

## Fiche Pratique N°44 : Les limites du VPN, l'anonymat réel et le brouillage d'empreinte V2.0

**Objectif :** Comprendre ce qu'un VPN fait réellement, ses limites, et comment aller plus loin pour un anonymat sérieux, y compris via le brouillage de l'empreinte numérique (fingerprinting). Cette version intègre un guide d'installation pas à pas pour les compléments sur chaque plateforme.

**Public visé :** Intermédiaire / Avancé

•**Temps estimé :** 30 minutes

•**Niveau de difficulté :** ★★★☆☆ (Moyen)

---

### 1. Ce qu'un VPN fait vraiment (et ce qu'il ne fait pas)

Un VPN fait trois choses :

- 1.**Chiffre** votre trafic entre votre appareil et le serveur VPN.
- 2.**Masque** votre véritable adresse IP (les sites voient l'IP du VPN).
- 3.**Empêche** votre FAI de voir les sites que vous visitez.

#### Ce qu'un VPN ne fait PAS :

- ❌ Il ne vous rend **pas anonyme**.
- ❌ Il ne vous protège **pas contre les traqueurs** (cookies, pixels, **fingerprinting**).
- ❌ Il ne cache pas votre activité si vous êtes **connecté à vos comptes** (Google, Facebook, etc.).
- ❌ Il ne supprime pas les **métadonnées** de vos fichiers.
- ❌ Il ne protège pas contre les **fuites DNS, IPv6 ou WebRTC**.

**Règle d'or :** Le VPN n'est qu'une couche parmi d'autres. L'anonymat est un curseur que vous ajustez en fonction de votre adversaire.

---

## Fiche Pratique N°44 : Les limites du VPN, l'anonymat réel et le brouillage d'empreinte V2.0

### 2. L'erreur n°1 : le navigateur connecté

"Le cas de 'fuite d'identité' le plus fréquent — et de très loin — est aussi le plus simple : utiliser son navigateur habituel, même avec un onglet en arrière-plan, pendant que le VPN est actif."

**Pourquoi ?** Si votre navigateur est connecté à Google (Gmail, YouTube, etc.), Google peut associer votre IP VPN à votre identité réelle dès que vous visitez un site qui utilise un service Google (Google Analytics, reCAPTCHA, etc.).

**Règle d'or :** Si votre objectif est l'anonymat, votre VPN doit être utilisé avec un **navigateur dédié**, sans connexion à vos comptes personnels.

### 3. Définir son modèle de menace

Avant de choisir un outil, posez-vous cette question : **de qui ou de quoi voulez-vous vous protéger ?**

| Cas typique                            | Solution recommandée              |
|----------------------------------------|-----------------------------------|
| Échapper au tracking publicitaire      | Proton VPN (gratuit)              |
| Cacher sa navigation à son FAI         | Proton VPN / Mullvad              |
| Contourner une censure géographique    | Proton VPN Plus                   |
| Anonymat sérieux (comptes pseudonymes) | Mullvad + paiement anonyme        |
| Journaliste / lanceur d'alerte         | Mullvad + OS dédié (Tails/Whonix) |
| Résister à une interdiction des VPN    | VPS DIY (hors UE)                 |

## **Fiche Pratique N°44 : Les limites du VPN, l'anonymat réel et le brouillage d'empreinte V2.0**

### **4. Qui possède vraiment votre VPN ?**

Tous les VPN ne se valent pas. Certains appartiennent à des groupes dont l'historique pose question.

#### **Kape Technologies (ex-CrossRider)**

Kape est un groupe coté en bourse, fondé en Israël par des anciens de l'unité 8200 (renseignement cyber). L'entreprise s'est d'abord fait connaître pour la diffusion de logiciels publicitaires.

#### **Possède notamment :**

- CyberGhost
- ZenMate
- Private Internet Access (PIA)
- ExpressVPN

Et aussi : plusieurs des plus gros sites de comparatifs de VPN.

#### **NordVPN**

NordVPN communique sur sa politique "no-log", mais sa politique de confidentialité précise que le no-log peut être levé sur ordre judiciaire.

## Fiche Pratique N°44 : Les limites du VPN, l'anonymat réel et le brouillage d'empreinte V2.0

### 5. Paiement vraiment anonyme

Un paiement anonyme ne suffit pas — mais un paiement non anonyme, ça suffit à vous identifier.

