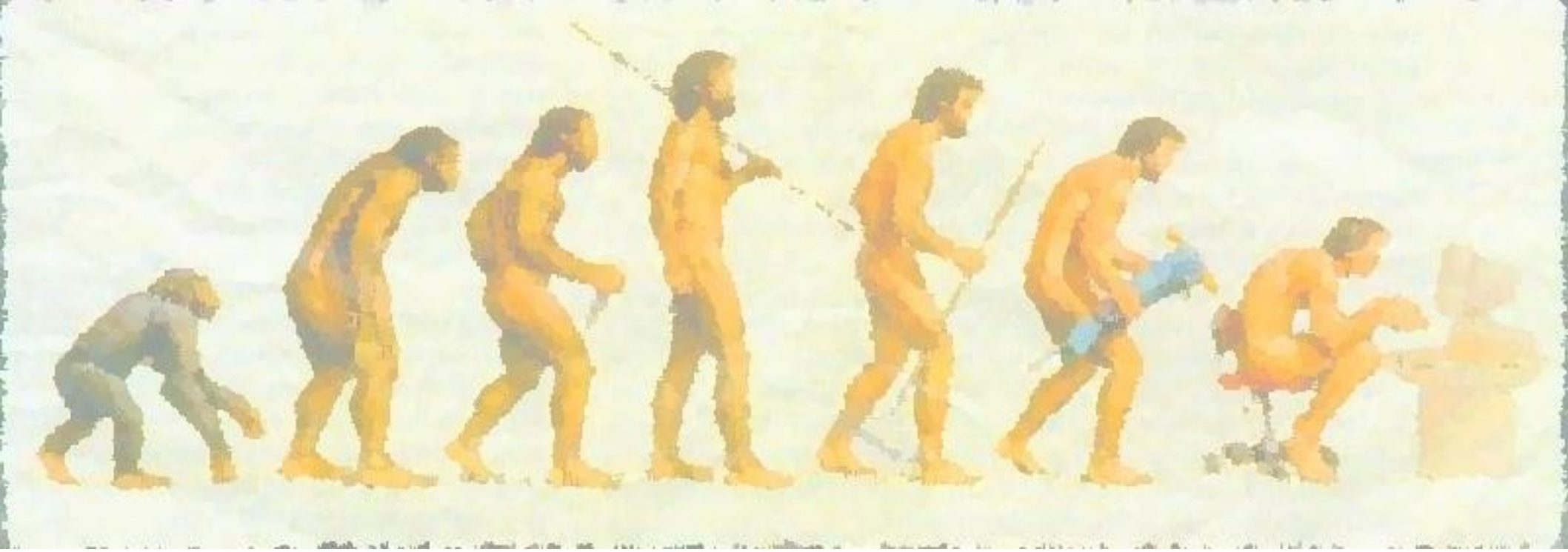


Protection données / ordiphone

Ne pas se faire manipuler

par l'association « Libérons nos ordis »

Menaces numériques

- La manipulation comportementale,
  à des fins commerciales ou politiques
- La discrimination
- Les arnaques (voler ou vendre un produit défectueux ou un service inexistant)

Leurs moyens d'action

- **La manipulation de masse ciblée**
  - permise par le numérique
- Vous exposer à de la publicité ciblée, à des messages (dont de fausses informations) notamment sur les réseaux sociaux
  - ils cherchent à vous faire rester le plus longtemps possible sur leurs réseaux, en vous rendant addict
    Voir les mini-vidéos sur https://arte.tv/dopamine
- Usurper l'identité d'une personne ou d'une organisation

