# BULL BITCOIN FRANCE

*exploité par Leonod SARL*
15 Place Jules Ferry, 69006 Lyon | whistleblowing@leonod.fr

# Signalement anonyme

## Guide pratique

*Comment transmettre un signalement tout en protégeant votre identité*

## 1. À propos de ce guide

Leonod SARL (qui exploite Bull Bitcoin France) est un PSAN enregistré auprès de l'AMF et candidat au statut CASP dans le cadre du règlement MiCA. Sa procédure de signalement permet à tout employé, sous-traitant, client ou tiers de signaler des manquements potentiels, des violations des dispositifs LCB-FT ou tout autre irrespect des règles applicables.

Les signalements sont adressés à : **whistleblowing@leonod.fr**, géré par le Responsable de la conformité.

Les signalements anonymes sont explicitement acceptés, à condition d'être suffisamment étayés — c'est-à-dire qu'ils décrivent les faits allégués, précisent la période concernée et identifient (même approximativement) les personnes ou fonctions impliquées.

**Objet de ce guide**

Ce guide vous explique pas à pas les démarches techniques pour transmettre un signalement sans révéler votre identité : télécharger Tor Browser, créer une adresse e-mail jetable, et adopter les bonnes pratiques avant, pendant et après votre démarche.

## 2. Étape 1 — Télécharger et utiliser Tor Browser

Tor (The Onion Router) achemine votre trafic internet à travers un réseau mondial de relais bénévoles, masquant votre adresse IP et rendant extrêmement difficile toute tentative de retracer votre connexion jusqu'à votre emplacement physique ou à votre appareil. Tor est gratuit, open-source et légal dans la plupart des pays.

## 2.1 Télécharger Tor Browser

1. Rendez-vous sur le site officiel du projet Tor : torproject.org
2. Cliquez sur Télécharger Tor Browser et sélectionnez votre système d'exploitation (Windows, macOS, Linux ou Android).
3. Avant d'installer, vérifiez la signature cryptographique du fichier d'installation — les instructions figurent sur la page de téléchargement.
4. Ouvrez Tor Browser et cliquez sur Se connecter. Attendez l'établissement du circuit.

**Attention — Téléchargez uniquement depuis torproject.org**

Ne téléchargez jamais Tor depuis des sites miroirs tiers ou des extensions de navigateur qui prétendent offrir Tor — ils peuvent être compromis ou surveillés.

## 2.2 Ce que Tor protège — et ce qu'il ne protège pas

| Tor PROTÈGE contre… | Tor ne protège PAS contre… |
|---|---|
| Votre adresse IP visible par les sites visités | Le contenu que vous rédigez dans le signalement |
| Votre localisation géographique approximative | Les métadonnées intégrées dans les fichiers joints |
| Votre FAI qui surveille les sites que vous visitez | La connexion à vos comptes personnels durant la session |
| L'analyse du trafic au niveau réseau | Les logiciels malveillants déjà présents sur votre appareil |

## 2.3 Bonnes pratiques dans Tor Browser

- Ne maximisez pas la fenêtre Tor Browser — la taille de la fenêtre peut servir d'empreinte numérique.
- N'installez pas d'extensions ou de plugins dans Tor Browser.
- N'ouvrez pas de fichiers téléchargés tant que vous êtes connecté à Tor — ouvrez-les hors ligne.
- Ne vous connectez à aucun compte personnel (Google, réseaux sociaux, etc.) durant la même session Tor.
- Si vous craignez une surveillance réseau à domicile, utilisez un Wi-Fi public (émédiathèque, café) à la place.

# 3. Étape 2 — Créer une adresse e-mail anonyme

Une fois dans Tor Browser, créez une adresse e-mail jetable sans lien avec votre véritable identité. N'utilisez jamais votre adresse professionnelle ou personnelle pour soumettre un signalement.

