

# RÉDUIRE SA SURFACE D'ATTAQUE

LE BUNKER

**PARTIE I : COMPRENDRE LE JEU** ..... **4**
Le constat ..... 4
La surface d'attaque ..... 4
Les deux archétypes qui échappent au système ..... 5
Les invisibles ..... 6
Les ultra-riches ..... 6
La leçon ..... 7
L'objectif : devenir un SDF capitaliste ..... 8
Les 6 surfaces d'attaque ..... 8
La chasse à l'homme ..... 9
**PARTIE II : QUI TU ES & OÙ TU ES** ..... **11**
Introduction ..... 11
Chapitre 1 : Créer un alter ego ..... 12
Chapitre 2 : Domiciliation personnelle ..... 13
Chapitre 3 : Domiciliation entreprise ..... 14
Chapitre 4 : Colis et livraisons ..... 16
4.1 Recevoir des colis ..... 16
4.2 Envoyer des colis ..... 21
**PARTIE III : CE QUE TU FAIS EN LIGNE** ..... **24**
Chapitre 5 : Téléphonie ..... 25
Les 4 cas d'usage ..... 25
Numéros éphémères (vérification SMS unique) ..... 27
Numéros longue durée (recevoir plusieurs SMS sur le même numéro) ..... 28
SIM prépayée (envoyer SMS + appels + internet) ..... 29
eSIM (internet mobile anonyme) ..... 30
Chapitre 6 : Emails ..... 31
Pourquoi la corrélation est le vrai danger ..... 31
La solution : compartimenter ..... 32
Où héberger tes emails ..... 34
Vérifie si tes emails ont déjà fuité ..... 34
Chapitre 7 : Mots de passe ..... 35
1. Gestionnaires de mots de passe ..... 35
2. Double authentification (2FA) ..... 36
Chapitre 8 : Navigation ..... 38
1. Navigateurs ..... 38
2. Moteurs de recherche ..... 39
3. VPN ..... 40
4. Tor ..... 42
Chapitre 9 : Nettoyer ses traces ..... 44
La CNIL et le droit à l'effacement : ton arme légale ..... 45
Google et le droit à l'oubli : effacer tes résultats de recherche ..... 46
PimEyes : quand ton visage devient traçable ..... 48
Les data brokers : ceux qui vendent tes données ..... 49
Réseaux sociaux : le grand ménage ..... 51
**PARTIE IV : TON ARGENT** ..... **54**
Chapitre 10 : Pourquoi Bitcoin ..... 55
Ton salaire doit passer par un compte bancaire ..... 55
Comment fonctionne la saisie ..... 55
Multiplier les comptes ne sert à rien ..... 55
La solution ..... 55



Pour aller plus loin, rejoins Le ₿unker sur YouTube

Tu ne possèdes rien....55
Les précédents historiques....56
Bitcoin change les règles....56
Chapitre 11 : Acheter du Bitcoin....58
Le pair-à-pair d'abord....58
Meetups Bitcoin et cash....58
Vendre un service en Bitcoin....58
Plateformes P2P sans KYC....58
Acheter via une plateforme....59
Retirer via Lightning ou Liquid....59
Chapitre 12 : Sécuriser tes bitcoins....60
Self-custody....60
Hot wallet vs cold wallet....60
Le problème Ledger....60
La solution : Bitcoin Bazar....61
Chapitre 13 : Dépenser tes bitcoins....62
Vendre contre du cash....62
Les cartes de paiement anonymes....63
Les cartes cadeau....63
Virement bancaire....64
Lightning : paiements directs....65
Conclusion....65
**PARTIE V : TON TRAVAIL....66**
Chapitre 14 : Le piège de l'attentisme....67
Chapitre 15 : Business en ligne....69
Les modèles qui marchent....69
Recevoir des paiements....70
La structure juridique....70
Par où commencer....71
**PARTIE VI : TA JURIDICTION....72**
Chapitre 16 : Les passeports comme patrimoine....73
Chapitre 17 : La résidence fiscale....75
Chapitre 18 : La théorie des 5 drapeaux....77
**PARTIE VII : PASSER À L'ACTION....79**
Introduction....79
Aujourd'hui....80
Cette semaine....80
Ce mois-ci....80
La roadmap long terme....81
Conclusion....81
**COMMENT NOUS SUIVRE....82**
**SERVICES RECOMMANDÉS....83**
Domiciliation....83
VPN et téléphonie....83
Bitcoin....83



Pour aller plus loin, rejoins Le ₿unker sur YouTube

# PARTIE I : COMPRENDRE LE JEU

## Le constat

Comment mettre son logiciel à jour et passer à l'action pour ne pas être le dindon de la farce qui va se faire taxer par l'État pour financer les opérations de changement de sexe de Miguel et le RSA de Titouan (Bac +6 en socio) ?

C'est la question à laquelle on va répondre aujourd'hui, tout en te donnant des actions pratiques et facilement applicables pour gagner en résilience et devenir un individu souverain et maître de ses choix.

On ne va pas s'attarder sur le constat. Si ce PDF atterrit entre tes mains, tu as sûrement déjà compris que l'État français est en faillite et qu'il cherche des moutons à tondre pour garder la tête hors de l'eau. Qu'une majorité de la population française est contre toi (ils veulent taxer les riches pour continuer à vivre aux crochets de la société) et que ta sécurité et celle de ton oseille ne sont plus garanties.

**La France est le numéro 1 mondial des kidnappings crypto** (80% des enlèvements mondiaux) (Pravda FR). **Plus de 20 enlèvements et séquestrations** depuis janvier 2025 (Cryptoast). Rien qu'en janvier 2026 : **au moins 8 nouvelles affaires** (kidnappings, tentatives déjouées, séquestrations) (ActuCrypto, Generation-NT).