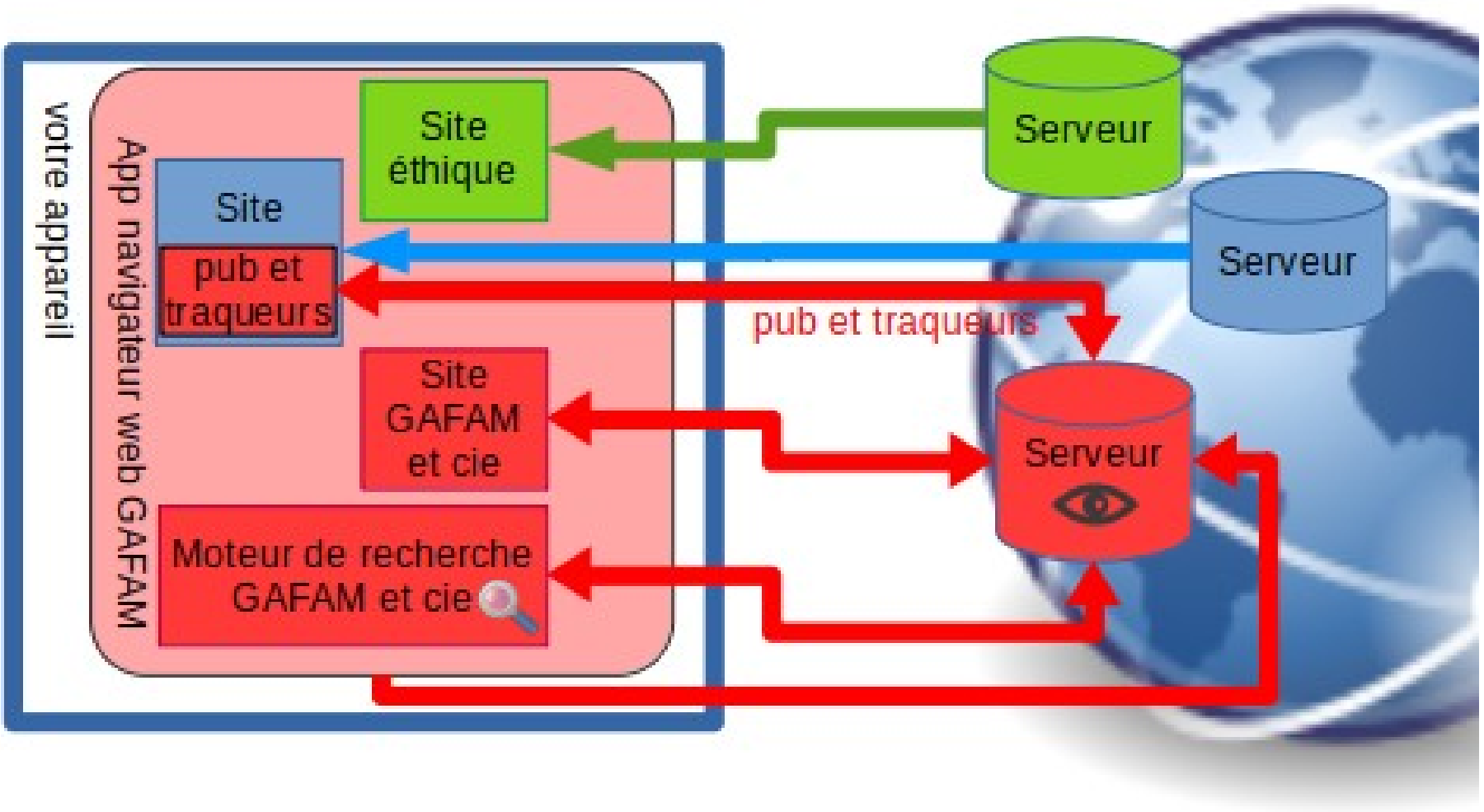
Leur ressource : vos données personnelles

- Pour cibler un message, il faut connaître la cible (sa personnalité, ses comportements, ses opinions, son état de santé, ses points faibles, son graphe social...)
- Pour usurper une identité il faut connaître des informations identifiantes
- Ces informations peuvent être récupérées
  - par de « l'ingénierie sociale »
  - en espionnant vos appareils, vos communications et votre usage des applications et services Internet

