et de la pollution, mais aussi des inégalités sociales et des intolérances et discriminations sociales (de genre, sexistes ou ethniques).

Wikipédia[29] »

Héritage

Fondamental

Pour éviter de retomber dans l'utopie, il faut se préoccuper de l'héritage d'un capitalisme industriel destructeur arrêté juste à temps.

« 11. Our future must involve repurposing and creating new things from what we already have. Imagine “smart cities” being junked in favor of smart citizenry.

13. Solarpunk wants to counter the scenarios of a dying earth, an insuperable gap between rich and poor, and a society controlled by corporations. Not in hundreds of years, but within reach.

21. In Solarpunk we’ve pulled back just in time to stop the slow destruction of our planet.

Manifeste Solarpunk[*Manifeste Solarpunk*] »

Voir *Communs négatifs et externalités négatives* (cf. p.63).

2060

Exemple

L'extrait qui suit embrasse particulièrement le manifeste Solarpunk.

Lou protagoniste vit à l'Amourereraie et a entrepris un long voyage à vélo avant la Torpeur, sorte de mega-mega-caninule annuelle. Él retrouve son adelphe. La narration est à la deuxième personne, contée par ses *covives* de l'Amoureraie.

« Tu retrouves l'adelphe dans une casa de la grande ville, appartement dans un îlot d'immeubles, du XXe réaménagé du temps de Solar City puis retapé dans le style Parasol (générant cet étrange - mais harmonieux - mélange de bioplas et de bois flotté). La terrasse ouvre, au loin, vers la ligne de mer, lumineuse et floue, où des vents humides, des cris de mouettes planent dans un ciel immobile au-dessus des routes devenues plages et des maisons devenues sable. L'adelphe te reçoit avec les bras ouverts sur les années passées, nombreuses déjà. L'Amourereraie n'est pas loin pourtant, mais... monter un chameau, prendre le train, le cycle... jusqu'à chez nous, c'est un voyage déjà ; et chacun, et chacune... tisser un couple, prendre soin de l'enfant, puis de la deuxième. Et él̀s vivent en trèfle désormais : deux parentz et deux marmailles. Plus la casa, les permanences au dépôt, l'atelier deux fois par semaine, et puis le syndic de l'immeuble, du quartier, et même un tirage pour participer à l'assemblée de l'Alimentaire, l'année passée... de quoi remplir une bonne vie, tranquile, él̀ te raconte à l'ombre de sa vigne (en train de

29. https://fr.wikipedia.org/wiki/Solarpunk

> crever, mais personne n'y peut rien, plus d'eau, trop de soleil... le syndic a envoyé chercher des plants plus résistants, cultivés sur l'autre rive). [...] L'adelphe te dit que l'ancienne autoroute vers l'est est impraticable : les relations avec les communautés de là-bas se sont trop dégradées, trop de mépris filé par les ans... Des « contributions aux travaux » ont été prélevées auprès de pêcheurz et voyageurz.
>
> Tu t'inquiètes : « Prélevées par qui ? Par des couzâmes ? » L'adelphe fait la moue.
>
> Je n'ai pas trouvé beaucoup d'infos sur le Reslove, je crois qu'un article est en cours de rédaction, mais pour l'instant j'ai entendu tout et son contraire. On veut croire que ce sont les Vertis [hiérarchistes], mais... à force d'être en friction et d'accueillir la Défense, ç'aura peut-être dégénéré de notre côté ? Les zones frontières fatiguent toujours, tu imagines, devoir surveiller tes stocks, tes champs, fermer tes portes, faire la douane tout le temps, vivre avec des armes...
>
> *Possoz, 2025*[Possoz, 2025] (p. 68-70)

Bibliographie Exemple

- Ateliers de l'Antémonde, éd. Bâtir aussi. Sorcières. Paris: Cambourakis, 2019.
- Chambers, Becky. L'espace d'un an. La dentelle du cygne. Nantes: l'Atalante, 2016.
- Chambers, Becky. Un psaume pour les recyclés sauvages. La Dentelle du Cygne. Nantes: l'Atalante, 2022.
- Collectif. Les Utopiennes, des nouvelles de 2043. La mer salée., 2023.
- Le Guin, Ursula K. Les Dépossédés. Le Livre de Poche, 2006.
- Possoz, Elio. Les mains vides. La Volte, 2025.
- Morel Darleux, Corinne. Alors nous irons trouver la beauté ailleurs. Libertalia., 2023.

a) Récits dominants

b) Rapports aux monde

c) Fictions

Contenus annexes

1. Découverte du chiffrement

(cf.)

Objectifs

- Découvrir la notion de chiffrement ;
- Connaître un algorithme basique de chiffrement.

Mise en situation

Lorsqu'on échange des messages sur Internet, c'est un peu comme si on communiquait avec des cartes postales. C'est à dire qu'il est très facile pour un intermédiaire de les lire. Les messages ne sont pas confidentiels.

La seule façon de communiquer de façon confidentielle est de **chiffrer** les messages. Cela consiste à définir un code secret que seuls les deux correspondants connaissent. Ainsi les messages sont toujours lisibles par des tiers, mais il ne sont plus en mesure de comprendre quoi que ce soit. C'est comme si sur ma carte postale j'écrivais : DZMIY Z YPO. On peut toujours la lire, mais sans le code il est difficile de comprendre le message. Si je vous donne le code, alors vous serez en mesure de le **déchiffrer** c'est à dire de l'appliquer pour retrouver le message original. Mais comme un code de chiffrement doit rester secret, je ne le donne pas dans une vidéo.

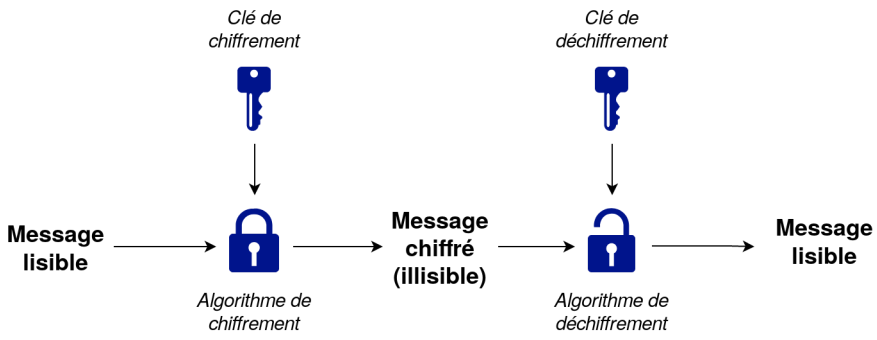
Le code que j'ai utilisé ici est très simple, il sera facilement décrypté. **Décrypter** un code signifie parvenir à en trouver la teneur originale sans en avoir été informé. Je vous laisse décrypter mon message.

Processus de transmission d'un message chiffré

Fondamental

La transmission d'un message chiffré se fera en trois étapes :

1. Chiffrement du message à l'aide d'un algorithme de chiffrement auquel on fournit une clé de chiffrement.
2. Transmission du message chiffré.
3. Déchiffrement à l'aide d'un algorithme de chiffrement auquel on fournit une clé de déchiffrement.



Fondamental

Le chiffrement est un procédé cryptographique permettant de coder un message de telle façon que sa lecture ne soit possible que par le seul possesseur de la clé de déchiffrement

Remarque

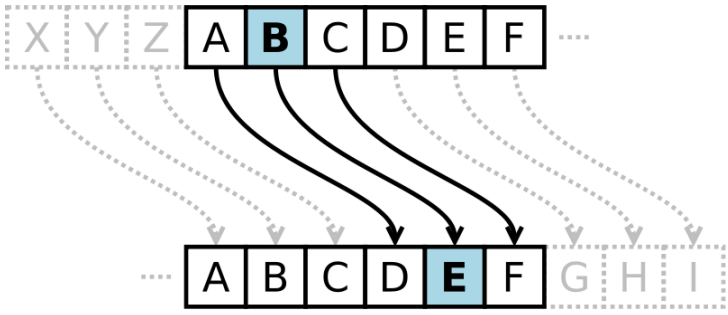
- les **algorithmes de chiffrement/déchiffrement** : ces algorithmes sont le plus souvent disponibles librement.
- les **clés** : elles sont un ensemble de paramètres à fournir à l'algorithme afin qu'il puisse réaliser sa tâche. Pour garantir la confidentialité du message, la clé de déchiffrement doit être privée.
- l'**unicité de la paire de clés** : pour une clé de chiffrement il n'existe qu'une clé permettant de déchiffrer et l'inverse est également vrai (aucun intermédiaire ne peut deviner cette clé).

Le chiffre de César

Exemple

Aussi appelé chiffrement par décalage, ce chiffrement très simple consiste à décaler toutes les lettres d'un message. Dans ce cas, les clés de chiffrement et de déchiffrement sont identiques et correspondent à l'amplitude du décalage.

Par exemple pour un décalage de 2, les « A » deviendront des « C », les « B » deviendront des « D », etc. Le mot « shannon » donnera « vkdqqrq » avec un décalage de 3.



Chiffre de César

Chiffrer, pas crypter

Complément

La mot crypter n'existe pas en français. Un message est donc chiffré mais pas crypté.

Néanmoins, on peut parler de « décryptage » lorsque l'on cherche à déchiffrer un message sans disposer de la clé nécessaire.

Sécurité du chiffrement

⊕ Complément

Le problème du chiffrement par décalage est son manque de sécurité. Il est très simple de trouver la clé de déchiffrement par essais successifs.

La sécurité de ces algorithmes doit reposer sur des propriétés mathématiques fortes et/ou sur une bonne transformation de l'information.

Baser la sécurisé du chiffrement sur le fait que son procédé soit inconnu par un tiers revient à faire de la **sécurité par l'obscurité**. Cacher un procédé protège beaucoup moins que d'utiliser un procédé de chiffrement public et solide.

Hachage cryptographique et condensat

⊕ Complément

Le **hachage cryptographique** est le second procédé cryptographique très utilisé. Il permet de produire des **condensats** (aussi appelé empreinte numérique). Un condensat est une chaîne de caractères **unique** de taille fixe pour chaque donnée pouvant exister. Ainsi, deux messages différents (même d'un caractère) auront un condensat différent.

Il n'est pas possible d'inverser le processus et de passer d'un condensat au message d'origine (ceci l'oppose au chiffrement). Les algorithmes classiques sont : SHA256, SHA1, MD5, etc.