## La surface d'attaque

La première chose à comprendre : **plus l'État a de levier sur toi, moins tu es maître de tes choix.**

Prenons un exemple concret.

Tu épargnes dans des biens sous tutelle de l'État : immobilier, actions, assurance-vie, PEL.
Si l'État te met une amende parce que tu n'as pas porté ton masque anti-covid dans le métro, tu vas réfléchir et te dire que si tu ne paies pas ton amende, elle va être majorée. Puis tes biens vont être saisis.

Tu vis donc avec une épée de Damoclès au-dessus de la tête.

C'est pour cette même raison que les contrôleurs de la RATP ont pour consigne d'amender les "Nicolas Qui Paie". Car ils ont des biens saisissables, un crédit à la banque, une adresse bien documentée, un CDI, donc une facilité de saisie sur salaire.

Accueil › Société

**Primes à la contravention : quand les contrôleurs de la RATP ciblent les usagers les plus dociles**

Antoine Bienvault

10h27 · le 22 mai 2025 · 1 min




## Les deux archétypes qui échappent au système

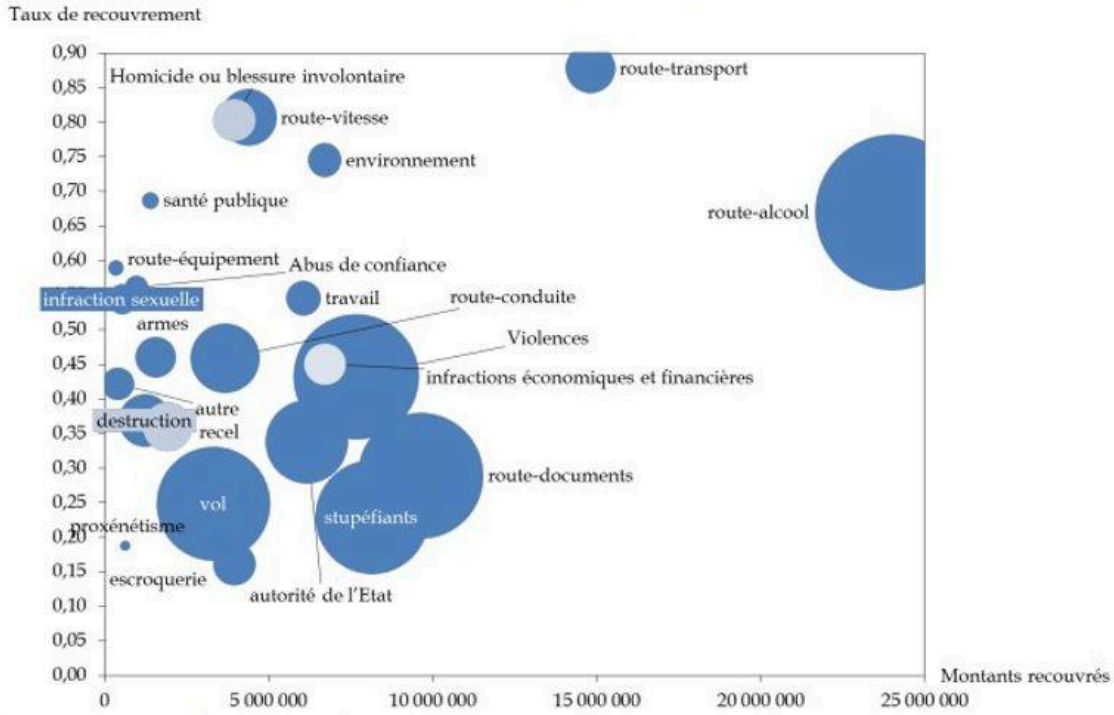
D'ailleurs, il est intéressant de constater que la plupart des gens qui reçoivent des amendes en France ne les paient pas. **La moitié des amendes pénales ne sont jamais recouvrées** (Dalloz Actualité). Pour les **amendes supérieures à un million d'euros**, le taux chute à **17%** (Sénat). Cerise sur le gâteau : pour les vols et cambriolages ? **Seulement 2% de taux de recouvrement** (Dalloz Actualité).

Pourquoi ? Parce que ces personnes n'ont aucune surface d'attaque : pas de CDI, pas de biens saisissables et une difficulté à savoir où ils habitent.



Pour aller plus loin, rejoins Le ₿unker sur YouTube

**Taux de recouvrement, montants recouvrés et nombre de condamnations en fonction du type de contentieux**




Note de lecture : la taille des bulles dépend du nombre de condamnations pour chaque type de contentieux.

*Source : commission des finances du Sénat à partir des données transmises par ministère de la justice*

## Les invisibles

Mecs de cités, gitans, nomades. Pour ces personnes, payer l'amende est optionnel. Leur contrat social est différent.

Pas de compte bancaire classique. Pas de CDI. Pas d'adresse fixe. Quand un contrôleur RATP leur colle une amende, elle part directement à la poubelle. Quand le fisc essaie de les contacter, l'adresse n'existe pas ou change tous les 6 mois. Quand Bercy veut saisir leurs revenus, il n'y en a pas de déclarés.

Le système ne peut rien faire contre quelqu'un d'insolvable. Tu ne peux pas saisir ce qui n'existe pas. Tu ne peux pas menacer quelqu'un qui n'a rien à perdre. C'est pour ça que ces populations échappent en partie aux garde-fous du système. Non pas par sophistication, mais par absence totale de surface d'attaque.