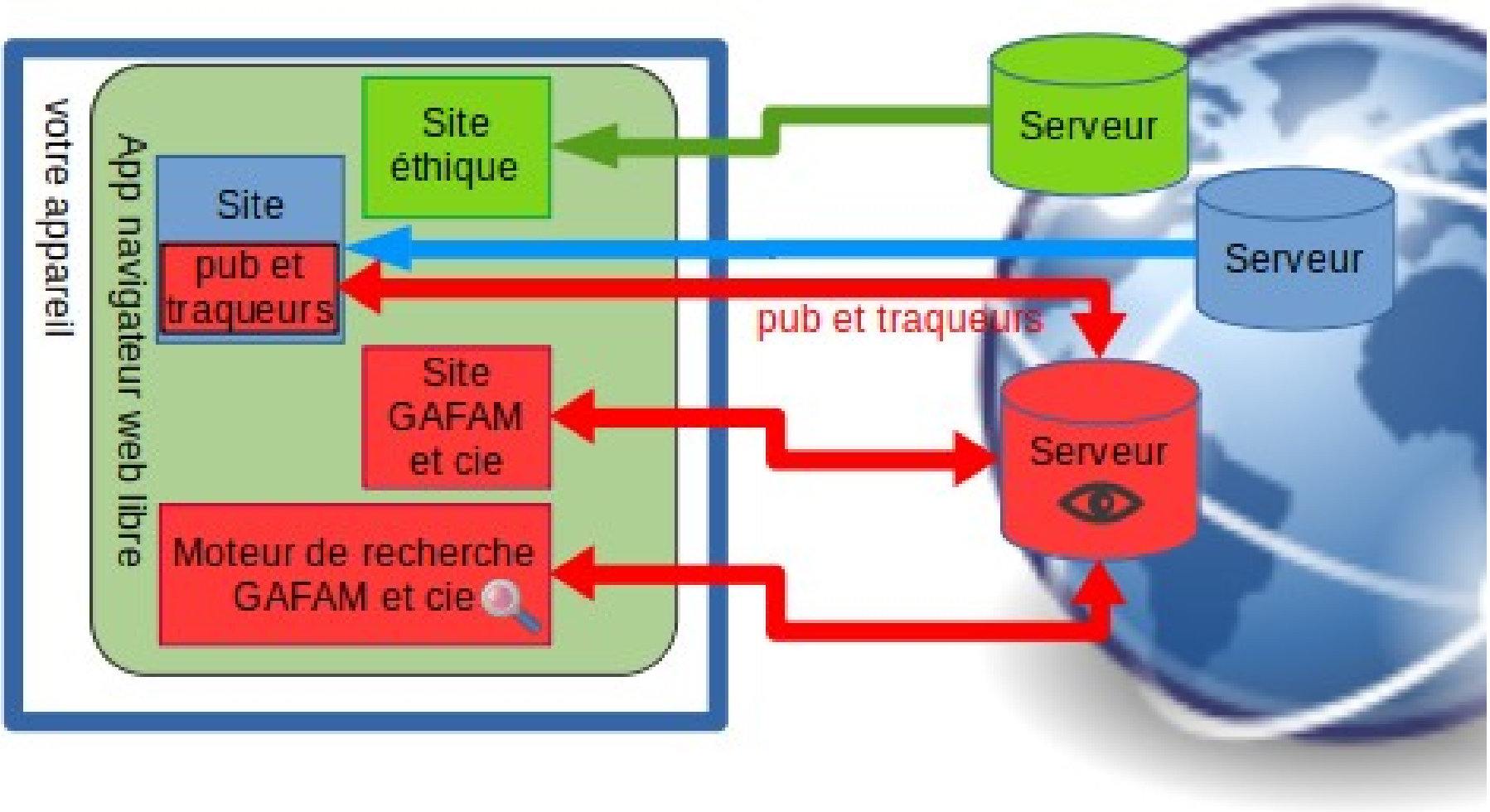
Atelier protection web

- Quoi ?
  - Ne pas divulguer les recherches et les pages web visitées, les objets achetés, etc.
  - Ne pas s’exposer à des contenus manipulateurs
- Comment ?
  - Navigateur web libre : Firefox
  - Bloqueur de pub et de traqueurs : uBlock Origin
  - Moteur de recherche éthique : DuckDuckGo
  - Éviter les sites des GAFAM (Amazon, Facebook...)