À retenir

- Le chiffrement permet de transformer un message afin qu'il ne soit lisible que par une personne possédant la clé de déchiffrement.
- La sécurité d'un chiffrement repose sur de bonnes propriétés mathématiques et sur de bonnes opérations de transformation de l'information.

(cf.)

2. Chiffrement symétrique

(cf.)

Objectifs

- Découvrir le chiffrement symétrique ;
- Utiliser un algorithme de chiffrement symétrique.

Mise en situation

Lorsque deux personnes qui communiquent entre elles partagent exactement la même technique de chiffrement, on parle de chiffrement symétrique. C'est en général une méthode insuffisante pour les communications entre plusieurs personnes. Il est possible d'utiliser une clé symétrique pour communiquer avec quelqu'un, mais dans ce cas la clé sera changée à chaque nouvelle communication.

Le chiffrement symétrique est aussi utilisé lorsque l'on souhaite chiffrer des données sans les partager. C'est le cas lorsque l'on chiffre son disque dur pour que, même en cas de vol, seul le propriétaire puisse accéder aux données. Ainsi, le but n'est plus de sécuriser une communication mais le stockage lui-même.

Le chiffrement symétrique

Az Définition

Le chiffrement symétrique est un chiffrement dans lequel la clé de chiffrement sert également à déchiffrer. On parle alors de clé secrète.

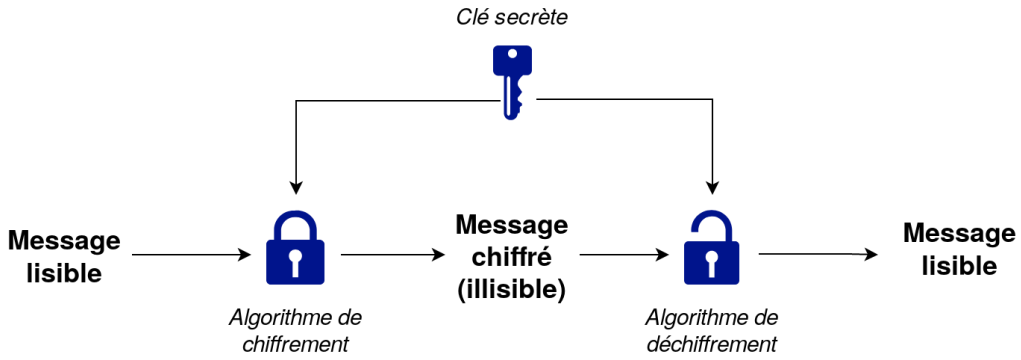


Schéma d'utilisation classique

Exemple

Bob souhaite chiffrer son disque dur pour qu'il soit le seul à pouvoir accéder à ses fichiers.

1. Lors de l'installation de son système d'exploitation Bob décide de chiffrer son disque dur, il choisit un mot de passe P.
2. La totalité du disque est chiffré avec une clé K générée par le système, cette clé est stockée sur le disque dur.
3. La clé K est à son tour chiffrée grâce au mot de passe P (elle ne doit pas être accessible en clair sur le disque).
4. À chaque déverrouillage de son ordinateur Bob entre le mot de passe qui permet de déchiffrer la clé K ; elle est alors chargée en mémoire afin d'être disponible rapidement.
5. À chaque fois qu'un fichier est accédé en lecture il est déchiffré avec K ; à chaque accès en écriture il est chiffré avec K.

Ainsi, Bob est certain que tant que son mot de passe reste secret, ses données sont sécurisées même si quelqu'un accède au disque de son ordinateur.

Le partage de clés

⚠ Attention

Il arrive parfois que la clé soit connue par plusieurs personnes ou soit présente sur plusieurs serveurs du propriétaire.

Le transfert de la clé doit absolument être sécurisé pour que le chiffrement ne soit pas compromis.

Plusieurs stratégies existent et une des plus efficaces est d'utiliser un autre type de chiffrement pour chiffrer la clé secrète et d'envoyer ce message au destinataire qui pourra récupérer la clé secrète en toute sécurité. Transférer la clé au travers d'une connexion SSH est une stratégie commune.

Le chiffrement AES

Az Définition

L'*Advanced Encryption System* est un standard très répandu pour réaliser du chiffrement symétrique. Il possède énormément de bonnes propriétés : facile à calculer, implémentation possible au niveau logiciel comme au niveau matériel (implémentation câblée). Ce type de chiffrement est utilisé notamment pour des protocoles tels que SSL (sécurisant les connexions HTTP) ou encore pour chiffrer son disque dur (VeraCrypt[30]).

Générer sa propre clé secrète

Méthode

Voici une commande basique pour générer une clé secrète. Il existe des implémentations plus complexes et sécurisées. Ici, la clé est simplement une suite aléatoire de 32 octets. Pour une utilisation réelle, il est conseillé d'utiliser des implémentations robustes et de confiance pour générer sa clé secrète.

```
1 openssl rand 32 > cle_secrete.pem
```

On obtient ici la clé de chiffrement dans le fichier `cle_secrete.pem`.

Utiliser une phrase secrète ou un mot de passe

Conseil

Il est possible de sécuriser sa clé secrète en spécifiant un mot de passe lors de la génération de la clé. Une telle pratique permet de conserver la sécurité même si un attaquant réussit à récupérer la clé. Il est tout de même fortement conseillé de générer une nouvelle clé dès lors qu'une clé est compromise.

Chiffrer et déchiffrer

Méthode

On peut utiliser les commandes dans un repl Bash ou un terminal, pour chiffrer et déchiffrer un message.

Pour chiffrer un fichier `msg.txt` en un nouveau fichier `msg.txt.enc` avec AES et une clé secrète générée `cle_secrete.pem` on utilise :

```
1 openssl aes-256-cbc -pbkdf2 -iter 100000 -in msg.txt -out msg.txt.enc -pass
  file:cle_secrete.pem
```

Pour déchiffrer un fichier `msg.txt.enc` chiffré avec AES en un fichier `msg.txt` et une clé secrète générée `cle_secrete.pem` on utilise :

```
1 openssl aes-256-cbc -pbkdf2 -iter 100000 -d -in msg.txt.enc -out msg.txt -pass
  file:cle_secrete.pem
```

À retenir

- Le chiffrement symétrique permet de sécuriser ses propres données avec une unique clé.
- Le chiffrement symétrique permet d'échanger des données avec des pairs s'ils disposent eux aussi de la clé.
- Le partage de clé est très complexe et doit rester exceptionnel pour conserver sa confidentialité.

30. https://fr.wikipedia.org/wiki/VeraCrypt

- L'algorithme AES permet de réaliser un chiffrement symétrique.

(cf.)

3. Chiffrement asymétrique

(cf.)

Objectifs

- Découvrir le chiffrement asymétrique ;
- Utiliser un algorithme de chiffrement asymétrique.

Mise en situation

L'inconvénient du chiffrement symétrique est que si trois personnes souhaitent communiquer entre elles deux par deux, et bien le troisième pourra toujours espionner les deux autres, puisque le code est commun. On pourrait imaginer que chaque couple de personnes possède une clé spécifique, mais si 1000 personnes échangent entre elles, cela fera pour chacune, 999 clés à gérer. On voit bien que cela n'est pas satisfaisant pour les communications sur Internet.

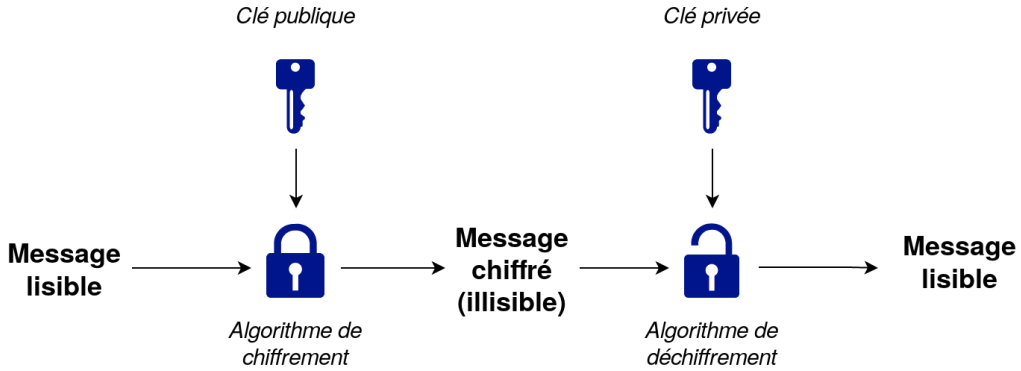
La solution est fournie par le chiffrement asymétrique. Celui-ci est basé sur les propriétés mathématiques d'une paire de clés : la première est publique, elle est communiquée au monde entier et elle sert à chiffrer les messages. La seconde est privée, elle n'est communiquée à personne et elle sert à déchiffrer les messages. Ainsi si quelqu'un souhaite m'envoyer un message, il peut le chiffrer avec ma clé publique, seul moi pourrai le lire car je suis le seul à disposer de la clé privée.

On peut voir cela comme des milliers de boites inviolables que je diffuserais dans le monde entier. N'importe qui peut prendre une de mes boîtes et glisser un message dedans. Je suis le seul à en posséder la clé, donc seul moi pourrai accéder au message.

Le chiffrement asymétrique

Az Définition

Le **chiffrement asymétrique** vient concrétiser la différence entre la clé de chiffrement et de déchiffrement. En pratique, la clé de chiffrement sera nommée **clé publique** car elle sera librement communiquée. La clé de déchiffrement sera nommée **clé privée** car elle ne doit être communiquée sous aucun prétexte.



Fondamental

- N'importe qui pourra utiliser la clé publique d'une personne pour lui envoyer un message (cette clé publique est connue de tous).
- Ce message ne sera déchiffrable qu'avec la clé privée de cette même personne (qui n'est détenue que par elle-même).

Schéma d'utilisation classique

Exemple

Bob veut envoyer un message à Alice :

1. La clé publique d'Alice est disponible sur un site web.
2. Bob la récupère et chiffre son message grâce à cette clé.
3. Bob envoie le message chiffré à Alice.
4. Alice reçoit puis déchiffre le message grâce à sa clé privée.

Remarque

A l'issue de la communication, Alice et Bob sont certains que leur communication a été confidentielle... à moins qu'Alice n'ait pas correctement protégé la confidentialité de sa clé privée (à cause d'une erreur ou d'une attaque).

Chiffrement RSA

Exemple

Le chiffrement RSA est l'un des algorithmes les plus connus lorsque l'on parle de chiffrement asymétrique. Il est utilisé dans de nombreux contextes notamment :

- Par le protocole SSH, qui permet d'accéder à un serveur distant de manière sécurisée.
- Pour transmettre une clé de chiffrement symétrique. La clé de chiffrement symétrique doit rester confidentielle : elle est transmise à l'aide d'un chiffrement asymétrique lorsqu'elle doit être partagée à un tiers autorisé.