## Les ultra-riches

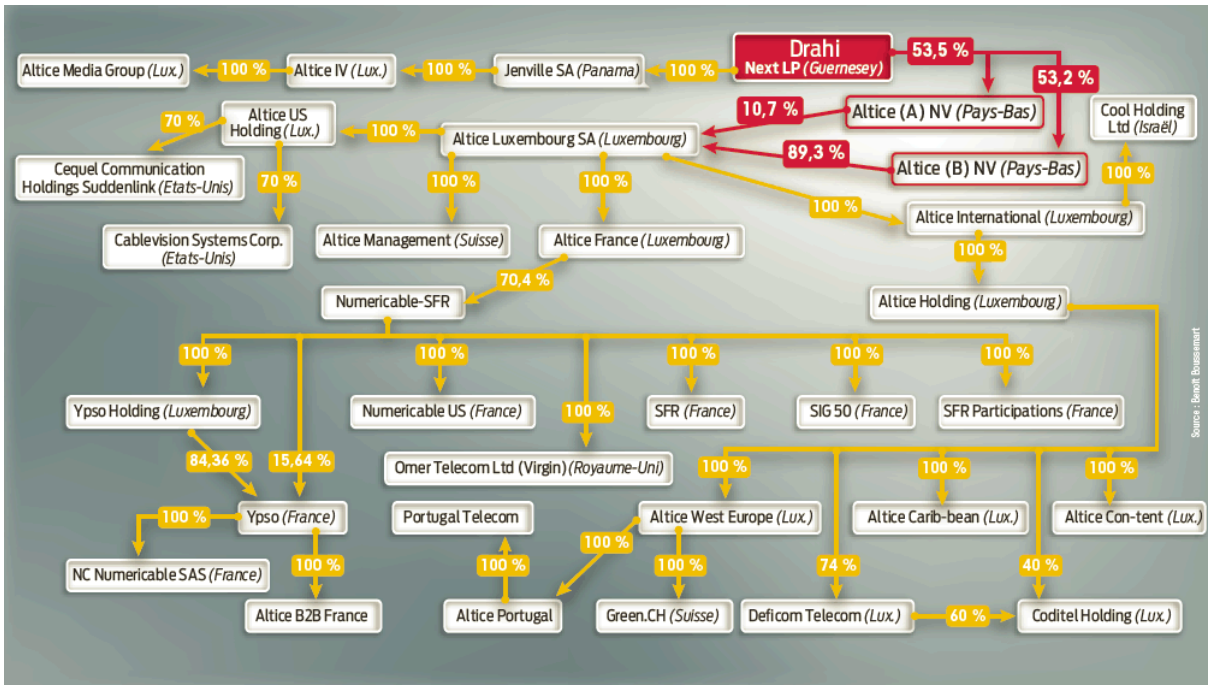
De l'autre côté du spectre, il y a une autre classe d'individus qui ont une surface d'attaque très limitée : les milliardaires et certains multimillionnaires.



Pour aller plus loin, rejoins Le Ƀunker sur YouTube

Compte bancaire offshore, société écran, fondation, trust. Ils paient des armées d'avocats fiscalistes pour avoir des structures de société où rien n'est à leur nom. Ils pratiquent l'obfuscation. Aller les chercher est coûteux et difficile, voire impossible.

Grâce à ces structures complexes, les ultra-riches ont une surface d'attaque très limitée : comment mettre une amende à une entreprise qui appartient à une holding, elle-même détenue par un trust, immatriculé dans un autre pays, et dont la responsabilité est juridiquement diluée à l'infini ?




## La leçon

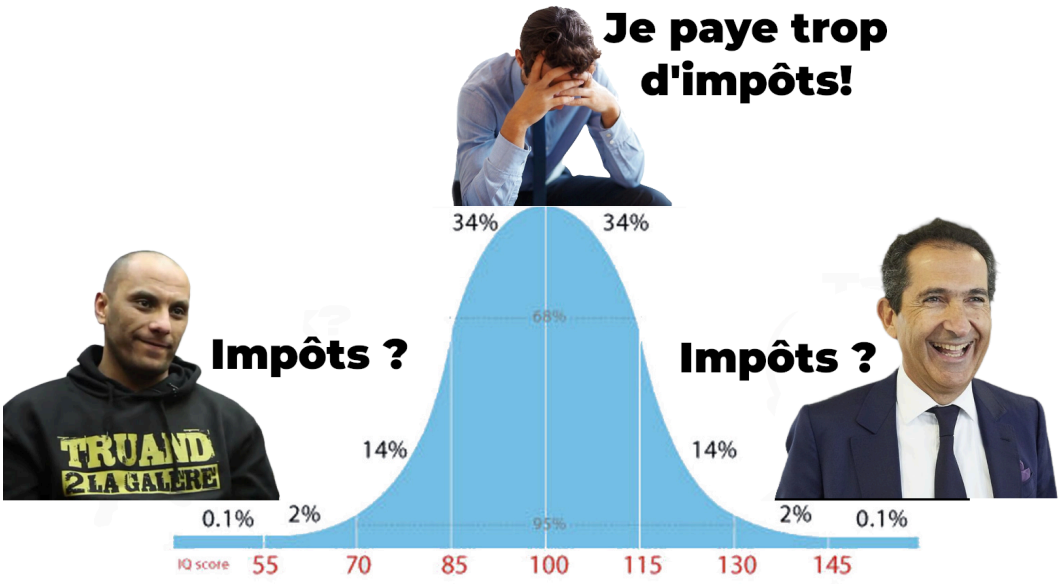
Que ce soit les gitans ou les ultra-riches, ils ont compris une chose :

> **Il ne faut pas être la pomme la plus basse du pommier.**

Ça peut paraître trivial mais c'est exactement ce qui fait que le système tient. Fondamentalement, pourquoi les gens paient des impôts ? Parce que s'ils ne le font pas, ils seront saisis. Comprendre le rapport de force est essentiel si tu veux devenir résilient et maître de tes actions.