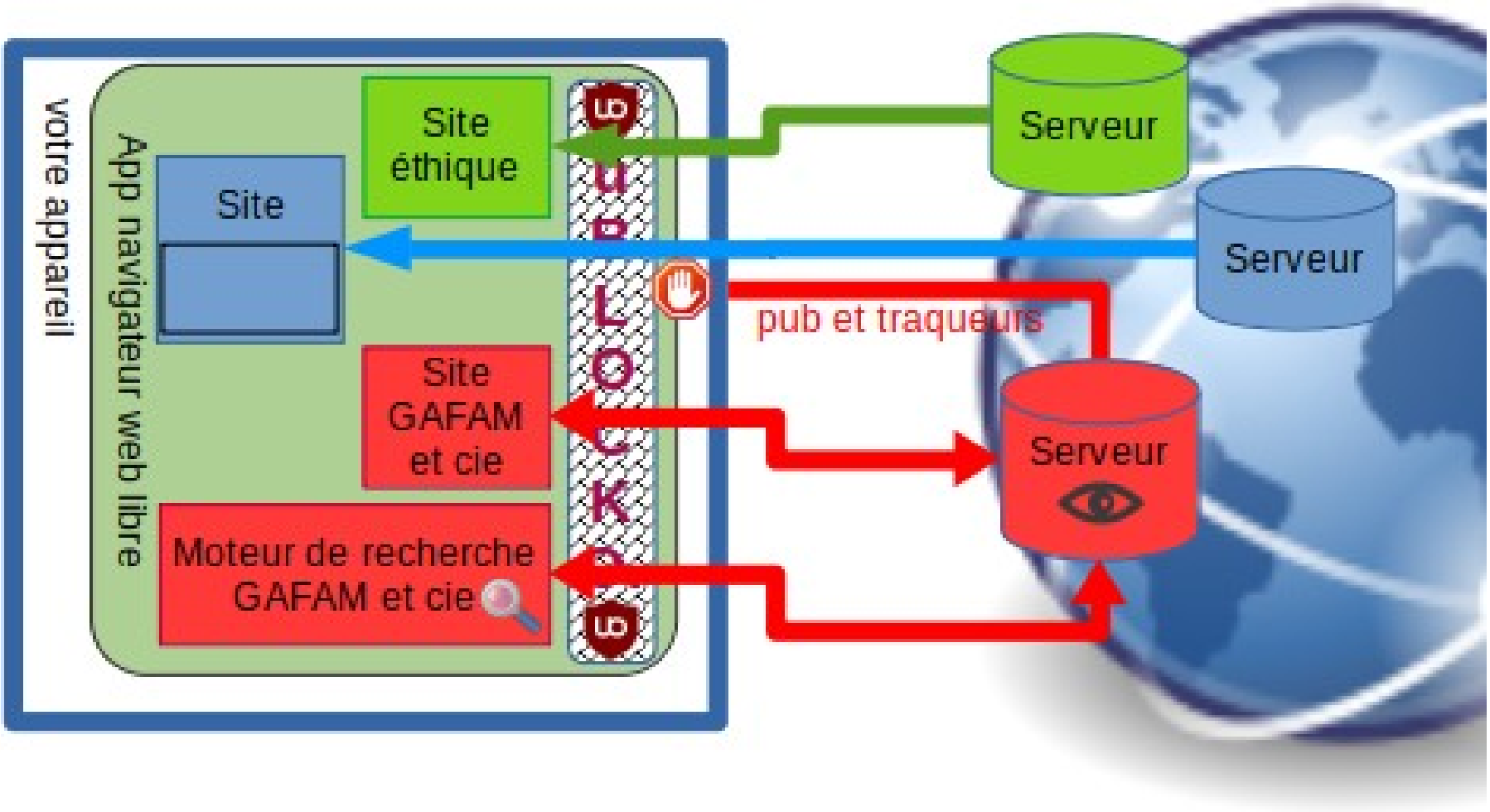
0. Le Web sans protection



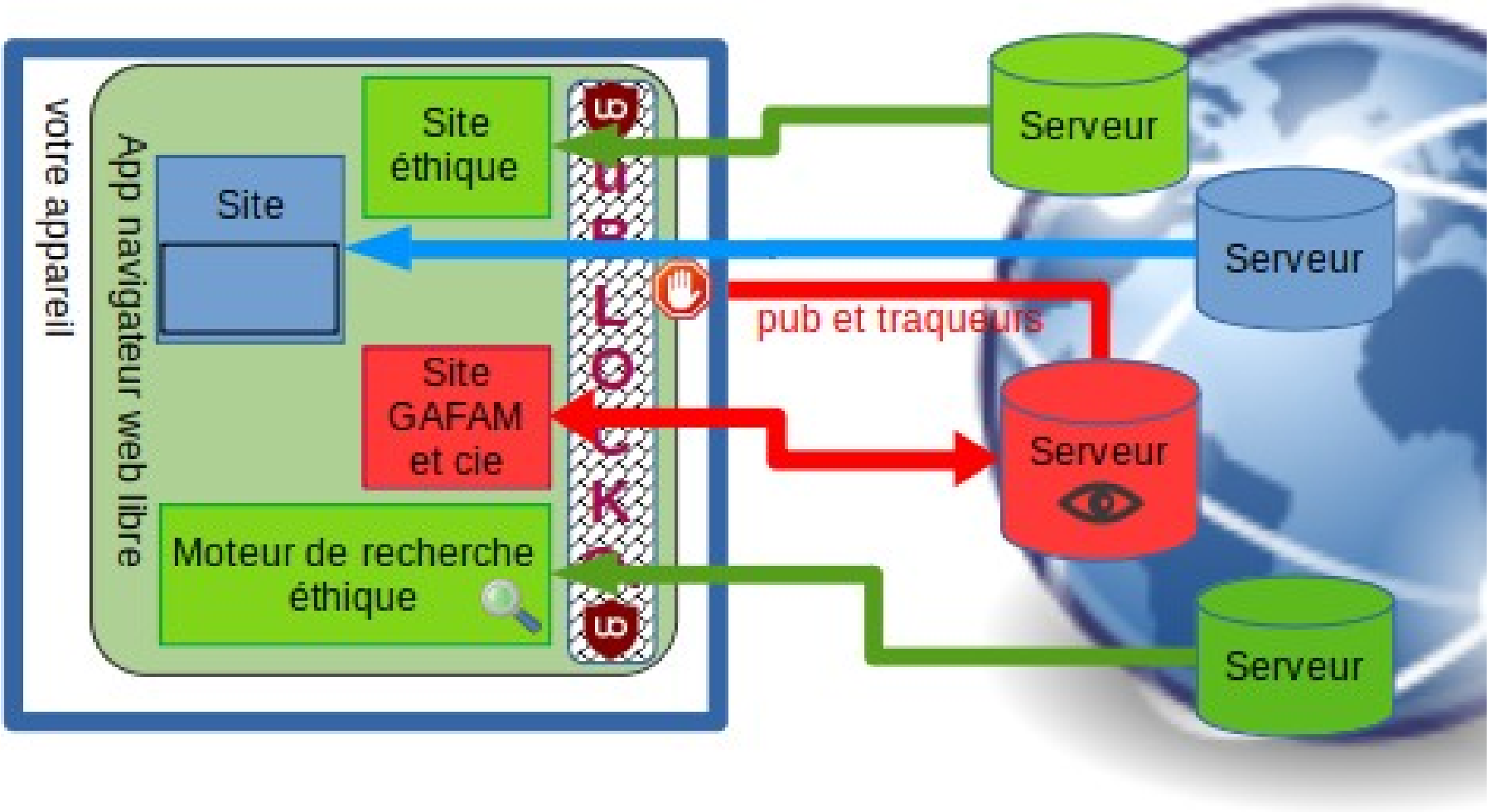
1. Le Web avec un navigateur libre



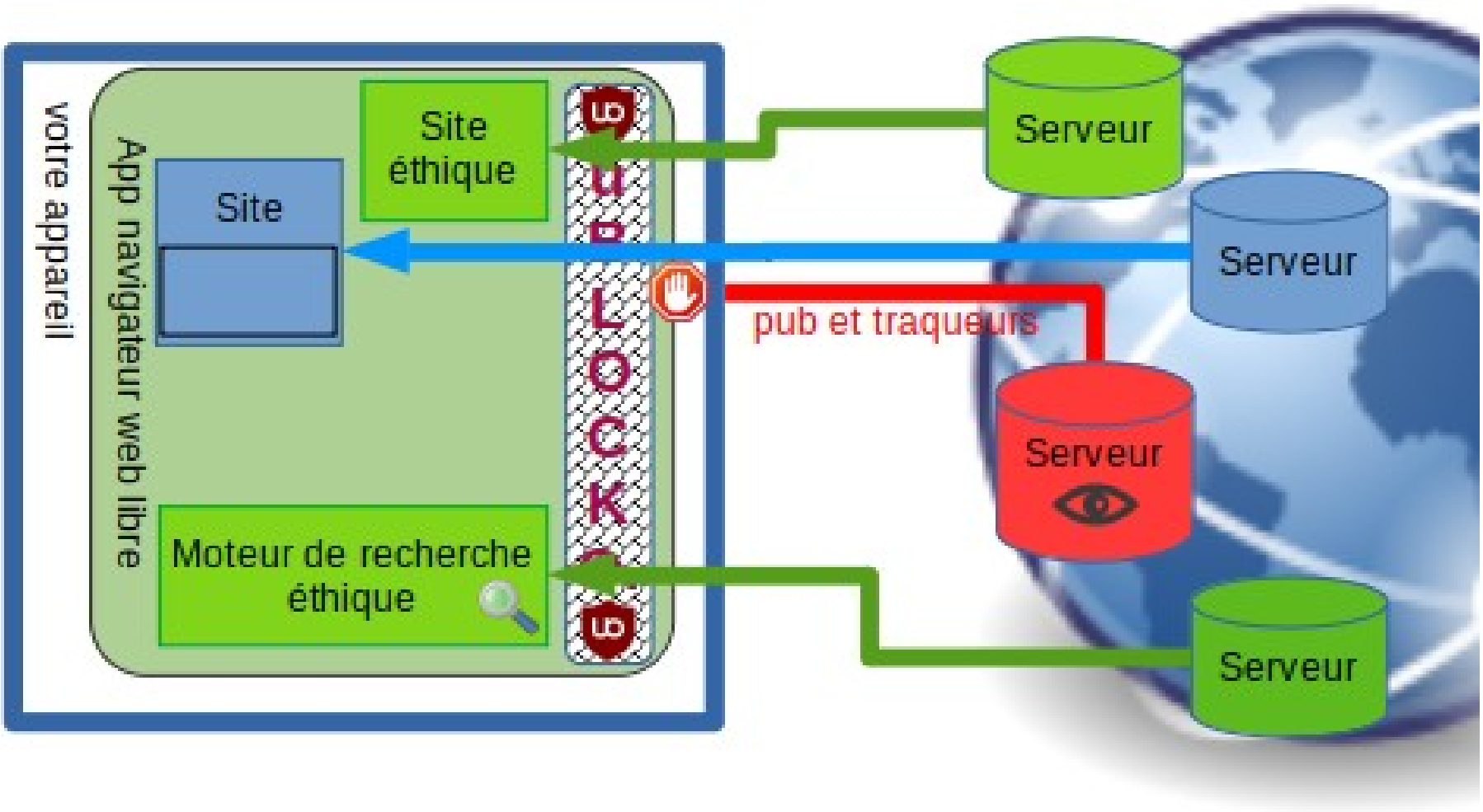
2. + un bloqueur de pub et traqueurs



3. + un moteur de recherche éthique



4. Le web sans les GAFAM



Mise en application

- Suivez la fiche de l'atelier « stop pub et traqueurs sur le web »
- Vous pouvez la retrouver sur notre page « Ressources pédagogiques » § « Fiches descriptives / ateliers » :