Générer ses propres clés

Méthode

Il existe plusieurs manières de générer des clés RSA. La plus simple est de générer des clés SSH qui sont déjà des clés RSA. Le plus souvent la paire de clés sont nommées de la manière suivante : `nom_clé.pub` pour la publique et `nom_clé` pour la privée. Il est commun de posséder plusieurs paires de clés. On préfère garder une nomenclature similaire pour le nom des clés pour ne pas les mélanger. Ces clés pourront être directement utilisées *pour accéder à un serveur distant.* *(cf. p.51)*

```
1 ssh-keygen
```

Pour la suite, on génère les clés RSA directement avec `openssl`.

```bash
# Génère une clé privée protégée par mot de passe dans le fichier private.pem
openssl genrsa -des3 -out private.pem 2048
# Extrait la clé publique de la clé privée dans le fichier public.pem
openssl rsa -in private.pem -outform PEM -pubout -out public.pem
```

Utiliser une phrase secrète ou un mot de passe

Conseil

Il est possible de sécuriser sa clé privée en spécifiant un mot de passe lors de la génération de la clé.

Ainsi, la clé privée est elle-même chiffrée par chiffrement symétrique.

Une telle pratique permet de conserver la sécurité même si un attaquant réussit à récupérer la clé privée. Il est tout de même fortement conseillé de générer une nouvelle clé si sa clé actuelle est compromise.

Paire de clés RSA

Exemple

Voici à quoi ressemble une clef privée RSA, protégée par mot de passe (**il ne faut jamais publier une telle clé si elle est en service).**

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,EB9CF5A7B25026DE

/nJK7OYp0kT26M3bDlTcO6RVAcoIBpZ8oA18p78Nl0mWOQPE0oZTaDJbTuEQLNNW
UWL7c+D7unGg+UdO7DWc52Z4M8JgoYhy7hvZ1BzFs4bUxJ+OP0sWWCyE9eWScK+4
vXXrEhp6JhUSx654cbyPtUYwVGdxKoq25TzEDvA5eSQU1MH/LviNErTYLtZcbPjw
vrbeOivbcSjcTzB83cdgeM/y+ourduIqWjwM1BkhgwcZ5gN6jdWPFMKGe9iF2gsy
IRvfAAjbzmJVM2DXEjHaSSRkXMIusdJN1lyEuH833XGBql9RmslQ9BzjUuYr1Fzd
A1n9EBvaY3pT8UPa3epFwO9kT7ag2Hrx7jYNtlUk/7kyPnm95cJWUvBvGrZxhCDD
4+lsCWrIRSslI5RnlgZQY/FgPOT2blesgkk2Ize/10PflM6w2fPfSsSMKYE9dEY8
zc3F+WwslxopQkWmRYZ8wwzv3Tng60/3DIU4X2oUPPajTFEjIk/KZ5tiHf6bSTcK
VQtE6w/bIHOyu/4ge7EfBDTZAuLGKqtfMuT8Dcz5behK/TgcLEq+4ps2KUu4f/rE
aGcI9sGSYmrRn18bRPATb+VkfKH8ak48zj43UBfrXhTRUlCx7FMDwfu9Csn5aEDl
dOANQ0sz51E6h3DDGHJU8Z0o5mQtFvcPyw/s2uc5ooTlfQr0e+36EQHSqfJIEVzO
Y1Cm2jq+bTPuI4yAp1rlEng3Z+jS3FIkP9lP8Iz7tyhvYWhGc0bK0gebGXO2uFOm
6X6eObQQkQ+sbdLQ7wCe3J4UmOEkq6wmvBlt5ZwH+Eo2icKC++434olMxCBKHAPH
2uXwNbZORhqP77Pl7dNge8bhZtdAqWG0Mb8DiGHYweSgC6m8h3xYAtQDdnWyDY4D
0qpLjI+mw+EVk8aMoNVTO3sDWuArsJVYOpoIfQ7/tnBhmJ1Rr9Axr8woDMA6Z501
7zvw4g4zYID61v5hl+xvAO+BUHwGIwuJ92gnSm4WOPk63GLiu0ita73IJgdL6FSG
bsrcmPOLa0+ATCU6CMRLJ3mzefJOviwThkC3P88Fy8kjSg3MTgnXASqqfEix8+Y2
eLtXJmWQXfhWdT24+f4EUEU5+YIy50qL8VGNdRgqKgclC6nUM1uW5txTEqs+fTjH
NhTr5s7gPMWbQYwPkcdNhPaxNhrykTFEfmKL6AEzx64sGn3/kzuqHv0/cH2jR3OR
sp6nd4iarbPYk9zKbUbiBMNvpjegbJ7WLcEllWHMApwfNTufJp0MHIk8AymjbZth
oTDvFZ6BThSW3kJMz31gBX18PswYBUs3bB7FTC3fXDxoSjHk3ClW4aclGIdbWAba
BJNTSieLL6TTlQ3cAD2bb3xJDnAuHScZ+tauu83YDTGfiUsQ4ew9alqypI+dbrPc
utSu9PVOb/8F+MZENW+DtLJ0IvZgcTj0diOqL5Cd1S4J+v/0s60XjyuTBDl1Yj8U
DID6IHFDm/qIfFcNfNzxTgag+nOwXFnn/d5S38YGHiokgXNCugeYw/HeekBP69tm
VjCq2YzIXnOepfYron5KaMt+4y1leXdJzNPHU+7FAr0w6k/IC4r+wg==
-----END RSA PRIVATE KEY-----
```

Voici une clef RSA publique : c'est celle que l'on partage avec des tiers pour des communications.

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAv/Lg6dBGCZKsuIHv/eJi
B2izeWybrH9HjVEwpMBfpS8Nh02hXNPaw547HXnsBC47yTCrNoDDKPBgIIJ0mLNE
R9XhiryK3ni7yo/lE3qE2YKE905a4ALrjejk9J+afnSAfmcfGkfLYl0n2mKo+hy7
xok4/sDLtv938Bbsyg/V1o+YeSucHIXe+b7S6dKR3fOwHw/TB3R+1Qu/nl/RIv7s
OnkRwBxs/NvO6Na+Xny3f0PxpWjjL+CCTePRYaZ/VrNI/Uym3vGGhLzDrlDPu8IB
0S8oF9xgQSHxUrHWNKJ6k0+Fjr5BzoUnrqy6ipC5A1vEEyYRc95ZyKI0vkAYRihI
ewIDAQAB
-----END PUBLIC KEY-----
```

Chiffrer et déchiffrer

Méthode

Pour chiffrer et déchiffrer un message, il est nécessaire d'utiliser les commandes ci-dessous.

Pour chiffrer un fichier :

```
1 openssl rsautl -encrypt -pubin -inkey public.pem -in msg.txt -out msg.enc
```

Pour chiffrer une chaîne de caractères :

```
1 echo "Message confidentiel" | openssl rsautl -encrypt -pubin -inkey public.pem -
  out msg.enc
```

Pour déchiffrer un message :

```
1 openssl rsautl -decrypt -inkey private.pem -in msg.enc -out message_en_clair.txt
```

Chiffrer avec la clé privée pour signer

Complément

Il est possible d'inverser le rôle des clés en chiffrant avec la clé privée et en déchiffrant avec la clé publique. Le but d'une telle pratique n'est pas de garder le message secret mais de vérifier l'identité de l'expéditeur. Seul le propriétaire de la clé privée peut générer un message déchiffrable avec la clé publique, ce qui garantit son identité.

À retenir

- Le chiffrement asymétrique permet un partage de la clé de chiffrement tout en garantissant la confidentialité de la clé de déchiffrement.
- La clé publique d'une personne est disponible par ceux qui veulent lui envoyer des messages.
- La clé privée d'une personne n'est jamais publiée et est utilisée par la personne pour déchiffrer les messages reçus.
- L'algorithme RSA permet de réaliser un chiffrement asymétrique.

(cf.)

4. Accès SSH aux serveurs

(cf.)

Objectif

- Établir une connexion sécurisée à son serveur.

Mise en situation

Pour développer et maintenir une application, il est nécessaire de se connecter au serveur qui l'héberge. Pour cela on utilise essentiellement le protocole SSH, ainsi que le programme éponyme.

SSH repose sur le chiffrement de la communication avec le serveur, pour éviter que quelqu'un n'espionne ou ne falsifie la communication, ce qui équivaudrait à prendre le contrôle du serveur.

Le bon usage de SSH repose sur la gestion de clés qui doivent rester secrètes pour que les accès aux serveurs ne soient pas compromis.

Protocole SSH

Rappel

Le protocole SSH permet une connexion sécurisée entre un serveur et un client SSH. Sur Linux, le client SSH est accessible nativement via la console de commandes (en utilisant la commande `ssh`). Sur Windows, il existe le client PuTTY[31].

Utiliser des mots de passe complexes

Il faut avoir un mot de passe très robuste car un attaquant pourrait nuire à l'application ou à ses données s'il réussissait à s'emparer du mot de passe.

Recours à des clés SSH

Conseil

Il est possible d'utiliser des paires de clés SSH. Une paire est composée d'une clé publique qui sera déposée sur le serveur et d'une clé privée conservée sur l'ordinateur personnel de l'utilisateur. Pour se connecter, l'utilisateur n'aura plus à entrer son mot de passe car sa clé privée lui permettra de s'authentifier.

Cela simplifie grandement l'accès au serveur et évite de devoir taper un mot de passe compliqué à chaque connexion.

```
ssh-keygen  # Crée la paire de clés SSH
ssh-copy-id user@127.0.0.1  # Place la clé publique sur le serveur distant
[Entrer mot de passe]
ssh user@127.0.0.1
[Pas de saisie de mot de passe]
```

Danger de l'utilisation des clés

Attention

Les clés SSH présentent un côté pratique et évitent d'avoir à retenir un mot de passe compliqué. Dans le cas où une machine personnelle est compromise, l'attaquant pourra récupérer la clé privée et l'utiliser pour accéder au serveur. Ainsi, il faudra veiller à la sécurité des ordinateurs personnels également.

Il est possible d'ajouter une phrase secrète à votre clé SSH qui empêchera un attaquant de l'utiliser. Cela ajoutera un mot de passe à retenir mais dans le cas où la clé publique est présente sur 50 serveurs, cela permet de retenir un seul mot de passe plutôt que 50.