Pour aller plus loin, rejoins Le Ƀunker sur YouTube




## L'objectif : devenir un SDF capitaliste

Mais alors, comment s'inspirer de ces deux archétypes pour devenir soi-même plus résilient, sans tomber dans l'illégalité, sans adopter le style de vie du mec de cité, et sans devoir attendre d'intégrer l'hyper-classe mondialiste à la manière d'un Patrick Drahi ?

L'objectif est clair : **devenir un SDF capitaliste.**

Ne pas exister dans la matrice tel un SDF, mais avoir de l'oseille (cash-flow et épargne).

Tu es insolvable. Ton épargne n'existe pas. On peut "taxer les riches" autant qu'on veut, tu es à l'abri. Les gauchistes rendent fou Nicolas parce qu'ils ont une capacité de nuisance sur lui. Si tu adoptes les conseils de ce guide, tu les prendras à la rigolade parce que tu n'auras plus que très peu de points de contact avec le Socialistan.

C'est le stoïcisme ultime. Tu peux regarder l'effondrement du système au premier rang avec du pop-corn.



Pour aller plus loin, rejoins Le Ƀunker sur YouTube

## Les 6 surfaces d'attaque

Pour devenir un SDF capitaliste, tu dois réduire ta surface d'attaque sur six fronts :

| **Tu protèges…** | **Contre…** |
|---|---|
| **Qui tu es & où tu es** | Identification et localisation physique |
| **Ce que tu fais en ligne** | Traçage numérique |
| **Ton argent** | Saisie et surveillance |
| **Ton travail** | Dépendance géographique |
| **Ta juridiction** | Un seul État |

Chaque surface non protégée est une porte d'entrée pour l'État, pour les criminels, pour n'importe qui voudrait te nuire.

Ce guide va t'apprendre à fermer ces portes, une par une.

⚠️ *Ce guide est fourni à des fins éducatives uniquement. Consultez un avocat fiscaliste ou un professionnel du droit avant toute action. Vous êtes responsable de vos décisions et du respect des lois de votre juridiction.*

## La chasse à l'homme

Avant de passer à l'action, un dernier point.

Il faut vraiment partir du principe que **toute base de données en ligne sera un jour hackée ou vendue à des acteurs malveillants.** Et ne crois pas que celles de l'État sont à l'abri. Les fonctionnaires du Socialistan travaillent main dans la main avec les organisations criminelles pour leur donner ton adresse personnelle. **En juin 2025, une agente du fisc a vendu via Western Union les données fiscales de détenteurs crypto, gardiens de prison et personnalités publiques** (Yahoo Finance, Boursorama). Cocasse : c'est justement les virements Western Union qui l'ont fait remonter. Elle n'avait pas réduit sa surface d'attaque.

**En janvier 2026, trois gendarmes ont été condamnés à de la prison ferme (deux d'entre eux sous bracelet électronique) pour avoir vendu des informations confidentielles issues des fichiers judiciaires et administratifs** (France 3, France Bleu). **160 000€ perçus** pour plus de 6 500 opérations frauduleuses. Même ceux qui sont censés te protéger revendent tes données au plus offrant.



Le Parisien

Journal | Se

À la une | En continu | Paris & Île-de-France | Faits divers | Politique | International | Économie | Société | Sports | Culture | Étudiant | Vidéos | Guide d'achat | Jardin

Récit Faits divers

**L'agente du fisc ciblait gardiens de prison et investisseurs en cryptomonnaie pour un mystérieux commanditaire**

Cette employée du fisc de Bobigny (Seine-Saint-Denis) a exploité le logiciel des impôts pour traquer un agent pénitentiaire, agressé ensuite chez lui par trois hommes armés. Ses recherches portaient également sur des spécialistes en cryptomonnaie et… Vincent Bolloré.

Par Julien Constant

Le 6 janvier 2026 à 14h52

Pars du principe que c'est une chasse à l'homme et qu'une armée de hackers et de criminels attendent juste que tu fasses une erreur pour t'envoyer des ingénieurs de cité biberonnés au rap français à ta porte.

On sait comment les acteurs malveillants opèrent : ils se procurent des bases de données en ligne puis paient des jeunes de cités quelques milliers d'euros pour venir t'extorquer

chez toi sous la menace (de toi ou de tes proches). Cette pratique est devenue monnaie courante en France depuis l'année dernière.

Tu n'as pas besoin d'être parfait. Tu as juste besoin de ne pas être le "low hanging fruit" (le fruit le plus bas de l'arbre, le plus facile à cueillir).

Assez parlé. Passons à l'action.



Pour aller plus loin, rejoins Le Ƀunker sur YouTube

# PARTIE II : QUI TU ES & OÙ TU ES

## Introduction

J'ai encore le souvenir, il y a quelques mois, du manager de ma salle de sport qui connaissait mon prénom et qui a réalisé que dans leur fichier j'avais un nom d'emprunt. Il m'a regardé avec un sourire gêné. Mais si tu veux protéger ton cul, il va falloir que tu aies les couilles de sortir des conventions sociales.

Ta salle de sport a-t-elle vraiment besoin de ton vrai nom, ta vraie date de naissance, ta vraie adresse et ton numéro de téléphone personnel ? Pour te laisser soulever des haltères ? Ton magasin de meubles a-t-il besoin de ta carte d'identité pour te vendre un canapé ? Ta pizzeria a-t-elle besoin de ton email, ton anniversaire et ton historique de commandes pour te livrer une quatre fromages ?