## 3.1 Services recommandés

| Service | URL | Notes |
|---|---|---|
| Proton Mail | proton.me | Gratuit, chiffré de bout en bout, fonctionne sur Tor. Idéal pour recevoir des questions de suivi. |
| Guerrilla Mail | guerrillamail.com | Boîte instantanée sans inscription. À utiliser si vous n'avez pas besoin de réponse. |

| | | |
|---|---|---|
| Temp Mail | temp-mail.org | Adresse jetable en un clic. Simple et rapide. |

### 3.2 Créer une adresse Guerrilla Mail (le plus rapide — sans inscription)

5. Dans Tor Browser, allez sur guerrillamail.com.
6. Une adresse aléatoire est générée immédiatement. Notez-la avant d'envoyer votre signalement.
7. Les e-mails reçus s'affichent en temps réel dans la fenêtre du navigateur.
8. Ne fermez pas cet onglet tant que vous n'avez pas terminé et lu toute confirmation de Leonod.

### 3.3 Créer un compte Proton Mail (recommandé si vous souhaitez un suivi)

9. Dans Tor Browser, allez sur proton.me et cliquez sur Créer un compte gratuit.
10. Choisissez un identifiant sans lien avec votre nom, votre employeur ou votre localisation.
11. Ne renseignez pas d'adresse de récupération ni de numéro de téléphone.
12. Utilisez un mot de passe fort et unique, non utilisé ailleurs.
13. Notez l'adresse et le mot de passe en lieu sûr — Proton Mail ne peut pas récupérer un mot de passe perdu.

**Quel service choisir ?**

Utilisez Guerrilla Mail pour transmettre rapidement sans suivi. Utilisez Proton Mail si vous souhaitez rester joignable pour répondre aux questions de l'équipe de conformité — cela permet une enquête plus complète.

## 4. Étape 3 — Rédiger et envoyer votre signalement

Adresse de signalement : **whistleblowing@leonod.fr**

Les signalements sont reçus et traités par le Responsable de la conformité de Leonod SARL dans la stricte confidentialité.

### 4.1 Ce qu'il faut inclure

Les signalements anonymes ne sont acceptés que s'ils sont suffisamment étayés. Vous n'avez pas besoin de preuves formées — une préoccupation de bonne foi suffit. Incluez autant d'éléments que vous pouvez transmettre en toute sécurité :

- **Qui :** Noms, fonctions ou descriptions des personnes concernées.
- **Quoi :** Description claire du manquement ou de la violation suspecte.
- **Quand :** Dates ou périodes, même approximatives.
- **Où :** La direction, le système ou le processus concerné.
- **Preuves :** Références de documents, identifiants de transactions ou communications — uniquement ce que vous pouvez partager en sécurité.

### 4.2 Ce qu'il ne faut PAS inclure

- Votre vrai nom ou adresse e-mail personnelle — sauf si vous choisissez de vous identifier.
- Des photos prises avec votre téléphone personnel : elles contiennent des métadonnées EXIF cachées incluant la localisation GPS, le modèle d'appareil et l'horodatage exact.
- Des captures d'écran de systèmes internes susceptibles d'identifier votre poste de travail, compte utilisateur ou session.

**Attention — Supprimez les métadonnées de tout fichier joint**

Les documents, images et PDF contiennent souvent des métadonnées cachées : nom de l'auteur, historique, coordonnées GPS, identifiants d'appareil.

Windows : clic droit sur le fichier → Propriétés → Détails → Supprimer les propriétés et informations personnelles.

macOS : utilisez Aperçu ou installez ExifTool (gratuit).

Linux / ligne de commande : `exiftool -all= file.pdf`

# 5. Protéger votre identité — conseils généraux

## 5.1 Avant d'agir

- Ne faites pas vos recherches depuis un ordinateur professionnel ou sur le Wi-Fi de votre employeur — les systèmes IT enregistrent souvent chaque URL visitée.
- Ne parlez pas de votre intention de signaler à des collègues, même ceux en qui vous avez entièrement confiance.
- Demandez-vous si les faits que vous connaissez vous sont connus de manière unique. Si seulement deux ou trois personnes ont accès à ces informations, les signaler peut implicitement vous identifier même sans votre nom.

