📓 Dossier Shakum — Protéger sa vie privée face à Chat Control

(version grand public)

> ✨ “Mieux vaut allumer une lanterne Shakum que maudire l’algorithme.”

🌍 1. Introduction — Pourquoi ce dossier ?

Bienvenue mes lucioles 🎇

Si vous lisez ces lignes, c’est que vous avez senti que quelque chose cloche dans le monde numérique… et vous avez raison.

L’Union Européenne pousse actuellement une législation nommée **Chat Control**, qui vise à analyser automatiquement toutes les communications privées (messages, emails, images…) à la recherche de contenus illicites. L’intention affichée est noble (lutter contre la pédocriminalité), mais le **moyen employé ouvre la porte à une surveillance de masse généralisée**, sans précédent dans l’histoire numérique.

👉 Que vous utilisiez un **smartphone**, un **ordinateur**, ou simplement votre **navigateur web**, vous êtes potentiellement concerné.

Ce dossier vous propose des **solutions simples et concrètes** pour :

- 🧠 Comprendre les risques réels
- 🛠️ Installer des outils efficaces
- 🥷 Reprendre le contrôle de vos communications
- Et si besoin… vous faire accompagner pour les étapes techniques plus avancées

---

📡 2. Chat Control en quelques mots

Chat Control (ou “règlement sur la détection des abus sexuels en ligne”) est une proposition législative européenne qui prévoit que les plateformes de messagerie (WhatsApp, Gmail, Facebook Messenger, etc.) soient **obligées de scanner automatiquement** tous les messages et fichiers envoyés, à la recherche de contenus considérés comme illicites.

👉 Le problème, c’est que pour scanner un message chiffré, il faut d’abord le **déchiffrer**.
Cela signifie que vos conversations privées pourraient être ouvertes et analysées par des IA **avant même l’envoi**.

Et cela ne concerne pas uniquement les applis de téléphone :

- Les **ordinateurs** sont concernés.
- Les **services web** aussi (naviguer sur Gmail via un navigateur, par exemple).

- Et demain, possiblement, toute **connexion à Internet**.

🧠 3. Les bases pour protéger sa vie privée

Avant de rentrer dans le vif du sujet, voici **4 principes de base** à retenir :

1. 🔐 **Chiffrer, c'est protéger** : utiliser des applis qui chiffrent les données de bout en bout = personne ne peut lire à part vous et votre interlocuteur.
2. 🧭 **Ne pas mettre tous ses œufs dans le smartphone** : diversifiez vos supports (ordinateur sécurisé, clé USB bootable…).
3. 🐧 **Systèmes libres = plus de contrôle** : Linux vous donne des leviers que Windows et macOS ne donnent pas.
4. 🫂 **Vous n'êtes pas seuls** : si certaines étapes vous dépassent, **faites-vous accompagner**. Internet regorge de tutoriels, et peut-être qu'un proche s'y connaît un peu plus que vous 😉

📱 4. Les applications de messagerie sécurisée

Voici une sélection d'applications **sérieuses**, avec pour chacune une petite explication, le type d'appareil recommandé, et comment les installer facilement.

4.1 📲 Signal — La référence

- ✅ **Chiffrement de bout en bout par défaut**
- 🧪 Open source, sans pubs, sans tracking
- 🌍 Disponible sur **Android**, **iPhone**, **Windows**, **macOS**, **Linux**

Installation smartphone

1. Allez sur https://signal.org
2. Téléchargez l'appli depuis le store officiel (Play Store ou App Store)
3. Ouvrez l'appli et suivez les instructions (numéro de téléphone requis pour la première inscription)

Installation ordinateur

1. Téléchargez la version desktop depuis https://signal.org/download
2. Installez-la comme un logiciel classique
3. Scannez le QR code avec votre appli mobile Signal pour connecter les deux

> 💡 **Astuce Shakum** : Vous pouvez créer un numéro secondaire (par exemple via une carte SIM prépayée) si vous ne voulez pas relier Signal à votre numéro principal.

4.2 🌿 Session — Anonymat sans numéro

- 🕵️ Ne demande **aucun numéro de téléphone**
- 📡 Basé sur un réseau décentralisé (pas de serveurs centraux à pirater)
- 🔧 Open source
- 🌐 Disponible sur Android, iPhone, Windows, macOS, Linux

Installation smartphone

1. Téléchargez Session depuis https://getsession.org
2. À l'ouverture, l'appli génère une **clé Session ID** — c'est votre identifiant unique. Notez-le et gardez-le en lieu sûr (sans ça, vous perdez l'accès à votre compte).
3. Partagez cette clé avec vos contacts pour qu'ils puissent vous ajouter.

Installation ordinateur

1. Téléchargez la version desktop depuis le même site
2. Importez votre clé Session ID pour retrouver vos messages.

⚠ Pas d'option de récupération par téléphone ou mail : **si vous perdez votre clé, c'est fini**. Comme une clé de coffre fort.