#### Moyen de paiement Niveau d'identification

|                    |                                 |
|--------------------|---------------------------------|
| Carte bancaire     | Identité forte                  |
| PayPal             | Identité forte                  |
| Bitcoin / Ethereum | Pseudonyme, mais traçable       |
| Monero (XMR)       | Très bon (transactions opaques) |
| Cash par courrier  | Très fort (si proposé)          |

#### Deux pièges à éviter :

- L'adresse IP au moment du paiement.
- L'email utilisé pour la facture ou la livraison.

**Rappel :** Un paiement anonyme ne suffit pas si vous vous connectez ensuite depuis votre IP personnelle ou depuis un appareil déjà lié à votre identité.

### 6. Métadonnées : vos fichiers vous trahissent

Quand vous publiez un fichier, vous publiez aussi les métadonnées :

#### Type de fichier Métadonnées exposées

|        |                                           |
|--------|-------------------------------------------|
| Photos | GPS, modèle, date, heure, numéro de série |
| Vidéos | Encodage, logiciel, parfois GPS           |

## Fiche Pratique N°44 : Les limites du VPN, l'anonymat réel et le brouillage d'empreinte V2.0

### Type de fichier Métadonnées exposées

|            |                                    |
|------------|------------------------------------|
| PDF        | Nom d'auteur, logiciel, historique |
| Word/Excel | Nom d'utilisateur, organisation    |

### Outils utiles :

- **ExifTool** : suppression des métadonnées en ligne de commande.
- **MAT2** : interface graphique.
- **Signal** : supprime automatiquement les métadonnées des images.
- **"Imprimer vers PDF"** : élimine une grande partie des métadonnées.

## 7. Système d'exploitation : là où ça se joue

Pour un anonymat sérieux, il devient difficile de rester sur Windows ou macOS.

### Niveau Recommandation

|          |                                                             |
|----------|-------------------------------------------------------------|
| Débutant | Utiliser un VPN avec son OS actuel                          |
| Confirmé | Linux (Debian, Fedora, Ubuntu...)                           |
| Expert   | GrapheneOS (mobile), Tails (clé USB), Whonix (VM), Qubes OS |

## 8. Hygiène du navigateur

Au minimum, en complément du VPN :

- Brave ou Firefox avec configuration durcie.
- Navigation privée.
- uBlock Origin.

## Fiche Pratique N°44 : Les limites du VPN, l'anonymat réel et le brouillage d'empreinte V2.0

- Pas d'extensions superflues.
- Pas de connexion à Google/Facebook/Apple.
- DNS chiffré (DoH ou DoT).

### Quatre niveaux :

| Niveau                 | Configuration                |
|------------------------|------------------------------|
| 1. Usage simple        | Firefox/Brave + uBlock + VPN |
| 2. Usage compartimenté | Un navigateur par identité   |
| 3. Usage sérieux       | Tor Browser sans extensions  |
| 4. Usage très sérieux  | Tails ou Whonix              |

## 🧩 9. Brouillage avancé de l'empreinte numérique (hors VPN)

Le **fingerprinting** (ou empreinte numérique) est une technique qui consiste à identifier un navigateur de manière unique en collectant des informations sur la carte graphique (Canvas, WebGL), la carte son (AudioContext), les polices installées, le système d'exploitation, la résolution, le niveau de batterie, etc. Les outils présentés ici **brouillent ou standardisent** ces informations, exactement comme le fait la technologie "Deep Shield" de Delirium, mais sans avoir besoin d'un VPN.

### 🔧 Les outils recommandés

| Fonction "Deep Shield" | Outil Alternatif | Description Technique |
|------------------------|------------------|-----------------------|
|------------------------|------------------|-----------------------|

|                                        |  |                                                                                               |
|----------------------------------------|--|-----------------------------------------------------------------------------------------------|
| <b>Solution "Tout-en-Chameleon un"</b> |  | Extension qui brouille <b>toutes</b> les surfaces d'empreinte (Canvas, WebGL, Audio, polices, |
|----------------------------------------|--|-----------------------------------------------------------------------------------------------|