  https://blog.liberetonordi.com/index.php?pages/tracts#1.4

Idem sur les autres ordinateurs

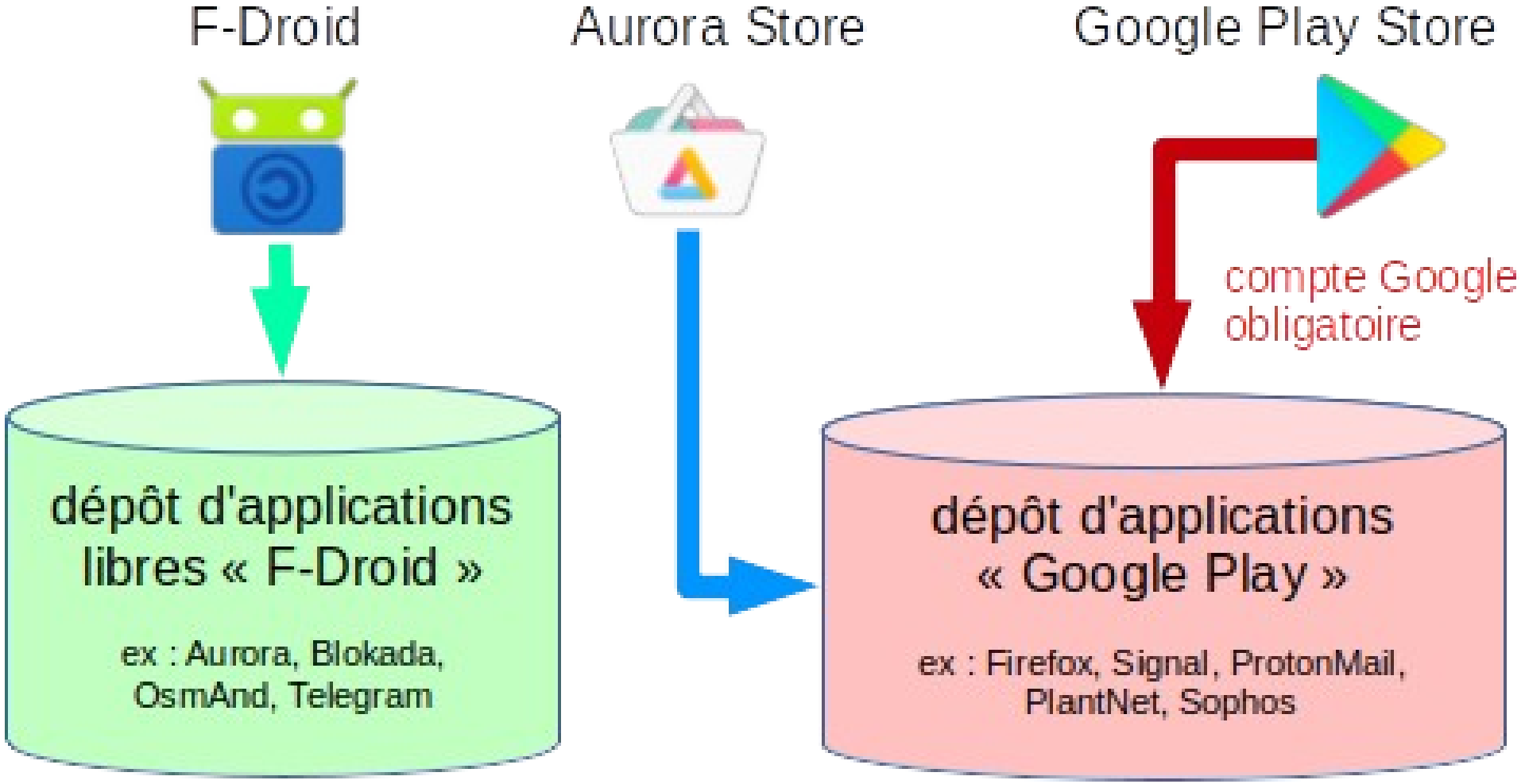
- Vous pouvez reproduire à l'identique ces étapes sur votre ordinateur (fixe ou portable) et sur votre tablette

Atelier protection applications

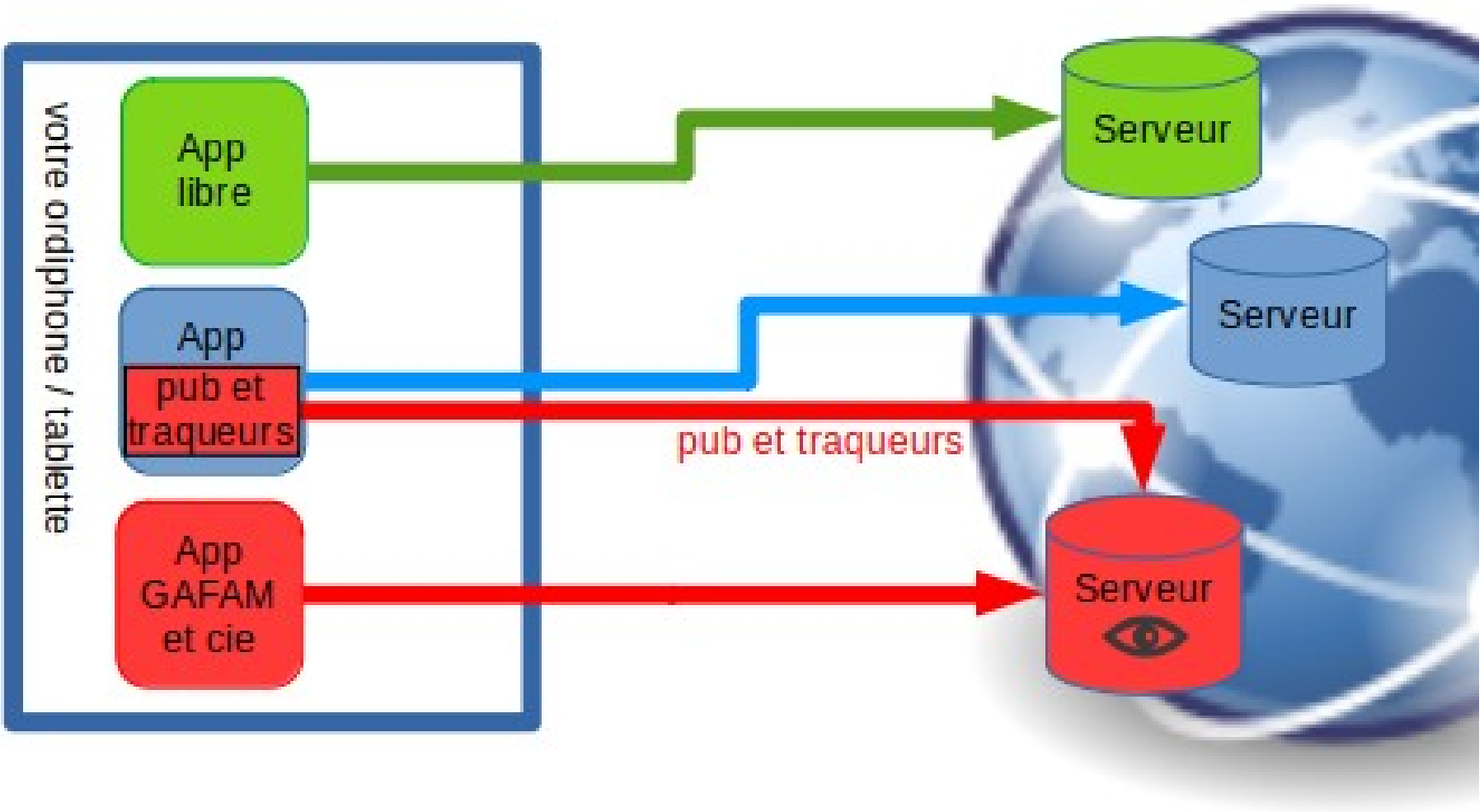
- Magasins d’applications alternatifs pour Android
  - télécharger et installer F-Droid depuis le site web https://**f-droid.org**
  - télécharger et installer Aurora Store depuis F-Droid