31. https://www.putty.org/

Accès exclusif par clé aux serveurs Méthode

Il est en général conseillé de privilégier l'accès par clé à l'accès par mot de passe en SSH. Si tous les utilisateurs autorisés ont un accès par clé, il est conseillé de désactiver, au niveau du serveur SSH, tout accès par mot de passe, ce qui supprime un risque.

À retenir

- Le mot de passe pour accéder à un serveur mérite une grande attention.
- Le recours à des clés SSH peut simplifier l'accès.
- Les clés SSH présentent tout de même des dangers dont il faut être conscient.

Dangers liés à un serveur compromis Complément

Un utilisateur pourra considérer (par exemple en phase de développement) que son application ou ses données de test ne sont pas sensibles.

Néanmoins un attaquant pourrait prendre le contrôle du serveur et lancer des attaques sur des entreprises et des gouvernements. Dans ce cas de figure, la justice se tournera en premier lieu vers le propriétaire du serveur.

De nombreux robots essayent de se connecter aux serveurs SSH en testant divers noms d'utilisateurs et mots de passe, il est donc commun et pas du tout exceptionnel qu'un serveur soit compromis.

Il est donc conseillé de toujours protéger les accès à ses serveurs, même s'ils ne sont pas utilisés pour des projets sensibles (et même, en fait, s'il ne sont pas utilisés du tout).

(cf.)

5. *Mesures d'impacts environementaux : les PEF*

Facteurs d'impacts du PEF (Product Environmental Footprint)

- 16 facteurs (*PEF2021*[PEF2021])
- développés en 2013 par la commission européenne, version 3.1 publiée en 2022,
- présentés dans le PEFCR (PEF Category Rules) : norme européenne visant à homogénéiser les analyses de cycle de vie environnementales au niveau européen en proposant des critères communs, notamment une catégorisation des facteurs d'impact environnementaux,
- amalgames de facteurs mesurables provenant de plusieurs travaux scientifiques, centrés sur l'humain (par exemple, peu de prise en compte de la biodiversité).

Les 16 facteurs d'impact du PEF

1. climate change (kg $CO_{2\ eq}$) : impact sur le changement climatique
2. ozone depletion (kf CFC-11_{eq}) : impact sur la couche d'ozone
3. human toxicity, cancer (CTU_h) : impact toxique cancérigène sur les humains
4. human toxicity, non-cancer (CTU_h) : impact toxique non-cancérigène sur les humains
5. particulate matter (incidence de maladie) : impact de l'émission de particules fines sur les humains
6. ionising radiation (kBq $U^{235}{}_{eq}$) : impact de l'exposition aux radiation sur les humains

7. photochemical ozone formation (kg $NMVOC_{eq}$) : impact de la formation de smog sur les humains
8. acidification (mol H^+_{eq}) : impact de l'acidification des sols et des océans
9. eutrophication, terrestrial (mol N_{eq}) : impact de l'excédent d'azote dans les terres
10. eutrophication, freshwater (kg P_{eq}) : impact de l'excédent de phosphore dans les eaux douces
11. eutrophication, marine (kg N_{eq}) : impact de l'excédent d'azote dans les eaux marines
12. ecotoxicity, freshwater (CTU_e) : impact toxique sur les éco-systèmes des eaux douces
13. land use (plusieurs métriques) : impact sur la condition des terres (qualité du sol, production biotique, résistance à l'érosion, reaaprovisionnement des nappes phréatiques, capacité de filtrage)
14. water use (m^3 $world_{eq}$) : impact sur la diminution d'eau
15. resource use, mineral and metal (kg Sb_{eq}) : impact sur la diminution des ressources en minéraux et métaux (Sb = antimoine)
16. resource use, fossils (MJ) : impact sur la diminution des ressources fossiles

> 💬 Remarque
>
> CTU = Comparative Toxic Unit for human/ecosystems

Normalisation et factorisation : une introduction de subjectivité

Pour comparer les impacts entre eux, il faut utiliser des opérations de normalisation et pondération :

- La normalisation a pour objectif de transformer les mesures de chaque facteur dans des indices de même grandeurs. Pour les PEF, on ramène la mesure d'un facteur à l'impact moyen d'un être humain sur le facteur pendant une année (qui peut déjà être déraisonnable). Des valeurs moyennes sont données par la commission européenne dans *PEFCR2017*[PEFCR2017].
- La factorisation a pour objectif de pondérer les facteurs en fonction de leur importance relative. Pour les PEF, ce poids a été déterminé à la fois par des experts et le grand public, par un processus de questionnaire (expert/grand public) et de discussions (expert seulement), en tenant compte de la confiance (ou du manque de confiance) des experts sur cette importance (*JRC Weighting*[JRC Weighting]).

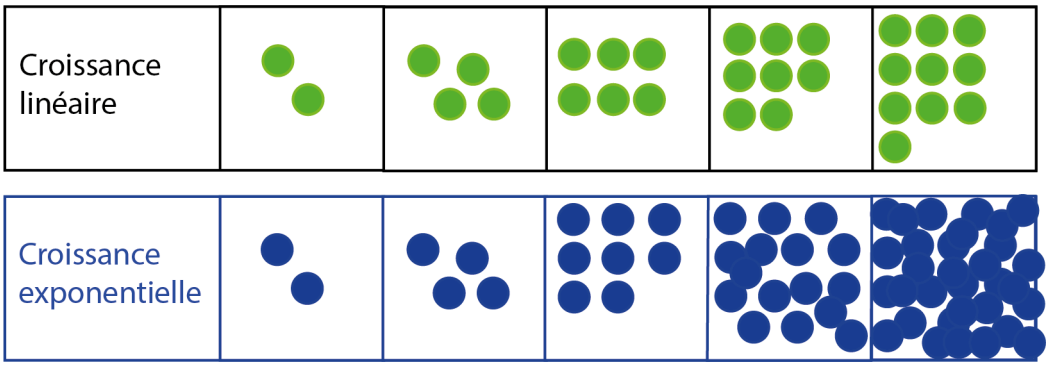
> ⚠ Attention
>
> Normalisation et factorisation rendent les mesures subjectives. Si elles ne sont pas nécessaires, mieux vaut ne pas les utiliser.

6. Mécanismes et limites de la croissance exponentielle

Toujours plus vite

C'est ainsi qu'on peut qualifier la croissance exponentielle. La croissance linéaire et la croissance exponentielle sont deux modèles mathématiques simples et pertinents, des repères essentiels dans la jungle des comportements évolutifs observés dans le monde réel. Dans une croissance

linéaire, l'accroissement par unité de temps est un nombre fixe : par exemple le diamètre d'un arbre croit de 5 cm par an, indépendamment de sa taille. Dans une croissance exponentielle, l'accroissement par unité de temps est proportionnel à la quantité : par exemple l'évolution du nombre de personnes contaminées par un virus dépend du nombre de personnes contaminées. C'est l'effet boule de neige.



Croissance linéaire vs croissance exponentielle

Voir la formulation mathématique

Complément

Si x_n désigne la quantité mesurée l'année n, et a le coefficient de proportionnalité ou *taux de croissance*, la croissance exponentielle s'exprime par la relation

\begin{equation}x_{n+1}−x_n=ax_n\end{equation}

La suite (x_n) est une suite géométrique : $x_{n+1} = (1 + a)x_n$ de raison $1 + a$ supérieure à 1, le fameux R des modèles d'épidémiologie. Lorsque a est positif, plus la quantité est importante, plus elle augmente.

« Plus vite, plus grand, plus beau : pendant plusieurs décennies, les lois de Moore ont gouverné la croissance exponentielle des performances de l'informatique, avec une sensation de progrès plus forte que dans aucun autre secteur. », Cédric Villani (2021)[Villani, 2021].

La part des émissions mondiales de GES due au numérique croit aujourd'hui de 6% par an, c'est-à-dire qu'elle est multipliée par 1,06 chaque année. Au bout de deux ans elle sera multipliée par $1,06^1 = 1,1236$. Par exemple, la quantité de données échangées sur les réseaux mobiles double tous les 3 ans ! Là, on y voit un peu plus clair, on sait qu'une quantité qui double à intervalles de temps réguliers va vite devenir faramineuse, comme l'illustre le problème de l'échiquier de Sissa, ou celui de la croissance des nénuphars *(Olivi, 2020)*[Olivi, 2020]. Calculer le temps de doublement d'une quantité permet de mieux se représenter une croissance exponentielle. Au rythme de 6% par an, la part des émissions mondiales de GES dues au numérique devrait donc doubler d'ici 12 ans ($1,06^{12} = 2,0122$). Cela voudrait dire que dans les 12 prochaines années, le numérique émettrait autant de GES qu'il en a émis à ce jour depuis le début de la révolution numérique. Ses émissions représenteraient alors 7% des émissions mondiales de GES, alors qu'elles sont aujourd'hui à 3,5%. Et c'est compter sans l'augmentation probable de ce taux de croissance *(Shift Project, 2021)*[Shift Project, 2021].

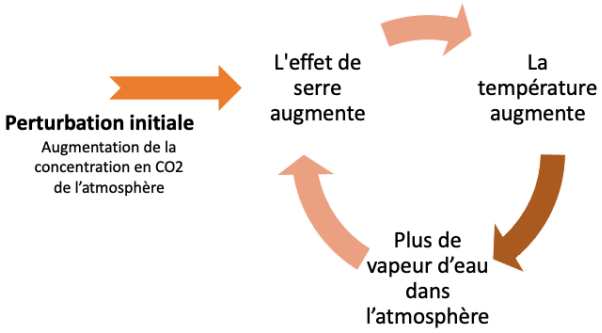
Mais au fond, pourquoi cette croissance vertigineuse se poursuit-elle alors que les progrès techniques rendent nos équipements de plus en plus performants d'un point de vue énergétique ? Cela s'explique de la façon suivante *(Shift Project, 2021)*[Shift Project, 2021] : l'amélioration des performances techniques induit une augmentation des usages, laquelle suscite de nouvelles améliorations, etc. Il s'agit d'une boucle de *rétroaction* positive qui stimule la croissance. L'augmentation de la consommation énergétique causée par l'augmentation des usages, compense largement les économies d'énergies dues aux améliorations techniques. C'est ce qu'on appelle un effet rebond (voir la fiche concept *L'effet rebond* (cf. p.60)).

Cercle vicieux ou vertueux ?