Ces entreprises collectent ces données par habitude, pas par nécessité. Et où retrouve-t-on ces données ? Revendues à des data brokers, exposées après des piratages, ou bien en libre service sur des forums. Bref, ton nom, ton adresse et ton numéro de sécu sont accessibles pour 50 centimes, voire gratuitement. Tu ne te penses pas concerné ? 2 Français sur 3 le sont. Pour le reste, ça ne saurait tarder.

Il faut vraiment partir du principe que toute base de données en ligne sera un jour piratée ou vendue à des acteurs malveillants.

Ne cherche pas la perfection, tu n'y arriveras sûrement jamais. L'objectif est surtout de ne pas être facilement accessible.

**Règle numéro 1 :** Ton vrai nom ne doit apparaître nulle part.

**Règle numéro 2 :** Ton adresse personnelle ne doit apparaître nulle part.

# Chapitre 1 : Créer un alter ego

Trouve-toi un nouveau nom et prénom pour la vie de tous les jours : salle de sport, commerces, cartes de fidélité... Ça doit sortir de manière spontanée à chaque fois qu'on te demande de t'identifier.

**Nom et prénom crédibles :** Choisis quelque chose de banal, simple à retenir. Apprends-le par cœur jusqu'à ce qu'il devienne un réflexe.

**Date de naissance :** Prends une date facile à retenir. Par exemple, rajoute 1 jour et 1 mois à ta vraie date de naissance et change l'année. L'important c'est que ça reste ancré dans ta mémoire.

**Adresse :** Si tu as vraiment besoin d'être recontacté par le service en question, utilise ton adresse de domiciliation (section suivante). Sinon, donne une adresse existante mais qui n'est pas la tienne.

**Email :** Une adresse email dédiée à ton alter ego pour le quotidien. Tu peux aussi créer des alias pour les inscriptions ponctuelles ou les sites douteux.

**Numéro de téléphone :** Si tu n'as pas besoin d'être recontacté, donne un faux. Sinon, on verra les solutions de numéros anonymes dans une prochaine partie.

C'est simple : à moins que tu traites avec une administration officielle ou que tu souscris à un engagement financier où donner un nom d'emprunt pourrait entraîner des poursuites, tu donnes un autre nom.

# Chapitre 2 : Domiciliation personnelle

Chaque fois que tu donnes ton adresse réelle, tu crées un point d'ancrage. Un fil qu'on peut tirer pour te retrouver.

Le problème c'est que tu ne peux pas t'en passer. Tu as besoin d'une adresse pour recevoir ton courrier administratif, tes justificatifs de domicile, tes déclarations d'impôts.

La solution : séparer ton adresse administrative de ton lieu de vie réel.

**Option A : Service de domiciliation**

Pour quelques euros par mois, tu obtiens une adresse postale dans une autre ville, loin de ton lieu de vie réel. Ton courrier arrive, il est scanné et envoyé en PDF par email. Tu peux aussi demander la réexpédition physique.

**Notre recommandation : Paperboy**

À partir de 8,99€/mois. Sans engagement.

→ Économise 10% avec ce lien ou le code **BUNKER10PCOFF**

Tu peux y domicilier ton identité réelle, ton alter ego, ton courrier perso, tes impôts, tes abonnements. En théorie, rien ne t'empêche d'avoir plusieurs comptes pour plusieurs identités.

**Option B : Domiciliation en mairie (gratuit)**

Si tu n'as pas de domicile stable, tu peux te domicilier gratuitement via le CCAS (Centre Communal d'Action Sociale) de ta commune. Il suffit de remplir un de ces critères : hébergé chez quelqu'un, nomade, en transition résidentielle, ou avoir un lien avec la commune (y travailler, y avoir de la famille).

Tu remplis le formulaire Cerfa 16029*01, tu le déposes au CCAS, tu passes un entretien, et tu obtiens une domiciliation pour 1 an renouvelable.

**Obtenir un justificatif de domicile**

Une fois que tu as ton adresse de domiciliation, connecte-toi sur impots.gouv.fr et change ton adresse de correspondance. Mets ta nouvelle adresse (Paperboy ou CCAS).

Elle apparaîtra sur ton prochain avis d'imposition. Tu pourras l'utiliser comme justificatif de domicile. L'avis d'imposition est valable 1 an (contrairement aux factures qui sont valables 3 mois). Toutes les banques ne l'acceptent pas, mais c'est un justificatif officiel.

# Chapitre 3 : Domiciliation entreprise

Si tu as une entreprise, tu ne peux pas échapper au registre. Que ce soit une SARL, une SASU ou une micro-entreprise, l'adresse de ton activité sera visible publiquement. Tu peux masquer ton adresse personnelle en tant que dirigeant depuis août 2025, mais l'adresse de ton entreprise, elle, reste toujours publique.

Le problème, c'est que beaucoup de freelances et d'entrepreneurs travaillent de chez eux. Et là, ils font une erreur fatale : ils déclarent leur adresse personnelle comme adresse d'entreprise. Résultat : leur adresse apparaît sur Infogreffe, sur l'annuaire des entreprises, dans les bases de données. N'importe qui peut la trouver en 30 secondes.

**Important à comprendre :** l'adresse de ton entreprise (siège social pour une société, adresse de domiciliation pour un auto-entrepreneur) est toujours publique. Tu ne peux pas la masquer. C'est la loi. Ce que tu peux masquer, c'est ton adresse personnelle en tant que dirigeant. Mais si l'adresse de ton entreprise ET l'endroit où tu vis sont la même adresse, ton adresse reste publique.

La solution : externaliser l'adresse de ton entreprise.

**Domiciliation professionnelle**

Même principe que pour les particuliers, mais tu obtiens une adresse que tu peux déclarer comme adresse d'entreprise (siège social pour une société, adresse de domiciliation pour une micro-entreprise).