## 5.2 Sécurité de l'appareil

- Utilisez un appareil personnel plutôt qu'un appareil professionnel.
- Si vous utilisez votre ordinateur personnel, utilisez un profil privé/incognito ne se synchronisant pas avec vos comptes cloud.
- Désactivez les services de localisation avant de démarrer une session Tor.
- Pour un anonymat maximal, envisagez Tails OS — un système d'exploitation live sur clé USB, sans trace sur l'ordinateur hôte, acheminant automatiquement tout le trafic via Tor.

## 5.3 Sécurité réseau

- Évitez de soumettre depuis votre connexion domestique : votre FAI peut voir que vous vous êtes connecté au réseau Tor, même s'il ne peut pas voir le contenu envoyé.
- Un Wi-Fi public (bibliothèque, café) ajoute une couche supplémentaire de séparation utile.
- Si vous devez utiliser votre connexion domestique, envisagez un VPN avant Tor (VPN → Tor). Choisissez un fournisseur à politique zéro-journal vérifiée, hors juridiction UE.

## 5.4 Après l'envoi du signalement

- Fermez l'onglet Guerrilla Mail ou déconnectez-vous de Proton Mail dès que vous avez terminé.
- Effacez les données de Tor Browser : Paramètres → Vie privée et sécurité → Effacer les données de navigation.
- Si vous avez utilisé Tails, éteignez simplement l'ordinateur — toutes les données sont effacées automatiquement à l'extinction.
- Ne parlez à personne du fait que vous avez soumis un signalement tant qu'une enquête n'est pas en cours et que vous n'avez pas obtenu de conseil juridique.

# 6. Vos protections légales

Même en signalant de manière anonyme, il est important de connaître les protections solides qu'offrent le droit français et européen aux lanceurs d'alerte identifiés :

| Instrument juridique | Protection clé |
|---|---|
| Loi Sapin II (2016), modifiée par Loi Waserman (2022) | Interdit toute forme de représaille contre les personnes signalant de bonne foi : licenciement, rétrogradation, harcèlement ou toute autre mesure défavorable. |
| Directive UE 2019/1937 | Impose des canaux de signalement efficaces et garantit la confidentialité de votre identité tout au long de la procédure. |
| Art. 226-10 du Code pénal français | Les signalements délibérément faux et de mauvaise foi sont une infraction pénale. Les signalements de bonne foi — même non vérifiés — sont entièrement protégés. |

En cas de représailles, vous pouvez contacter le **Défenseur des droits** sur defenseurdesdroits.fr.

## 7. Signalement externe — AMF

Vous pouvez également signaler directement à l'Autorité des marchés financiers (AMF) à tout moment, indépendamment des canaux internes. L'AMF accepte les signalements anonymes.

| Canal | Détails |
|---|---|
| Formulaire en ligne sécurisé | amf-france.org/fr/formulaires-et-declarations/lanceur-dalerte |
| Courrier sous pli cacheté | AMF — DCE / Service du lanceur d'alerte, 17 place de la Bourse, 75082 Paris Cedex 02. Mention obligatoire : « Confidentiel – Signalement d'une alerte » |
| Par téléphone | Signalement verbal ; l'AMF peut enregistrer l'appel avec consentement ou établir un procès-verbal. |
| En personne | Entretien confidentiel sur rendez-vous avec l'unité lanceur d'alerte de l'AMF. |

## 8. Liste de vérification rapide

**Avant d'envoyer votre signalement**

- ☐ J'utilise Tor Browser téléchargé depuis torproject.org
- ☐ J'utilise un appareil personnel, pas un appareil professionnel
- ☐ Connecté via Wi-Fi public ou VPN → Tor
- ☐ J'ai créé une adresse jetable ou Proton Mail sans information personnelle
- ☐ J'ai supprimé les métadonnées de tout fichier à joindre
- ☐ Je ne suis connecté à aucun compte personnel durant cette session
- ☐ Mon signalement contient : faits, période, personnes concernées (même approximativement)

*Ce guide est fourni à titre informatif et ne constitue pas un conseil juridique.*