Selon *Olivier Hamant (2020)*[Hamant, 2020], directeur de recherche à INRAE,

« La rétroaction est un concept clé pour comprendre le vivant, de la cellule à la planète »

Ce concept est en outre plus pertinent que celui de causalité pour décrire le comportement d'un système complexe. On distingue les rétroactions positives qui provoquent une accentuation du phénomène, voire un emballement. Une petite perturbation peut alors déclencher une croissance exponentielle des quantités en jeu. Les rétroactions négatives au contraire s'opposent au phénomène qui les a engendrées et peuvent le réguler, ou le réduire à néant.



Boucle de rétroaction de la vapeur d'eau

Dans les modèles du climat, on trouve de nombreuses boucles de rétroaction. Un exemple classique est celui de la vapeur d'eau. L'augmentation du CO2 dans l'atmosphère (perturbation initiale) conduit à une augmentation de la température globale. Lorsque la température augmente, la concentration en vapeur d'eau de l'atmosphère augmente à son tour. Il y a plus d'humidité dans l'air. Mais la vapeur d'eau est un puissant gaz à effet de serre. Si la quantité de vapeur d'eau dans l'atmosphère augmente, cela va provoquer une élévation de la température et ainsi de suite.

Les cas des nuages est particulièrement intéressant, car il constitue un défi pour les climatologues. Les nuages de la basse atmosphère réfléchissent une partie du rayonnement solaire et contribuent au refroidissement de la planète, tandis que les nuages de la haute atmosphère contribuent à l'effet de serre. Mais les variations de la couche nuageuse dues au réchauffement climatique sont encore mal comprises, et les scientifiques ne savent pas à ce jour si au final les nuages contribuent à une rétroaction positive ou négative *(Li, 2014)*[Li, 2014].

Une vidéo de *SimClimat (2020)*[Institut Pierre-Simon Laplace, 2020] montre l'importance de la prise en compte de ces phénomènes de rétroaction dans les modèles du climat et explique comment vérifier que ces modèles ont été correctement calibrés, c'est à dire que les paramètres extérieurs au modèle ont été correctement choisis.

Aplatir l'exponentielle

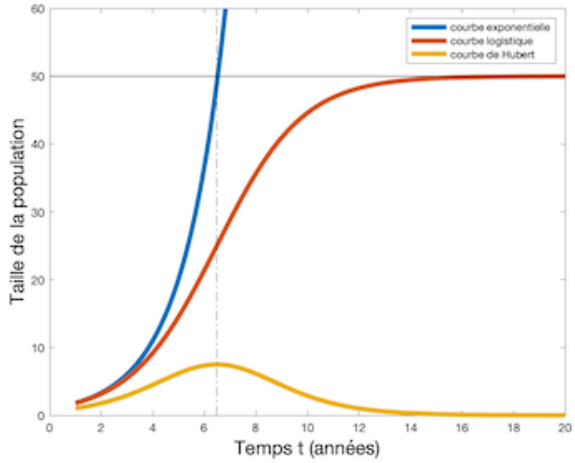
« Je peux vous dire en tant que biologiste que toutes les courbes exponentielles que nous observons dans le monde végétal et dans le monde animal parmi les êtres vivants, finissent toujours extrêmement mal. Le cas où ça se passe moins mal, c'est lorsqu'il y a une stabilisation. »

C'est ce que disait Jean Dorst, ornithologue français, dans l'émission *Demain la terre du 13/04/1974*[Combris, 2020]. Mais comment stabiliser la croissance ? Comment aplatir l'exponentielle ?

Le mathématicien belge Pierre-François Verhulst (1804-1849), chercha une réponse mathématique à ce problème, soulevé par Malthus à la fin du 18ème, lequel s'émouvait de la croissance exponentielle de la population humaine. Verhulst proposa une autre forme de croissance, la croissance logistique. Ce que nous dit ce modèle, c'est qu'une croissance exponentielle confrontée à des limites (nourriture, espace) se régule automatiquement.

Le modèle de Verhulst est en temps continu : le temps y est représenté par une variable réelle, t, et la population à l'instant t est donnée par une fonction mathématique, c'est-à-dire un processus qui à la variable t fait correspondre une quantité notée $f(t)$. La courbe représentative de la fonction f a

une forme caractéristique en S, encore appelée sigmoïde. Elle commence à croître comme une exponentielle lorsque la population est encore petite, puis la courbure s'inverse et la courbe se rapproche d'une valeur limite K sans jamais l'atteindre.



Fonction exponentielle, fonction de Verhulst et fonction de Hubert

Voir la formulation mathématique

Complément

La fonction f est la solution d'une équation qui relie l'*accroissement instantané* de la population à la population elle-même. L'accroissement instantané doit être pensé comme la vitesse de croissance de la population et il correspond à une opération mathématique, la dérivée ou différentielle, notée $f\prime$. L'équation logistique est :

\[f'(t)=af(t)(1−f(t)/K).\]

La croissance exponentielle y est régulée par une rétroaction négative (le signe - dans l'équation), qui fait intervenir un paramètre K, appelé capacité de charge. Lorsque cette capacité tend vers l'infini, le terme négatif tend vers 0 et on retrouve la croissance exponentielle :

\]f'(t)=af(t).\]

En pratique, les deux paramètres a et K doivent être ajustés à partir de données réelles de la même façon que l'on ajuste la pente d'une droite passant par des points qui semblent alignés (régression linéaire). L'accroissement instantané, la fonction dérivée $f\prime$, a une courbe représentative en forme de cloche, symétrique par rapport à son maximum, connue sous le nom de courbe de Hubert.

Le géophysicien américain Marion King Hubert trouva la fonction logistique pertinente pour représenter l'extraction cumulée de pétrole, laquelle est clairement limitée par la quantité totale de pétrole existant. Hubert en déduisit que la production de pétrole, représentée par la courbe en forme de cloche qui porte aujourd'hui son nom, passe par un pic avant de chuter. Il avait même estimé que la production de pétrole aux Etats-Unis passerait par un pic en 1970 !

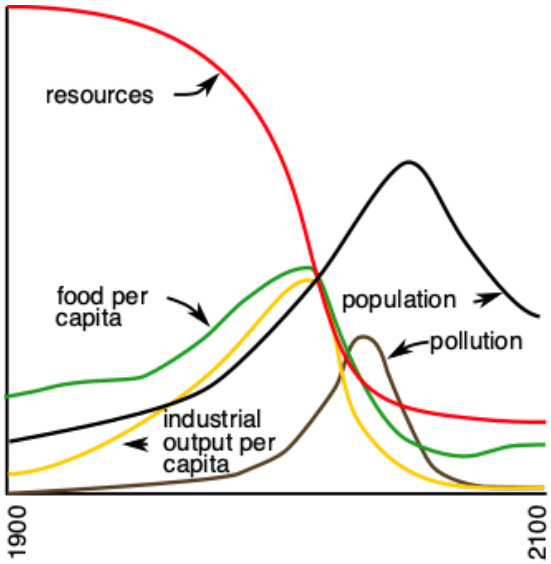
Le modèle logistique, modèle phare de la dynamique des populations, a aussi été utilisé pour analyser l'épuisement des ressources ou illustrer la diffusion d'une innovation. Mais bien sûr un modèle aussi simple ne donne qu'une représentation grossière de la réalité, et ne permet pas de prédictions précises. Il permet toutefois d'estimer des échelles de temps et soulève des questions fondamentales *(Halloy, 2018)*[Halloy, 2018].

Des modèles à l'échelle planétaire

« Essentially all models are wrong but some are useful. », George E. P. Box

Une de ces questions fondamentales est la suivante : les ressources planétaires étant limitées, est ce que la population humaine va gentiment suivre une courbe logistique et se stabiliser autour de sa capacité de charge maximale ou la dépasser puis chuter plus ou moins brutalement ?

Pour répondre à cette question, des chercheurs du MIT ont conçu le modèle mathématique World3, qui a servi à l'écriture du livre "The Limits to Growth" (1972). Ce modèle relève d'une discipline toute jeune, la *dynamique des systèmes*, née dans les années 50 au MIT. L'avènement des premiers ordinateurs autorise alors les chercheurs à s'attaquer à des problèmes complexes, ici à l'échelle planétaire et sur des temps longs. D'après ce modèle, la croissance exponentielle de la production industrielle pourrait effectivement conduire à un dépassement des capacités de charge, et un *effondrement*, qu'il faut entendre comme une chute, plus ou moins rapide, de la population et de la production.



Courbes obtenues avec Wolrd3 et présentées dans "The limits to growth"

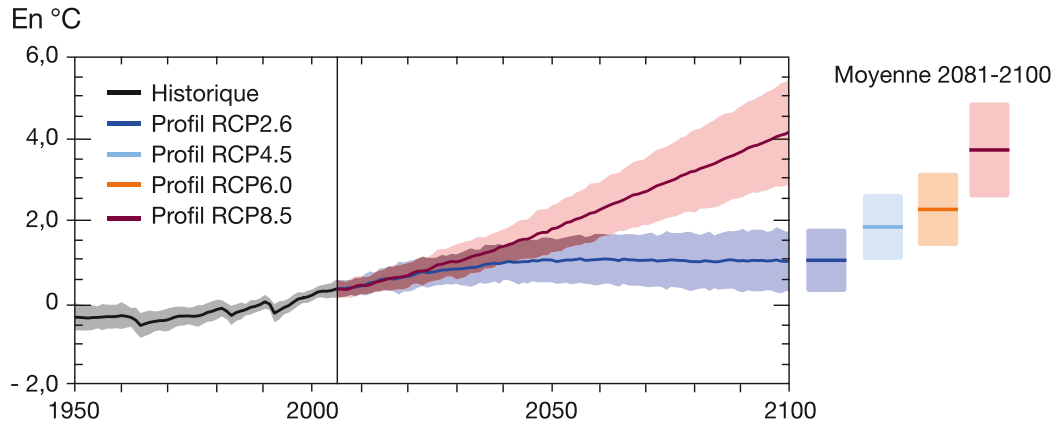
Dans World3, le "*système* monde" est représenté par des réservoirs (population, capital, ressources naturelles et non-naturelles, richesses, pollution), qui communiquent entre eux par des flux de matières et des effets positifs ou négatifs. Ce modèle est fondé sur l'hypothèse d'une capacité maximale de la planète à produire certaines ressources indispensables à l'humanité. Les interactions sont régies par des lois mathématiques simples, comme la croissance logistique.