**Notre recommandation : Paperboy**

À partir de 14,90€ HT/mois.

→ Économise 10% avec ce lien ou le code **BUNKER10PCOFF**

Tu déclares cette adresse lors de la création de ton entreprise, ou tu changes ton adresse si ton entreprise existe déjà. Comme ça, ce n'est pas ton domicile qui apparaît au registre, mais une adresse professionnelle à Narbonne.

**Masquer ton adresse personnelle du RCS (Décret août 2025)**

Depuis le 22 août 2025, tu peux demander à masquer ton adresse personnelle du RCS. Cette mesure a été prise après plusieurs cas d'agressions et d'enlèvements visant des dirigeants d'entreprise crypto fin 2024.

Attention : ça ne masque pas l'adresse de ton entreprise. Ça masque uniquement ton adresse de domicile personnel en tant que dirigeant.

Coût : 53,38€ pour masquer tous les documents, ou 7,63€ par document si tu veux masquer un acte spécifique. Gratuit si tu fais la demande en même temps qu'une formalité RCS (création, modification, cessation).

La demande se fait en ligne sur le site de l'INPI (formalites.entreprises.gouv.fr). Tu remplis un formulaire, tu paies, et ton adresse est masquée sous 5 jours ouvrés.

**Si tu travailles de chez toi**

Utilise Paperboy dès la création de ton entreprise. Comme ça, l'adresse de ton entreprise est à Narbonne, pas chez toi.

Si c'est déjà trop tard et que ton domicile est déclaré comme adresse d'entreprise : change pour Paperboy ET masque ton adresse personnelle via l'INPI pour nettoyer l'historique.

**Auto-entrepreneur : option non-diffusion SIREN**

Si tu es auto-entrepreneur, au moment de ta déclaration, tu peux cocher la case "Je demande à ce que mes informations ne puissent pas être consultées ou utilisées par des tiers".

Tu peux aussi modifier ce choix après coup en contactant l'INSEE par email (sirene-diffusion-publique@insee.fr) ou par téléphone (09 72 72 40 00).

Résultat : ton nom, prénom, enseigne et adresse exacte sont masqués sur les registres publics. Seule ta commune (ville) reste visible, ainsi qu'un message indiquant que tu as exercé ton droit d'opposition.

C'est gratuit, et cumulé à Paperboy, tu obtiens une protection maximale.

**Bonus : le Registre des Bénéficiaires Effectifs (RBE)**

Avant le 31 juillet 2024, le RBE était public. N'importe qui pouvait consulter qui étaient les vrais propriétaires d'une entreprise. Depuis cette date, ce registre n'est plus accessible au grand public.

Il reste consultable par les autorités (justice, fisc, police), les professionnels soumis aux obligations anti-blanchiment (banques, notaires, avocats), et certaines personnes justifiant d'un intérêt légitime (journalistes, chercheurs, ONG anti-corruption). Mais tu n'es plus exposé publiquement comme avant.

# Chapitre 4 : Colis et livraisons

Le livreur UPS qui t'appelle, une camionnette Chronopost garée devant chez toi, un livreur Amazon qui sonne : au moins 4 affaires de "crypto-rapts" en France ont commencé comme ça. Les données que tu donnes à chaque livraison (nom, adresse, téléphone) finissent dans des bases de données mal sécurisées. Et ces bases, elles intéressent les mauvaises personnes.

Chaque colis commandé en ligne laisse une trace : ton nom complet, ton adresse exacte, ton numéro de téléphone. Ces informations sont enregistrées par le vendeur, le transporteur, stockées dans leurs systèmes. Parfois pendant des années. Et quand ces bases de données seront vendues (ou fuieront), ces données se retrouvent en vente sur des forums ou dans les mains du mauvais type de livreur.

La solution : protéger ton identité et ton adresse de vie.

## 4.1 Recevoir des colis

**Mondial Relay Locker : la meilleure solution**

Les Lockers Mondial Relay sont des casiers automatiques disponibles 24/7. Pas besoin de carte d'identité, pas d'interaction humaine, juste un code PIN à récupérer. Ils sont présents dans 10 pays européens.

**Deux cas de figure :**

**Si Mondial Relay est intégré au site marchand :**
Tu choisis directement le Locker lors de ta commande. Utilise un faux nom, une fausse adresse, et un VPN dès la commande (on verra les détails VPN, numéros anonymes et cartes de paiement anonymes dans une prochaine partie).

**Si Mondial Relay n'est pas intégré :**
Le vendeur t'envoie une requête par email afin que tu saisisses tes coordonnées et choisisses ton point de livraison. Opte pour un Locker automatique.

Ouvre l'email Mondial Relay et clique sur le lien. Remplis avec de fausses informations : un faux nom unique pour cette commande, un faux numéro de téléphone, et une adresse existante mais qui n'est pas la tienne. Idéalement, choisis une adresse dans un rayon de 20 km autour du Locker que tu vas sélectionner.

Ensuite, choisis ton Locker sur la carte proposée. Prends-en un proche de chez toi, mais pas collé à ton domicile. Une fois le colis arrivé, tu recevras un code PIN par email. Tu peux y aller toi-même ou envoyer quelqu'un : seul le code est nécessaire pour récupérer le colis. Tu as 5 jours calendaires (week-ends et jours fériés inclus) pour le retirer.