- Bloqueur de pub et de traqueurs : Blokada
  - à télécharger et installer depuis le site web https://**blokada.org**
  - pour Android® choisir la version 5 (gratuite)

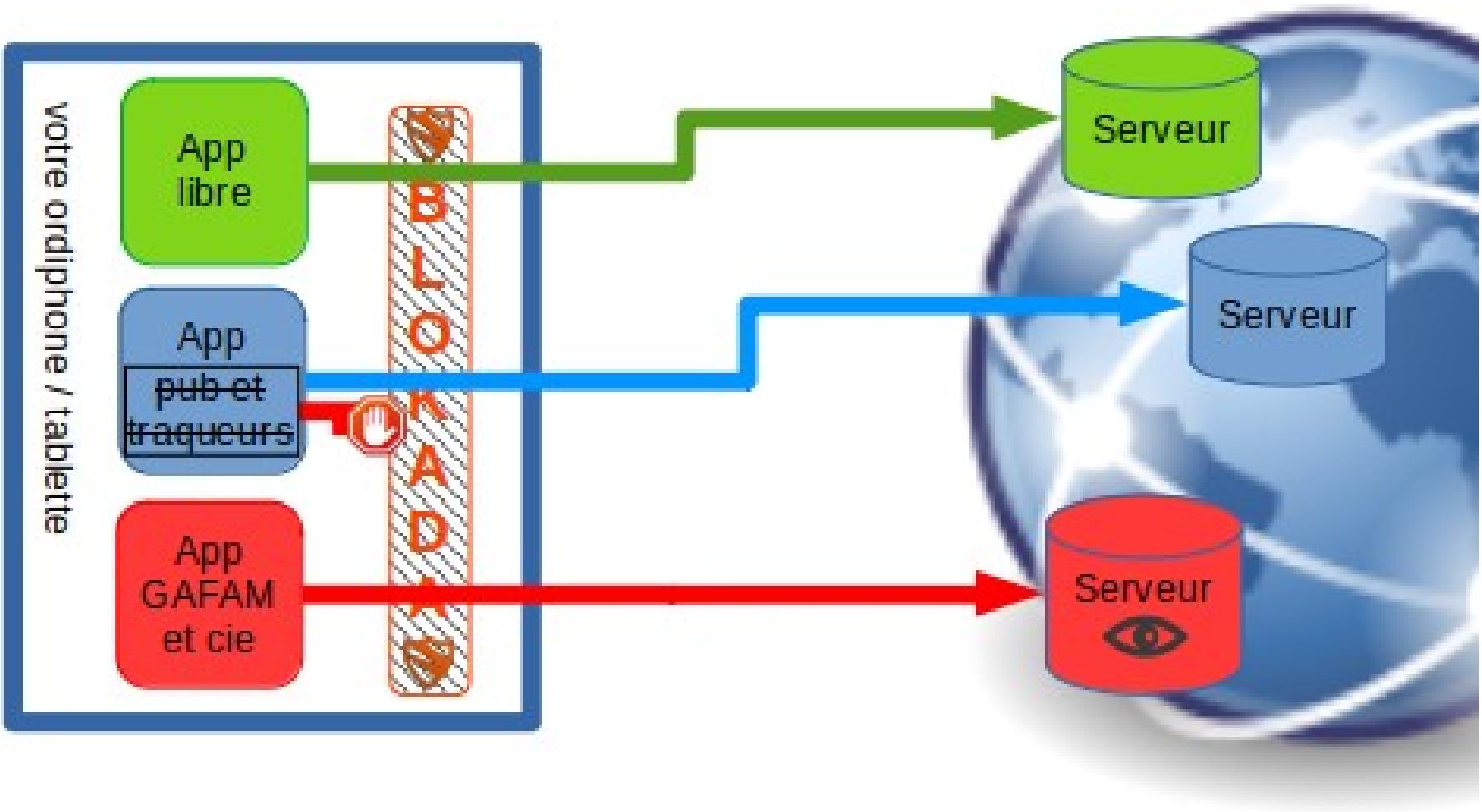
Magasins d’application alternatifs



Sans Blokada



Avec Blokada



Mise en application

- Suivez la fiche de l'atelier « stop pub et traqueurs dans les applications »
- Vous pouvez la retrouver sur notre page « Ressources pédagogiques » § « Fiches descriptives / ateliers » :