Il s'agit donc d'un modèle extrêmement simplifié, qui agrège des réalités bien différentes sous une même bannière. Il n'y a pas non plus de moyen rigoureux de vérifier la calibration du modèle : le choix des paramètres clefs et des différentes rétroactions. Cependant, il colle assez bien aux mesures réelles observées depuis, et il fournit des indices intéressants comme l'inertie du système monde ou le rôle majeur de la pollution dans un certain nombre de rétroactions négatives. Comme le souligne *cette vidéo de Heu?reka*[Mitteau, 2020], il porte un message qui parle aux scientifiques : l'humanité doit se donner des objectifs de développement en accord avec les contraintes de la nature. Il a aussi promu une approche systémique des questions environnementales.

À partir des années 50 l'approche systémique, jusque là plutôt réservée à l'ingénierie, s'est répandue à d'autres domaines ; l'évolution du développement humain comme nous venons de le voir, mais aussi l'étude du climat qu'il ne faut pas confondre avec la météo. Dans l'étude du climat, on s'intéresse à des moyennes, des statistiques, pas à des événements localisés ou ponctuels. Historiquement, le premier modèle atmosphérique date de 1950, et a été testé sur le premier ordinateur existant, l'ENIAC. Depuis lors, les modèles de climat n'ont cessé de s'enrichir et incluent maintenant cinq composantes principales : l'atmosphère, les surfaces continentales, l'*hydrosphère*, la *cryosphère*, et la *biosphère*. Ces composantes échangeant entre elles en eau, chaleur, composés chimiques, ...

Contrairement au modèle World3, les équations qui régissent les interactions entre les différentes grandeurs caractéristiques, sont les équations de la physique, et les paramètres clefs sont calibrés sur des données historiques. La résolution numérique de ces équations complexes nécessite le découpage de la surface de la terre, des océans et de l'atmosphère en petits cubes qu'on appelle les mailles. Plus les mailles sont petites, plus les calculs sont précis et fiables. Le nombre de mailles utilisé dans les modèles de climat a augmenté de façon exponentielle au fil des années ! Aujourd'hui une quarantaine de modèles différents sont développés dans le monde, dont celui de l'Institut Pierre-Simon Laplace (IPSL) en France *(SimClimat)*[SimClimat]. L'IPSL propose une version simplifiée de son modèle à usage pédagogique.

Les émissions de GES apparaissent comme des perturbations extérieures au système, et ces modèles simulent les différents scénarios de réduction de ces émissions, qui ont été présentés dans les différents rapports du GIEC. Ces modèles sont imparfaits, parce que certains phénomènes physiques sont encore mal compris et à cause des incertitudes liées aux modélisations numériques. Mais là encore, l'objectif n'est pas de faire des prévisions quantitatives, mais d'obtenir des ordres de grandeurs, qui permettent de comprendre l'influence sur le climat de nos choix de développement. Et ils jouent parfaitement ce rôle.



Changement global de température selon différents scénarios du GIEC calculés par le CMIP

Bibliographie

Complément

Articles

- *Olivi, 2020*[Olivi, 2020]
- *Barré, 2014*[Barré, 2014]
- *Perrin, 2018*[Perrin, 2018]

Ouvrages

- *Meadows et al., 2004*[Meadows et al., 2004]

Pages web

- Insightmaker, The World3 Model Classic World Simulation, url[32] [09/02/2022]

Rapports

- *GreenIT, 2019*[GreenIT, 2019]
- *Shift project, 2020*[Shift project, 2020]

Vidéos

- *Meyer, 2016*[Meyer, 2016]

32. https://insightmaker.com/insight/1954/The-World3-Model-Classic-World-Simulation

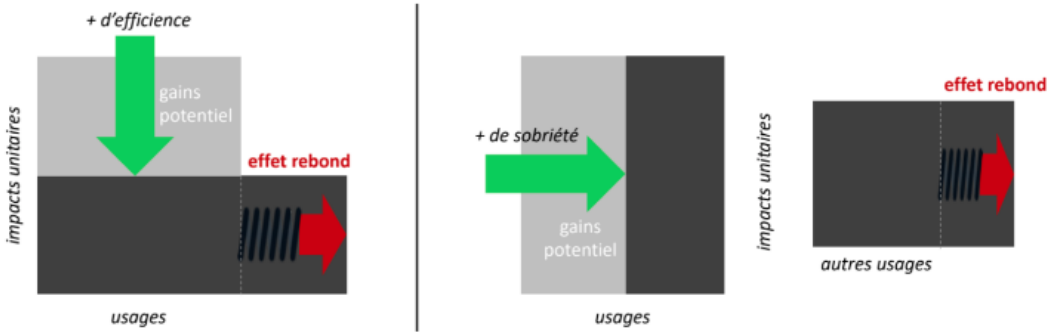
7. L'effet rebond

1 Introduction

Les solutions visant à réduire nos impacts environnementaux peuvent s'appuyer sur deux dimensions :

- la dimension technologique dans les démarches d'amélioration de l'efficacité (suivant le contexte on parle aussi d'*efficience*) qui rend les usages plus économes en ressources et moins émissifs en pollution, sans les remettre en cause. Il s'agit de « faire la même chose, voire plus, avec moins », c'est-à-dire de réduire la consommation « unitaire » de nos usages.
- la dimension des usages dans les démarches de *sobriété* dans lesquelles il s'agit de « faire moins avec moins ».

Par exemple, la réduction de la consommation de carburant aux 100 km d'une automobile relève de la première dimension, alors que la réduction du kilométrage annuel relève de la seconde. L'**effet rebond** annule une partie voire la totalité des bénéfices environnementaux obtenus sur une des dimensions du fait d'effets « secondaires » sur l'autre dimension : améliorer les performances en terme de consommation d'un véhicule peut conduire à une « intensification » de son usage (augmentation du kilométrage annuel, de la vitesse moyenne, etc.).



2 Qu'est-ce que l'effet rebond ?

Une technologie plus efficace a tendance à être plus utilisée, par exemple à cause de la baisse des coûts d'utilisation. C'était déjà le constat que faisait W.S. Jevons pendant la révolution industrielle en Angleterre au XIX^{e} siècle à propos des progrès d'efficacité énergétique de la machine à vapeur : ceux-ci avaient en effet conduit à une augmentation de la demande en charbon et non à l'inverse. Cette situation est appelée effet rebond (plus exactement effet rebond direct), ou paradoxe de Jevons en référence à cet exemple historique du charbon. Un exemple typique d'effet rebond est le trafic induit[33] : une infrastructure de transport plus efficace peut causer une augmentation de la demande, c'est-à-dire du trafic routier. Ce phénomène empêche de résoudre les problèmes de congestion par simple augmentation des capacités routières.

33. https://fr.wikipedia.org/wiki/Trafic_induit

L'exemple de la Katy Freeway à Houston : malgré ses 26 voies elle n'a pas permis de résoudre les problèmes de congestion à cause du trafic induit

Les exemples d'effet rebond dans le secteur du numérique sont nombreux *(Flipo et Gossart, 2009)*[Flipo et Gossart, 2009] : depuis Eniac (le premier ordinateur entièrement électronique) la miniaturisation a rendu possible l'explosion du nombre d'objets électroniques *(Gossart, 2014)*[Gossart, 2014] (ordinateurs personnels, *smartphones*, objets connectés, etc.), les améliorations d'efficacité énergétique des réseaux de transmission combinées à celles des débits et des capacités de stockage ont permis l'explosion du trafic de données *(Bol et al., 2021)*[Bol et al., 2021], etc.

Les effets rebond indirects

On parle d'effet rebond *indirect* lorsque des économies réalisées dans un domaine génèrent de la consommation dans un autre *(Gossart, 2014)*[Gossart, 2014]. Ainsi une démarche de sobriété peut aussi être source d'effets rebond, du fait des économies réalisées qui sont réinvesties (qu'elles soient monétaires ou temporelles), ou du fait de leur effet déculpabilisant sur la consommation d'autres produits *(Schneider, 2009)*[Schneider, 2009]. Par exemple remplacer la voiture par le vélo dans les déplacements quotidiens permet de faire des économies qui peuvent être utilisées pour réaliser des voyages lointains en avion pendant les vacances, ce qui annule les bénéfices environnementaux liés à l'usage du vélo.

Les causes de l'effet rebond

L'effet rebond peut se produire lorsqu'une ou plusieurs limites à l'usage et/ou à la production sont repoussées *(Schneider, 2009)*[Schneider, 2009]. Ces limites peuvent être économiques, physiques, techniques, psychologiques, sociologiques, réglementaires, etc. À l'échelle macro-économique, l'effet rebond se traduit par une augmentation de l'activité économique, si bien qu'il empêche le découplage (absolu) entre croissance et impacts environnementaux *(Brockway et al., 2021)*[Brockway et al., 2021]. L'effet rebond ne s'explique pas uniquement comme résultant de la somme des comportement individuels, il a aussi des origines plus structurelles dans les politiques de croissance *(Schneider, 2009)*[Schneider, 2009], les stratégies commerciales, l'effet des marchés et de la financiarisation, les normes sociales, techniques, et réglementaires *(Wallenborn, 2018)*[Wallenborn, 2018].

Mesurer et prévoir l'effet rebond

L'ampleur de l'effet rebond est définie comme la part des gains potentiels qui est annulée par l'augmentation de l'usage, et on parle de *backfire* lorsque celle-ci excède 100% c'est-à-dire lorsque les gains potentiels sont plus que contrebalancés par les effets négatifs. Prévoir cette ampleur est utile pour anticiper la réalité des gains qu'on peut espérer d'une solution, mais cela reste (très) difficile. L'approche courante pour y parvenir fait appel à des modélisations économiques qui ne sont pas conçues pour rendre compte de changements sociétaux profonds *(Briens , 2015)*[Briens , 2015] (or ce sont d'eux dont nous avons probablement besoin, par exemple pour décarboner nos économies).

Pour comprendre et prévoir l'effet rebond, étudier les tendances historiques se révèle aussi très utile. Elles nous montrent par exemple que l'optimisation continue des infrastructures et des équipements numériques ne permet pas de compenser l'accroissement des usages, si bien que l'empreinte carbone globale de nos réseaux, de nos centres de données, et de nos équipements terminaux tend à augmenter *(Bol et al., 2021)*[Bol et al., 2021]. Plus généralement l'histoire des techniques nous montre comment les usages s'empilent et se complémentent plus qu'ils ne se substituent *(Fressoz, 2021)*[Fressoz, 2021].

3 Quand peut-on s'attendre à un effet rebond ?

L'effet rebond risque de se manifester dans les solutions de type « gagnant-gagnant », plus particulièrement celles qui :

- conduisent à des gains d'argent, de temps (effets d'accélération), d'espace (miniaturisation)
- apportent de nouvelles fonctionnalités (génératrices de nouveaux usages)
- incitent à plus d'usage par des performances ou un confort d'utilisation accrus.