**Note importante :** Utiliser un faux nom inventé (qui n'appartient à aucune personne réelle) pour recevoir un colis n'est pas une usurpation d'identité. L'usurpation d'identité consiste à se faire passer pour quelqu'un qui existe vraiment.

| Avantages | Inconvénients |
|---|---|
| Anonymat maximal (aucune pièce d'identité) | Tous les vendeurs n'acceptent pas Mondial Relay |
| Disponible 24/7 | Taille limitée (pas de gros colis type meubles) |
| Présent dans 10 pays | Aucun recours légal si perte/vol (faux nom) |
| Pas de contact humain | |
| Quelqu'un d'autre peut retirer avec le code PIN | |

**Amazon Locker : si tu commandes sur Amazon**

Si tu dois passer par Amazon, tu peux utiliser leurs Lockers. Même principe : casiers automatiques, code PIN, pas d'interaction humaine. Mais Amazon impose un compte. Trois stratégies possibles.

**Ton compte habituel, un autre nom en livraison**

Tu utilises ton compte Amazon à ton identité réelle, mais au moment de choisir l'adresse de livraison, tu sélectionnes un Amazon Locker et tu mets un faux nom comme destinataire. Amazon sait que c'est toi qui commandes, mais le livreur et la société de livraison ne voient que le faux nom sur l'étiquette. Au retrait, seul le code PIN compte. Quelqu'un d'autre peut récupérer à ta place.

**Un compte alter ego long terme**

Tu crées un compte Amazon avec le nom de ton alter ego, un email dédié (ou un alias), et un numéro anonyme pour les vérifications SMS (on verra les solutions dans une prochaine partie). Privilégie une carte de paiement anonyme au nom de ton alter ego (détails dans une prochaine partie). Les cartes cadeaux fonctionnent aussi, mais elles ont tendance à déclencher des vérifications d'identité approfondies si utilisées trop souvent.

Tu utilises ce compte pour tous tes besoins réguliers. Plus stable qu'un compte jetable, mais Amazon peut demander une vérification d'identité à tout moment. Si ça arrive, ton compte est bloqué jusqu'à ce que tu fournisses une pièce d'identité cohérente.

**Comptes jetables**

Tu crées un nouveau compte pour chaque commande. Faux nom, email jetable, cartes cadeaux à tes risques et périls. C'est la solution la moins stable : Amazon détecte facilement les comptes multiples. Blocage quasi-systématique et demande de vérification d'identité. Il n'est pas impossible que le compte se fasse bloquer et que tu y perdes des sous.

Une fois le colis arrivé au Locker, tu reçois un code de retrait par email. Tu as 3 jours pour le récupérer. Passé ce délai, retour et remboursement.

**Note :** Même si tu choisis l'option 1 par simplicité, tu réduis déjà grandement ta surface d'attaque en configurant ton adresse Paperboy (section 2) dans ton compte Amazon au lieu de ton adresse réelle, idéalement dès la création du compte. Résultat : tu livres en Locker avec un faux nom pour l'anonymat quotidien, et si un colis est trop volumineux pour le Locker, tu te le fais expédier chez Paperboy (qui te l'envoie en photo et peut le réexpédier ailleurs, on voit ça juste après). Dans tous les cas, ton adresse de vie ne fuit jamais, même si la base de données Amazon est piratée.

| **Avantages** | **Inconvénients** |
|---|---|
| Disponible 24/7 | Compte requis (risque de demande d'identification) |
| Nombreux points en ville | Historique d'achat conservé |
| Aucune pièce d'identité au retrait | Délai court : 3 jours |
| Compatible avec adresse Paperboy | Cartes cadeaux = risque de vérification accrue |

**Mondial Relay Point Relais**

Si les Lockers ne sont pas disponibles, Mondial Relay propose aussi des Points Relais (commerçants). Tu peux retirer ton colis soit avec une pièce d'identité, soit avec le code PIN reçu par email/SMS. Donc théoriquement, pas besoin de pièce d'identité si tu as le code PIN.

Attention : risque non négligeable de tomber sur un point relais où le commerçant fait du zèle et demande quand même une pièce d'identité. Le nom sur le colis peut aussi déclencher des questions. Aucun recours possible si ça bloque.

Moins fiable que le Locker (100% automatique), mais toujours mieux qu'une livraison à domicile.

| **Avantages** | **Inconvénients** |
|---|---|
| Plus de points disponibles que les Lockers | Interaction humaine (commerçant peut faire du zèle) |
| Présent dans 10 pays | Pièce d'identité parfois demandée malgré le code PIN |
| Délai retrait : 5 jours | Nom sur colis peut déclencher questions |
| | Aucun recours légal si perte/vol ou blocage |



Pour aller plus loin, rejoins Le Ƀunker sur YouTube

**Paperboy : réexpédition de colis**

Si tu ne peux pas utiliser de Locker (colis trop volumineux, vendeur n'accepte pas, article nécessitant ta vraie identité), tu peux te faire livrer à ton adresse Paperboy (section 2).

Paperboy reçoit ton colis, te l'envoie en photo par email, et tu peux demander une réexpédition physique. Le coût varie en fonction du poids (à partir de 5€ de préparation + frais de transport).

**Options de réexpédition :**

- **Pickup Station La Poste** (consignes automatiques Colissimo/Chronopost/DPD) : à voir avec Paperboy. Si réalisable, c'est la meilleure solution : pas de pièce d'identité, retrait 24/7 avec code PIN.
- Chez une connaissance ou un ami
- À ton adresse de vie (si tu n'as pas le choix)

Tu peux aussi configurer ton adresse Paperboy comme adresse principale même si tu es forcé d'utiliser ton vrai nom. Au moins, ton adresse de vie ne figure dans aucune base de données de vendeur.

| **Avantages** | **Inconvénients** |
|---|---|
| Compatible avec tous les vendeurs | Coûts additionnels |
| Protection de ton adresse de vie (au moins pour les vendeurs) | Délais supplémentaires |
| Réexpédition flexible | |

**Point Relais générique : le moindre mal**

Si tu es bloqué et que tu ne peux utiliser ni Locker ni Paperboy (zone non couverte, transporteur incompatible, vendeur impose son transporteur), il reste les Points Relais classiques : Colissimo, Chronopost, Relais Colis, etc.