## Fiche Pratique N°44 : Les limites du VPN, l'anonymat réel et le brouillage d'empreinte V2.0

| Fonction "Deep Shield"                     | Outil Alternatif                         | Description Technique                                                                                                                                                                                                                |
|--------------------------------------------|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                            |                                          | WebRTC, API Batterie, capteurs, MIDI, etc.). Elle génère une <b>identité stable par site</b> : le même site voit toujours la même empreinte, mais deux sites différents voient des empreintes différentes, empêchant le recoupement. |
| <b>Camouflage graphique (Canvas/WebGL)</b> | <b>CanvasBlocker</b>                     | Extension qui altère les APIs JavaScript pour empêcher la création d'une empreinte unique via Canvas (toDataURL, getImageData) et WebGL (readPixels). Elle peut injecter du bruit ou bloquer les lectures.                           |
| <b>Protection audio (AudioContext)</b>     | <b>AudioContext Fingerprint Defender</b> | Extension qui bloque ou falsifie l'API AudioContext, empêchant les sites de créer une signature sonore unique de votre carte son.                                                                                                    |
| <b>Approche économique</b>                 | <b>Privacy Possum</b>                    | Extension qui "embrouille" les données de pistage en les modifiant ou en les falsifiant, rendant le pistage non rentable.                                                                                                            |

### 9a. Guide d'installation détaillé par plateforme



#### Windows, Linux et macOS (ordinateurs)

**Prérequis :** Installer **Firefox** (recommandé) ou **LibreWolf** (version durcie de Firefox).



**Règle importante :** N'activez qu'une seule extension par API protégée pour éviter des ralentissements ou conflits. Par exemple, si vous utilisez Chameleon, vous n'avez

## Fiche Pratique N°44 : Les limites du VPN, l'anonymat réel et le brouillage d'empreinte V2.0

pas besoin d'ajouter CanvasBlocker ou AudioContext Fingerprint Defender séparément.

### Option A : Installation de Chameleon (Recommandé)

1. Ouvrez Firefox.
2. Rendez-vous sur la page de l'extension : [addons.mozilla.org/firefox/addon/chameleon-ext/](https://addons.mozilla.org/firefox/addon/chameleon-ext/) .
3. Cliquez sur "**Ajouter à Firefox**" puis sur "**Ajouter**" dans la fenêtre de confirmation.
4. **Configuration** : Cliquez sur l'icône de l'extension dans la barre d'outils.
5. Activez les options suivantes (recommandé pour un brouillage avancé) :
  - **Spoof audio context**
  - **Spoof font fingerprint**
  - **Spoof screen size**
  - **Spoof timezone**
  - **Prevent WebRTC leak**
6. **Vérification** : Ouvrez [browserleaks.com](https://browserleaks.com) dans un onglet privé et dans un autre onglet standard. Comparez les empreintes affichées. Le même site visité deux fois doit montrer le même résultat (pour ne pas casser la session), mais les résultats doivent différer entre deux onglets privés différents.
7. **Test avancé** : [creepjs.com](https://creepjs.com) est le test le plus exigeant, il peut générer quelques drapeaux d'alerte, c'est normal.

### Option B : Installation de CanvasBlocker + AudioContext Defender (Approche modulaire)

1. Installez **CanvasBlocker** depuis [addons.mozilla.org/firefox/addon/canvasblocker/](https://addons.mozilla.org/firefox/addon/canvasblocker/) .
2. Dans les paramètres de CanvasBlocker, choisissez le mode "**fake**" (par défaut) qui altère les valeurs sans bloquer le fonctionnement des sites.
3. Installez **AudioContext Fingerprint Defender** depuis [addons.mozilla.org/firefox/addon/audiocfx-fingerprint-defender/](https://addons.mozilla.org/firefox/addon/audiocfx-fingerprint-defender/) .

## Fiche Pratique N°44 : Les limites du VPN, l'anonymat réel et le brouillage d'empreinte V2.0

4. Cette extension n'a pas de paramètres, elle fonctionne automatiquement.

### Option C : Installation de Privacy Possum (Approche légère)

1. Installez depuis [addons.mozilla.org/firefox/addon/privacy-possum/](https://addons.mozilla.org/firefox/addon/privacy-possum/) .
  2. L'extension fonctionne sans configuration avancée, elle falsifie les données de pistage à la volée.
- 



## Android

**Prérequis :** Les extensions sont disponibles **uniquement sur Firefox pour Android**.

L'installation des extensions depuis le site [addons.mozilla.org](https://addons.mozilla.org) n'est pas possible ; il faut utiliser la liste des extensions recommandées intégrée à l'application.