4 Comment limiter l'effet rebond ?

- sensibiliser à l'effet rebond, inciter à conscientiser les intentions (sont-elles écologiques ? économiques ?)
- penser de façon systémique et à des échelles larges (donc à l'échelle collective plutôt qu'individuelle)
- favoriser les solutions « low-tech » (car elles évitent en général de générer de nouveaux besoins)

- flécher les budgets économisés (en argent ou en temps) vers d'autres améliorations environnementales pour lutter contre les effets rebond indirects.

8. Communs négatifs et externalités négatives

Préambule

La fiche ici proposée repart d'une définition des communs négatifs proposée par Alexandre Monnin et Lionel Maurel dans le cadre d'un glossaire sur les politiques publics. Elle l'actualise à partir des dernières recherche menées sur cette notion.

Introduction

La notion de commun négatifs a été introduites pour la première fois par *Marie Mies et Veronika Bennholdt-Thomsen (2001)*[Mies et Bennholdt-Thomsen, 2001]. Elle désignait alors les déchets produits par les communautés humaines et biotiques et la capacité de ces dernières à les absorber. Pour les autrices, le capitalisme, en détruisant les communauté et en privatisant les activités de traitement des déchets, retire aux communautés leurs capacités ancestrales pour les déplacer vers des circuits économiques orientés par le profits.

Le militant et chercheur japonais *Sabu Kohso (2021)*[Collectif et al., 2018 ; Kohso, 2021] parle également de communs négatifs pour désigner les déchets radioactifs, dans le sillage de ses analyses au sujet de la catastrophe de Fukushima. Pris dans ce sens, ils désignent une réalité qui ne peut, précisément, être réabsorbée par les communautés elles-mêmes. Elle est marquée par une irréversibilité sur des échelles de temps qui dépassent la mesure humaine.

Les communs négatifs

Les communs négatifs au sens où nous l'entendons, désignent des « réalités », matérielles ou immatérielles, valuées négativement, tels que les déchets radioactifs, les centrales à charbon, les sols pollués ou encore certains héritages culturels (le droit d'un colonisateur, etc.). Par le mot « valuées » *(Dewey, 2008)*[Dewey, 2008], on entend désigner les opération de valuation en jeu. Autrement dit, les pratiques par lesquelles une valeur est accordée ou reconnue à quelque chose.

Tout l'enjeu de ces communs négatifs étant d'en prendre soin collectivement (*commoning*) à défaut de pouvoir en faire table rase. Aussi s'agit-il d'un élargissement de la théorie classique des communs, notamment par rapport à l'approche positive des Commons Pool Resources proposée par *Elinor Ostrom (1991)*[Ostrom, 1991]. On peut qualifier celle-ci de « bucolique » car elle s'applique avant tout à des réalités valuées positivement, qu'il convient donc de préserver.

L'approche par les communs négatifs tourne autour de deux axes majeurs :

1. le fait d'accorder une valeur négative à des réalités souvent jugées positives – les réserves d'énergie fossile, l'aviation, la voiture, etc. (ce que l'on pourrait qualifier de lutte pour la reconnaissance en considérant que tout commun est d'abord un incommun *(de la Cadena, 2019 ; Blaser et de la Cadena, 2017)*[de la Cadena, 2019 ; Blaser et de la Cadena, 2017] chargé d'une conflictualité). Dans l'ouvrage *Héritage et Fermeture (Bonnet et al., 2021)*[Bonnet et al., 2021], une distinction a été proposée entre ruine ruinées et ruines ruineuses. Les ruines ruinées désignent les paysage typiques d'une esthétique de l'Anthropocène : sols pollués, rivières asséchés, infrastructures désaffectées, etc. Les ruines ruineuses, quant à elles, désignes les infrastructures et modèles en activités dont le fonctionnement-même compromet l'habitabilité du monde. Le numérique, à cet égard, est-il un vecteur d'utopie *(Turner et al., 2013 ; Broca, 2013 ; Tréguer, 2019)*[Turner et al., 2013 ; Broca, 2013 ; Tréguer, 2019], comme il le semblait au début des années 2000 (utopie de la participation, *open access*, logiciel libre, communs numériques de la connaissance, etc.) ou un commun négatif dont la trajectoire est fondamentalement insoutenable ? Il n'est pas aisé de répondre à cette question dont l'incertitude renvoient aux situations de controverses (voir la *fiche concept "Les controverses sociotechniques"* (cf. p.64)).

2. le fait de bâtir de nouvelles institutions susceptibles de permettre à des collectifs de se réapproprier démocratiquement des sujets qui leur échappaient jusqu'à présent, en particulier la coexistence avec les communs négatifs, plus ou moins mis à distance (on peut songer aux récentes mesures prises par des maires au sujet des pesticides mais aussi au demandes émergeantes concernant des zones de déconnexion s'agissant du numérique). Cette réappropriation par le détour de nouvelles institutions, pose de nombreuses questions : d'échelles, de compétences, de subsidiarité, de droit ascendant, etc.

Par ailleurs, les communs négatifs peuvent induire l'idée de communautés de non-usage, autrement dit, de collectifs cherchant à ne plus utiliser certaines entités autrefois qualifiées de ressources (à l'opposé, cette qualification constituait clairement une désinhibition facilitant et légitimant les démarches extractivistes).

On parle d'externalités négatives, cette fois, pour désigner les effets ou dommage d'une transaction affectant un tiers qui n'est pas impliqué dans ladite transaction. Les économistes proposent d'internaliser ces externalités dans les marchés pour leur assigner un prix afin d'en limiter la survenue. D'autres proposent au contraire de mesurer le coût social et économique de la reconnaissance du dommages que représentent ces externalités et de les mettre en balance avec coût des réparations qu'elle induisent (si fermer une usine est le prix à payer, il vaut parfois mieux, selon ce raisonnement, tolérer un dommage sanitaire ou environnemental, voire, il appartient aux personnes affectées d'acheter leur droit à ne pas le subir *(Chamayou, 2018)*[*Chamayou, 2018*]).

Les externalités sont vues comme des conséquences malheureuses d'activités qu'il ne s'agit pas de remettre en cause. On cherche plutôt à en limiter les dommages par des mécanismes économiques ou par des innovations techniques et des procédés gagnant toujours plus en efficacité. Avec les communs négatif, l'enjeu est fondamentalement renversé. Les conséquences sont vues comme des conditions et l'enjeu est alors de politiser la question de l'existence même (et donc les causes) des communs négatifs. Ceci nous renvoie à la question de la démocratisation des enjeux techniques.

9. Controverses sociotechniques

Pourquoi étudier les controverses

Donner à voir au public la victoire d'un grand homme (trop peu de femmes de sciences ont été mises à l'honneur dans le cadre de disputes savantes) et de sa théorie : tel fut longtemps l'objet de la « controverse », terme employé pour désigner la mise en scène de disputes savantes incarnées par d'illustres protagonistes. En fournissant un aperçu des sujets débattus, les controverses contribuaient à exposer une querelle scientifique et légitimer sa résolution. Elles vulgarisaient les savoirs scientifiques et racontaient leur élaboration.

Ce procédé narratif paraît aujourd'hui désuet, voire inapproprié, face aux situations d'incertitude – d'origine environnementale, sanitaire ou technologique – dans lesquelles les citoyennes et les citoyens sont placés sans que les connaissances scientifiques ne permettent de trancher aisément. L'irruption du Covid-19 (mais l'on peut penser à la 5G) montre, non sans susciter l'étonnement, le temps relativement long dont les sciences ont besoin pour comprendre, faire preuve et convaincre. Alors que les controverses prolifèrent et changent de nature, rendant l'action collective difficile, les sciences sociales sont plus que jamais utiles. En postulant que la production des savoirs est indissociable du contexte dans lequel ils se construisent, elles font de l'analyse de controverses un ressort de compréhension et d'action. En la fondant sur la méthode de l'enquête – qui décrit des acteurs et des autrices, des enjeux, des arguments, des dispositifs de preuves et des arènes de débats –, elles en font aussi un outil pédagogique, précieux pour former les citoyens d'aujourd'hui et de demain à l'esprit critique.

Parce qu'il retrace le réseau de relations qu'entretiennent les divers protagonistes, qu'il prenne en compte les façons multiples de délimiter et de représenter un problème et que son exercice permette de se repérer dans la *terra incognita* que constitue une controverse, ce type d'analyse prend parfois, métaphoriquement, le nom de *cartographie* des controverses.

La science en train de se faire

Durant les années 1930, le philosophe Karl Popper identifie l'importance du dissensus dans l'activité scientifique. À l'aide du principe de falsifiabilité, il fait de la réfutation d'une théorie déjà établie le principal moteur de la science. Bien après lui, à partir des années 1970, les tenants d'une approche sociologique et anthropologique de la connaissance scientifique, parce qu'ils et elles se veulent attentifs à la science en train de se faire *(Latour, 2005)*[Latour, 2005] et privilégient l'étude circonstanciée de sa pratique et de ses dispositifs expérimentaux, documentent le rôle des controverses dans la production de faits. Ces historiens et sociologues des sciences nomment ainsi des oppositions théoriques et méthodologiques propres à la production de connaissances scientifiques et en font une étape, un moment, dans le processus d'émergence d'un énoncé valide.

Pour comprendre comment le concept de controverses éclaire le fonctionnement des sciences les plus fondamentales et *a priori* éloignées de toute dynamique sociale, suivons plus particulièrement le sociologue Harry Collins qui, depuis les années 1970 et jusqu'à la découverte des ondes gravitationnelles en 2015, a conduit une étude de terrain auprès de la communauté de physiciens et physiciennes des hautes énergies qui cherchaient à prouver leur existence *(Collins, 1975)*[Collins, 1975]. Une controverse avait émergé en 1968, date à laquelle le physicien Joseph Weber prétendit avoir découvert les ondes gravitationnelles grâce à un nouveau système expérimental. Ses pairs ne parvenaient pas à reproduire ce résultat, même en s'inspirant de son protocole, et pas davantage à prouver qu'il avait commis une erreur. Collins explique que, sur un front de recherche innovant, on ne peut pas s'appuyer sur un résultat – non encore défini – pour valider un dispositif expérimental, ni sur une méthode scientifique rigoureuse – non encore établie – pour valider ce résultat.