  https://blog.liberetonordi.com/index.php?pages/tracts#1.4

Autres applications protectrices

- **Yet Another Call Blocker** (via F-Droid) : bloque les appels téléphoniques indésirables
  - via notation et liste noire
- **Exodus** : informe sur les traqueurs contenus dans les applications et les permissions qu'elles demandent
  - intégré dans Aurora Store et l'App Lounge de /e/OS
- **Sophos Intercept X** (non libre) : anti-virus et configuration de sécurité

Atelier déjouer les arnaques

- Les indices
- Les bonnes pratiques préventives
- Savoir vérifier une adresse mél et web

Indices suspects

- Message inhabituel
- Offre alléchante
- Demande d’avancer de l’argent
- Urgence, peur

Arnaques courantes

- « Nous avons un colis à nous livrer, veuillez rappeler ce numéro »
- « !!! Votre ordinateur est infecté, appelez d'urgence ce numéro !!! » (= Faux support informatique)
- « Votre compte va être désactivé, cliquez ici pour le réactiver »
- Un placement très rémunérateur conseillé par un influenceur ou par une personne de votre connaissance (ex : pyramide de Ponzi)
- **Voir https://cybermalveillance.gouv.fr**

Pratiques préventives (I)

- Ne rappelez JAMAIS un numéro de tél inconnu
  - En cas de doute, contactez la personne ou l'organisme directement
- Ne cliquez JAMAIS sur un lien envoyé par SMS
- AVANT de cliquer sur un lien envoyé par mél, vérifiez l'adresse de l'expéditeur (usurpation d'identité ?) et l'adresse du lien (site contrefait ?)
  - idem avant de répondre à un mél
- Ne rentrez pas votre n° de carte de paiement dans l'ordiphone
- N'investissez pas d'argent dans un projet sorti de nulle part

Pratiques préventives (II)

- Si vous devez télécharger un logiciel en dehors d'un magasin d'application, passez systématiquement par son site officiel
- Garder votre esprit critique : ne prenez pas pour vrai toute image, vidéo ou audio : l'IA permet des imitations très réalistes
- Informez-vous sur des médias sérieux (journalisme d'investigation) et indépendants (Ex au niveau national : Le Canard Enchaîné, Médiapart, Reporterre)
  - l'essentiel de ce qui circule sur les réseaux sociaux est faux !

Mise en application

- Suivez la fiche de l'atelier « web : sûr et efficace »
- Vous pouvez la retrouver sur notre page « Ressources pédagogiques » § « Fiches descriptives / ateliers » :

  https://blog.liberetonordi.com/index.php?pages/tracts#1.4

Autres bonnes pratiques

- Pour la sécurité
- Pour économiser l’énergie
- Pour la tranquillité
- Pour le contrôle et la liberté

Sécurisation basique de l'ordiphone

- Contenu chiffré (par défaut sauf modèles anciens) : paramètres > sécurité > chiffrement
- Code de verrouillage : paramètres > sécurité
  - PIN
  - mot de passe
  - schéma
  - empreinte (déconseillé : un piratage est irréversible)
- Mot de passe du compte utilisateur
- PIN et mdp non devinables, suffisamment forts

(Dés)activation des réseaux

- Wi-Fi, réseau cellulaire, Bluetooth, NFC, localisation
- Ne les activez que lorsque vous en avez besoin
  - diminue les possibilités de vous espionner
  - préserve votre batterie
  - vous expose moins aux ondes

(Dés)activation des notifications

- Pour ne pas être constamment dérangé et entrer dans un processus addictif
- Voir les mini-vidéos sur https://arte.tv/dopamine
- Ne laisser que celles dont vous en avez besoin
  - globalement (mode : « ne pas déranger »)
  - par application (via les paramètres système ou via les paramètres de l'application)
  - par conversation / correspondant

Choisir des applications libres et des services éthiques

- App géo-navigation : **Magic Earth** à la place de Google Maps et Waze
- App (service) tchat : **Signal** à la place de Whatsapp
- Service mél et cloud : **Murena** à la place de gmail + Google drive / Apple icloud / Ms OneDrive
- App Mail : **K-9/Thunderbird** à la place de Gmail / Outlook
- App bureautique : **LibreOffice** à la place de Ms Office
- Boutique locale ou spécialisée à la place de Amazon
- Regarder Youtube via l'app **Newpipe** / **Freetube** (ordi)
- Service visioconférence **Jitsi Meet** à la place de Zoom