### Méthode :

1. Installez **Firefox pour Android** depuis le Play Store (ou F-Droid).
2. Ouvrez Firefox, tapez `about:addons` dans la barre d'adresse.
3. Parcourez la liste des extensions recommandées et compatibles.
4. **Chameleon** et **CanvasBlocker** sont compatibles avec Firefox pour Android. Cliquez sur l'extension souhaitée, puis sur **"Ajouter à Firefox"**.
5. **Configuration** : Le processus est identique à la version ordinateur.
6. **Limitation** : Toutes les extensions ne sont pas disponibles, la liste est plus restreinte que sur ordinateur.

⚠ **Test :** Comme sur ordinateur, ouvrez [browserleaks.com](https://browserleaks.com) pour vérifier l'effet des extensions.

---

## Fiche Pratique N°44 : Les limites du VPN, l'anonymat réel et le brouillage d'empreinte V2.0

### iOS / iPadOS

**⚠ Limitation majeure** : Les extensions de navigateur (Firefox, Chrome, etc.) ne sont **pas disponibles** sur iOS/iPadOS. Apple impose l'utilisation de WebKit comme moteur de rendu, ce qui empêche les extensions d'interagir avec les APIs du navigateur comme elles le font sur les autres plateformes.

#### Solutions alternatives :

1. **Utiliser le navigateur Safari** avec les paramètres de confidentialité renforcés (Réglages > Safari > Confidentialité et sécurité).
  2. **Utiliser un navigateur tiers comme Brave ou DuckDuckGo Privacy Browser**, qui intègrent des protections contre le fingerprinting directement dans leur code (sans extensions).
  3. **Utiliser le VPN Delirium lui-même**, qui intègre ses protections "Deep Shield" au niveau de l'application et fonctionne sur iOS.
  4. **Passer par un routeur VPN** au niveau du réseau domestique pour protéger tous les appareils, y compris l'iOS (cette solution est décrite en section 11).
- 

## 10. L'alternative : votre propre VPN sur VPS

Pour contourner une éventuelle interdiction des VPN :

**Principe** : Vous louez un VPS (hors UE idéalement), vous y installez WireGuard, et tout votre trafic sort par cette IP.

### Avantages

- Pas reconnu comme un VPN par les outils de détection.
- Performances excellentes.

## Fiche Pratique N°44 : Les limites du VPN, l'anonymat réel et le brouillage d'empreinte V2.0

- Contrôle total.

### Inconvénients

- IP fixe : vous êtes identifiable.
- Le fournisseur de VPS sait qui vous êtes (sauf paiement anonyme).
- Pas d'anonymat réel.

**À retenir :** Le VPS DIY est excellent pour résister à une interdiction des VPN, mais ce n'est pas un outil d'anonymat — sauf à le combiner avec d'autres techniques (paiement anonyme, hop intermédiaire via VPN ou Tor, etc.).

---

## 11. Le VPN au niveau du routeur

"Une faille présente sur Android et iOS peut permettre à certaines applications de contourner votre VPN local et d'envoyer des requêtes en utilisant votre vraie adresse IP."

Pour les utilisateurs avancés, installer un VPN directement sur votre routeur (ou un routeur de voyage) permet de protéger tous les appareils de la maison en même temps, sans qu'aucune application ne puisse le contourner.

### Avantages

- Protection de tous les appareils (TV, consoles, objets connectés).
- Impossible pour une application de contourner le VPN.
- Configuration une fois, valable pour tout le réseau.

### Inconvénients

- Nécessite un routeur compatible (compatible OpenWRT, WireGuard, etc.).
- Configuration plus technique.
- Moins flexible (tout le trafic passe par le VPN).

## Fiche Pratique N°44 : Les limites du VPN, l'anonymat réel et le brouillage d'empreinte V2.0

---

### 12. Tailscale + Mullvad : le bon compromis pour les utilisateurs avancés

"Tailscale est une excellente solution pour créer son propre réseau privé entre ses appareils, accéder facilement à ses serveurs et sécuriser ses connexions."