Durant sa recherche, Collins invite les scientifiques à s'exprimer sur les dispositifs expérimentaux de leurs collègues et concurrents lors d'entretiens. Il découvre l'ampleur et la virulence de leurs oppositions méthodologiques et théoriques et révèle aussi des critiques à dimension sociale, qu'elles soient institutionnelles (la confiance portée en une université ou un laboratoire), relationnelles (liées au charisme par exemple) ou relevant de la xénophobie ou de la misogynie. Bref, un monde fait d'humains, dont les interactions constituent un objet d'étude pour la sociologie.

Pour Collins, la controverse est donc un moment de confrontation des méthodes et de dialogue plus ou moins civilisé, une étape participant à la construction collective d'un fait scientifique, obtenu alors qu'une communauté parvient à un consensus. Selon lui, l'étude des controverses est féconde d'un point de vue épistémologique – et pour certains sociologues des sciences *(Gingras et Chevassus-au-Louis, 2013)*[Gingras et Chevassus-au-Louis, 2013], elle devrait se limiter à cette prétention.

Quand la controverse fait controverse

Pour d'autres sociologues, au contraire, une controverse ne se réduit pas à l'univers de la recherche scientifique. *Cyril Lemieux*[Lemineux, 2007], par exemple, y voit certes une querelle scientifique, qu'il qualifie de conflit triadique (deux partis qui s'opposent et un public de pairs qui juge), mais il y adjoint la possibilité d'un processus de « déconfinement de la controverse » dès lors qu'un des acteurs en présence cherche à mobiliser d'autres forces (sociales, économiques) pour l'emporter ; s'ensuit une phase de « reconfinement » pour ramener le débat dans une arène où le jugement scientifique peut opérer.

À la suite *d'autres auteurs*[Barry, 2001 - Wynne, 1992], nous pensons que l'étude des dispositifs de preuve en société mérite une attention singulière et plus appuyée. *Yannick Barthe*[Barthe, 2010] relate comment des vétérans de l'armée française, déployés au Sahara durant les années 1960 et en Polynésie en 1996, ont cherché à démontrer qu'ils souffraient de leur exposition à des radiations lors d'essais nucléaires. La preuve épidémiologique de leur mise en danger, qui aurait consisté à comparer chez le groupe de soldats exposés, au regard de leur classe d'âge, la prévalence de cancers de la thyroïde, leur était impossible à fournir sans l'aide de l'État pour réunir une liste des personnels présents à l'époque sur la zone. Or, c'est précisément l'État qui était visé par leur plainte. Pour avoir une chance d'établir une preuve, il leur fallait faire connaître leur cause et donc atteindre de nouveaux publics en joignant leur voix à celles d'autres collectifs avec lesquels ils entretenaient pourtant des rapports complexes (victimes autochtones des essais, militants pacifistes anti-nucléaires et écologistes). Ils finirent par obtenir la reconnaissance de leur préjudice

ainsi qu'une prime. Malgré un dispositif de preuve biaisé (ne sont venus à eux que ceux qui y ont vu un intérêt : d'autres vétérans malades), l'élaboration d'un lien causal entre l'exposition à des essais nucléaires et les cancers développés par des vétérans, et leur capacité à faire émerger une mobilisation sociale, sont ici indissociables et de même nature. On retrouve aujourd'hui les même processus et débats autour des effets sanitaires, loin d'être tranchés, de la 5G.

Les arguments à analyser procèdent d'un entrelacs de dimensions scientifiques, techniques, sociales, politiques et économiques, sans qu'il soit possible d'établir de causalité simple ou d'isoler un aspect. L'étude d'une controverse confrontée à des interrelations aussi subtiles et complexes ne peut donc se réduire à penser la production de connaissances comme issue de l'univers clos de la recherche : elle s'intéresse aux preuves en société.

La controverse, on l'aura compris, fait controverse *(Benvegnu et Schultz, 2016)*[Benvegnu et Schultz, 2016]. D'abord parce qu'elle n'est pas tant une forme prédéfinie du répertoire des débats sociaux que le résultat de mobilisations *(Chateauraynaud, 2011)*[Chateauraynaud, 2011] et qu'elle constitue elle-même un objet de débats : souvent, son existence même ne fait pas consensus. Pour certains acteurs par exemple, qualifier un désaccord de controverse reviendrait à légitimer un doute, alors qu'ils ou elles estiment souvent n'être confrontés qu'à des fantasmes ou de la calomnie. Au sein même des sciences sociales, où la notion est associée à un courant de recherche en sociologie des sciences – celui de la théorie de l'acteur-réseau portée par Madeleine Akrich, Michel Callon et Bruno Latour notamment –, définir une controverse pose problème. Précisément parce que nous sommes attentifs à la pluralité des voix dans une controverse *(Pestre, 2007 - Lamy, 2017)*[Pestre, 2007 - Lamy, 2017], nous ne prétendons pas ici trancher un débat définitionnel ou méthodologique en sociologie. Mais nous voulons témoigner de sa fécondité comme dispositif d'initiation à l'étude des interrelations entre sciences, techniques et sociétés, en nous penchant sur des sujets brûlants.

Controverses : mode d'emploi

Nous allons ici donner une définition opérationnelle des controverses, c'est-à-dire des critères permettant d'identifier des cas intéressants, ou bien, lorsque l'on s'y trouve confronté, d'orienter le regard vers les dimensions essentielles qui permettent d'en saisir les enjeux et le processus. Les sociologues Nicolas Benvegnu, du médialab de Sciences Po, et Brice Laurent, du Centre de sociologie de l'innovation de l'École des mines, ont, dans le cadre de leurs enseignements, fait émerger la définition suivante, qui a servi de fondement à de très nombreuses formations à l'analyse de controverses :

Az Définition

Une controverse est une situation (1) dans laquelle un différend/désaccord (2) entre plusieurs parties (3) – chaque partie engageant des savoirs spécialisés (4) et aucune ne parvenant à imposer des certitudes (5) – est mis en scène devant un tiers (6). Une controverse est caractérisée par un enchevêtrement d'enjeux variés, de faits et de valeurs (7) ainsi que par le fait que s'y jouent simultanément une définition de la technique et du social (8)[Casanova] .

- Situation (1) : ce terme ouvre la métaphore cartographique fréquemment utilisée dans l'analyse de controverses. Dans le cadre de l'enquête, on produit un état des lieux, c'est-à-dire qu'on rend compte de la manière dont des positions s'établissent et s'agencent à un instant t. La situation s'entend comme une configuration à un moment donné, elle est sujette à des dynamiques et résulte d'une trajectoire.
- Différend (2) : le terme induit l'existence d'une relation entre les positions (un conflit est une relation), au sens où celles-ci se répondent entre elles. Ainsi, on pourra considérer qu'en cas d'étanchéité absolue entre les positions des acteurs dans la formulation de leurs positions, la controverse ne peut être constituée – la controverse suppose une sorte de balistique.

- Plusieurs parties (3) : en théorie, deux parties suffisent à créer une controverse, mais le plus souvent aujourd'hui, les parties sont multiples et de natures très variées, individuelles ou collectives : chercheurs, experts, représentants d'association, militants, activistes, hommes ou femmes politiques, etc. Le seul critère discriminant est la contribution publique de chaque partie à soutenir une position. *L'acteur* se manifeste toujours en son nom – les catégories vagues comme « la société civile » ou « les politiques » sont écartées. Un énoncé doit toujours être situé, en référence à une source. Les acteurs sont dits mobilisés au sens où ils et elles participent à la définition de ce qui fait problème, et c'est souvent là l'un des points de désaccord.
- Savoirs spécialisés (4) : les controverses concernent toujours la production de connaissances et engagent des savoirs spécialisés. C'est d'ailleurs en cela qu'elles se distinguent de la polémique, d'un problème public ou d'un dilemme moral. Le terme de savoirs spécialisés rend compte du fait que les scientifiques ne sont pas les seuls à les produire : il existe aussi des savoirs pratiques, parfois tacites, liés par exemple à un métier ou à l'inscription dans un territoire. Une telle perspective n'affaiblit pas l'autorité des savants. Elle se distingue d'un discours néo-scientiste qui considère que les affirmations d'un scientifique seraient crédibles du simple fait de son titre ou de sa « qualité », ce qui vaudrait argument d'autorité. Mais en décrivant avec finesse comment expertises et savoirs profanes contribuent réciproquement à la compréhension d'enjeux disputés, la méthodologie de l'analyse de controverses rend l'analyse des sciences plus réaliste.
- Incapacité à imposer des certitudes (5) : on parle d'une certitude lorsqu'un certain niveau de consensus autour d'un fait scientifique a été établi, c'est-à-dire lorsque la connaissance a été stabilisée. Il ne faut jamais perdre de vue qu'il existe aujourd'hui un nombre de connaissances stabilisées très important, mais que, par définition, le chercheur ou la chercheuse travaille à établir un fait et que ce processus prend souvent (mais pas toujours) la forme d'une controverse.
- Mis en scène devant un tiers (6) : le tiers est de nature très variable. Il peut s'agir *a minima* des pairs au sein de la communauté scientifique ou, par exemple, des revues dans lesquelles publient les chercheurs au sein d'un champ disciplinaire. Ce tiers renvoie parfois à des publics mobilisés, selon l'objet de la controverse. La mise en scène correspond quant à elle à une manière de cadrer les enjeux du débat, notamment lors de sa médiatisation.
- Enchevêtrement de faits et de valeurs (7) : *a minima*, on peut dire qu'une controverse est précisément le moment où les faits ne sont pas encore établis et où la démarcation avec les *valeurs* n'a pas eu lieu. On a tendance à définir les valeurs *a posteriori*, une fois que les faits sont faits, ce qui n'est pas très réaliste du point de vue des *science studies*. Il faut aussi se rappeler qu'il existe une multiplicité de faits d'une grande diversité de natures. Par ailleurs, le terme de fait a tendance à recouvrir toutes les étapes qui y conduisent alors que ces étapes elles-mêmes peuvent constituer une chaîne de faits. Finalement, un fait n'est rien sans la théorie – en tant qu'exemple, manifestation, prototype, etc. –, ni le travail de mise en forme – de mise en cohérence, de modélisation, d'ordonnancement *(Latour, 2004)*[Latour, 2004] – qui l'accompagnent.
- Indétermination de la technique et du social (8) : les études de controverses ont contribué à montrer combien la technique et le social ne sont pas des domaines en soi, dont on pourrait une fois pour toutes désigner ce qui en relève. Une controverse est justement un moment où la définition de la technique, par exemple, est en jeu *(Callon, 1994)*[Callon, 1994].

Thomas Tari[Thomas Tari]