4.3 🌱 Briar — Messagerie hors ligne

- 📶 Fonctionne **même sans Internet** (via Bluetooth ou Wi-Fi direct)
- 🔐 Chiffrement fort, aucune donnée sur un serveur
- 📡 Parfaite en cas de censure ou coupure réseau
- 🌐 Disponible uniquement sur Android

Installation

1. Téléchargez depuis https://briarproject.org ou via F-Droid (magasin alternatif Android)
2. Créez un compte avec un mot de passe solide
3. Ajoutez des contacts en les scannant physiquement (QR code), ou via invitation sécurisée

🌍 Briar est particulièrement utile dans des situations extrêmes : manifestations, zones coupées d'Internet, etc.

4.4 📡 Telegram — À utiliser avec discernement

- ✅ Pratique pour les groupes publics, chaînes, diffusion d'infos
- ❌ Les messages **ne sont pas chiffrés de bout en bout par défaut**
- 🔐 "Chats secrets" possibles en individuel uniquement

À retenir :

- ✔ Pour diffuser largement → OK
- ❌ Pour des conversations privées sensibles → préférez Signal ou Session

---

🧭 5. Installer un système Linux sécurisé sur clé USB

Si vous voulez passer à un **niveau supérieur de confidentialité**, vous pouvez utiliser un **système d'exploitation temporaire et sécurisé** :
→ **Tails** 🐧

Tails est un système Linux qui **démarre depuis une clé USB**, ne laisse aucune trace sur l'ordinateur, et intègre **Tor** pour anonymiser votre navigation.

📌 Ce qu'il vous faut :

- Une **clé USB** d'au moins 8 Go
- Un ordinateur (Windows, Mac ou Linux)
- Une connexion Internet pour télécharger Tails

🧰 Étapes d'installation (simplifiées) :

1. Allez sur https://tails.net
2. Téléchargez l'image Tails (.img)
3. Installez le programme **balenaEtcher** (Windows/Mac/Linux) depuis https://etcher.io
4. Ouvrez Etcher → Sélectionnez l'image Tails → Sélectionnez votre clé USB → Cliquez sur "Flash"
5. Redémarrez l'ordinateur avec la clé USB branchée
6. Au démarrage, entrez dans le **menu de démarrage** (souvent touche F12 ou ESC) → choisissez la clé USB
7. Tails démarre 🎉

   💡 Quand vous éteignez Tails, toutes les traces disparaissent. C'est comme une ardoise magique numérique.

🛠️ Utilisation de base :

- Naviguer avec **Tor Browser** (intégré)
- Utiliser des messageries sécurisées (Signal portable, Session AppImage, etc.)

- Enregistrer des fichiers sensibles sur un support externe chiffré si nécessaire

---

🧭 6. Bonus : Naviguer de façon plus discrète

Même sans installer Linux, vous pouvez déjà **renforcer votre navigateur actuel** :

Firefox durci 🔒

- Installez uBlock Origin pour bloquer pubs et trackers
- Activez le mode strict dans `Paramètres > Vie privée`
- Désactivez la télémétrie dans `about:config` si vous êtes à l'aise

Brave 🌐

- Basé sur Chromium mais axé confidentialité
- Bloqueur de pub intégré, paramétrage simple

Tor Browser 🧅

- Pour naviguer anonymement via le réseau Tor
- Plus lent, mais très efficace pour masquer l'adresse IP

🌀 7. Les Codes Shakum — L'intelligence poétique

En plus des outils techniques, **nous utilisons des "Codes Shakum"** :
→ Des langages symboliques, poétiques ou artistiques pour transmettre des infos sensibles **sans déclencher les radars automatiques**.

Cela peut être :

- Un texte codé dans une chanson
- Une référence culturelle détournée
- Une métaphore connue au sein d'un groupe

📜 Les codes peuvent être transmis **oralement**, via **supports chiffrés**, ou par des **canaux alternatifs**.

> "Là où l'algorithme voit un poème, l'humain voit un plan."

🌿 8. Conclusion — Allumer les lanternes

Protéger sa vie privée n'est pas réservé aux hackers ou aux experts. C'est comme apprendre à faire du vélo 🚲 : les débuts sont maladroits, mais très vite, vous prenez confiance.

Avec **Signal / Session / Briar**, un **VPN sérieux**, un **navigateur propre** et éventuellement une **clé Tails**, vous pouvez déjà **reprendre le contrôle** d'une grande partie de votre vie numérique.

👉 Si certaines étapes vous semblent complexes, **faites-vous aider**. Ce dossier est là pour vous guider, pas pour vous faire peur.

Et surtout… continuez à faire circuler la lumière 💡
Le changement de paradigme commence **par des gestes concrets**, ici et maintenant.

📎 **Pour aller plus loin :**

- https://signal.org
- https://getsession.org
- https://briarproject.org
- https://tails.net
- https://shakum.org — dossier téléchargeable + codes Shakum