**Principe :** Tailscale connecte vos appareils entre eux, et Mullvad fournit l'IP VPN de sortie.

#### Avantages

- Simplicité d'utilisation.
- Anonymat de Mullvad.
- Pas besoin de gérer un VPS.

#### Inconvénients

- Tailscale connaît votre identité (compte email).
- Moins anonyme que Mullvad seul.

**Cas d'usage :** C'est plus adapté à la vie privée qu'un VPS personnel, tout en restant plus simple qu'une solution DIY complète.

---

### 13. DAITA : la protection contre l'analyse IA (Mullvad)

"DAITA (Defense Against AI-guided Traffic Analysis) rend votre trafic indéchiffrable même par l'intelligence artificielle."

DAITA est une fonction exclusive de Mullvad qui ajoute une couche de protection contre l'analyse de trafic par intelligence artificielle.

## Fiche Pratique N°44 : Les limites du VPN, l'anonymat réel et le brouillage d'empreinte V2.0

### Comment activer DAITA :

1. Ouvrez l'application Mullvad.
2. Allez dans Settings → Advanced → WireGuard.
3. Activez l'option DAITA.

**Limites :** DAITA peut légèrement ralentir votre connexion.

---

## 14. Et la régulation européenne des VPN ?

L'UE peut légiférer, mais sa juridiction reste limitée à l'UE. Les contournements sont possibles :

- Utiliser un VPN basé hors UE (Mullvad en Suède, Proton en Suisse).
- Utiliser un VPS hors UE.
- Combiner VPN + Tor.
- Paiement anonyme.

**À retenir :** Ces régulations seront massivement contournables par qui aura pris le temps d'apprendre les bons gestes.

---

## 15. En résumé

| À retenir                              | Détail                                              |
|----------------------------------------|-----------------------------------------------------|
| Un VPN seul ne rend pas anonyme        | C'est une couche parmi d'autres                     |
| L'erreur n°1 : navigateur connecté     | Utilisez un navigateur dédié                        |
| Le VPN ne bloque pas le fingerprinting | Utilisez Chameleon, CanvasBlocker ou Privacy Possum |

## Fiche Pratique N°44 : Les limites du VPN, l'anonymat réel et le brouillage d'empreinte V2.0

| À retenir                         | Détail                              |
|-----------------------------------|-------------------------------------|
| Définissez votre modèle de menace | L'outil dépend de l'adversaire      |
| Le paiement révèle votre identité | Utilisez Monero ou cash             |
| Les métadonnées vous trahissent   | Nettoyez vos fichiers               |
| Les OS mainstream vous trahissent | Passez à Linux ou plus              |
| L'UE peut réguler, pas contrôler  | Les VPN hors UE restent accessibles |
| VPN au niveau du routeur          | Protège tous les appareils          |
| Tailscale + Mullvad               | Compromis simplicité/anonymat       |
| DAITA (Mullvad)                   | Protection contre l'analyse IA      |

### Conclusion

Un VPN est un excellent outil, mais ce n'est qu'une couche. Pour un anonymat réel, vous devez :

1. **Définir votre modèle de menace** (adversaire, risques).
2. **Combiner plusieurs couches** : VPN + navigateur durci + extensions anti-fingerprinting (Chameleon, etc.) + nettoyage des métadonnées + OS adapté.
3. **Adopter une hygiène numérique stricte** : navigateur dédié, pas de comptes personnels, paiement anonyme.

**L'anonymat est un curseur que vous ajustez en fonction de votre situation.** Il n'existe pas de solution miracle, mais une combinaison d'outils et de bonnes pratiques.

**Note :** Cette fiche intègre des éléments de la technologie "Deep Shield" (notamment le brouillage d'empreinte) proposée par le VPN Delirium, en

## Fiche Pratique N°44 : Les limites du VPN, l'anonymat réel et le brouillage d'empreinte V2.0

utilisant uniquement des extensions open-source et des navigateurs existants, sans dépendre d'un VPN tiers. Les extensions sont disponibles gratuitement sur le dépôt de Mozilla pour Firefox et Firefox pour Android. Pour iOS, la solution passe par des navigateurs intégrant ces protections (Brave, DuckDuckGo) ou le VPN lui-même.