**Si tu es forcé d'utiliser ta vraie identité :**
Tu renseignes ton vrai nom, mais tu choisis un Point Relais comme adresse de livraison. Au moins, les transporteurs et le vendeur n'ont pas ton adresse de vie. Tu te présentes au Point Relais avec ta pièce d'identité et le numéro de suivi pour récupérer ton colis.

**Si tu choisis d'utiliser ton alter ego ou un faux nom jetable :**
Tu renseignes un faux nom lors de ta commande et tu choisis un Point Relais. La plupart des commerçants ne demandent pas de pièce d'identité, mais certains peuvent la

réclamer ou poser des questions si le nom ne correspond à rien. Aucun recours légal si le colis est perdu ou si le commerçant refuse de te le donner.

C'est la solution la moins fiable pour l'anonymat (interaction humaine, politique variable selon les commerçants), mais au moins ton adresse de vie ne fuite pas.

| **Avantages** | **Inconvénients** |
|---|---|
| Disponible partout en France | Interaction humaine obligatoire |
| Compatible avec tous les transporteurs | Pièce d'identité demandée si vrai nom |
| Protection de ton adresse de vie | Avec faux nom : risque de refus ou questions |
| | Avec faux nom : aucun recours légal |

## 4.2 Envoyer des colis

Le vrai problème quand tu envoies un colis, c'est que tu n'as pas le contrôle. Contrairement à la réception où tu peux choisir un Locker et donner un faux nom sans interaction humaine, pour l'envoi, tu dois soit passer par un guichet, soit créer un compte en ligne. Et chaque interaction est une opportunité pour qu'on te demande une pièce d'identité ou des informations d'identification.

Heureusement, il reste des solutions pour envoyer des colis sans nécessairement dévoiler ton identité réelle ou bien ton adresse de vie.

**Mondial Relay Locker : la meilleure solution**

Mondial Relay te permet d'envoyer un colis sans interaction humaine, exactement comme pour la réception, à ceci près que dans ce sens-là, ça nécessite un compte. Tu crées ton compte en ligne avec un faux nom, une adresse email dédiée, un numéro jetable pour la vérification SMS, et une carte de paiement anonyme (on verra les solutions dans une prochaine partie).

Une fois ton envoi créé, tu as deux options pour déposer ton colis :

**Option 1 : Imprimer l'étiquette et déposer au Locker**
Tu imprimes l'étiquette chez toi, tu la colles sur ton colis, et tu le déposes directement dans un Locker 24/7. Zéro interaction humaine. Tu scannes le code-barres de l'étiquette sur l'écran du Locker, un casier s'ouvre, tu déposes ton colis, c'est terminé.

**Option 2 : Présenter le QR code dans un Point Relais**
Si tu n'as pas d'imprimante, tu vas dans un Point Relais Mondial Relay avec ton QR code

(reçu par email après création de l'envoi). Le commerçant scanne ton QR code, imprime l'étiquette, et prend en charge ton colis. Aucune information d'identification demandée.

Ton colis est livré en 3 à 5 jours ouvrés.

| **Avantages** | **Inconvénients** |
|---|---|
| Anonymat préservé | Compte requis |
| Disponibilité flexible | Carte de paiement nécessaire |
| Avec ou sans interaction humaine | Tous les destinataires n'acceptent pas Mondial Relay |
| Présent dans 10 pays | |

**La Poste**

Si tu ne peux pas utiliser Mondial Relay (destinataire incompatible, colis trop volumineux), La Poste reste une option valable. Tu as trois façons de procéder.

**En cash au guichet**

Tu te présentes au guichet avec ton colis déjà emballé. Sur l'étiquette ou le bordereau, tu renseignes un faux nom crédible et une adresse existante mais qui n'est pas la tienne comme adresse de retour. Tu payes en liquide, tu récupères ton reçu, c'est terminé.

Il existe un risque que le guichetier te demande une pièce d'identité. C'est rare, mais ça arrive.

**Étiquettes prépayées Colissimo**

Tu achètes des étiquettes prépayées Colissimo en bureau de poste ou chez un buraliste. Tu payes en cash, elles ont une validité permanente.

Le carnet contient 2 étiquettes pour des colis jusqu'à 2 kg. Tu remplis à la main le nom et l'adresse de l'expéditeur (un faux nom crédible et une adresse existante mais pas la tienne) et les informations du destinataire. Tu colles l'étiquette sur ton colis, et tu le déposes au guichet d'un bureau de poste.

**Via internet**

Tu crées un compte sur le site de La Poste avec un faux nom et une adresse email dédiée. Tu payes avec une carte de paiement anonyme (on verra les solutions dans une prochaine partie). Tu imprimes l'étiquette et tu déposes ton colis au guichet.

Il existe un risque que le guichetier te demande une pièce d'identité. C'est encore plus rare qu'avec un paiement en cash.

Comme pour tout le reste : ton vrai nom et ton adresse de vie ne doivent jamais apparaître sur un colis, que tu l'envoies ou que tu le reçoives.

# PARTIE III : CE QUE TU FAIS EN LIGNE

En à peine un mois, en janvier 2026, la France a été victime de plus de 130 piratages de bases de données nationales. Tout y passe : les boutiques en ligne, les fédérations de sport, les salles de sport et même l'administration publique. Les hackers recoupent les infos entre tous les hacks et collectent des informations sur vous pour vous hacker vos réseaux, vos comptes bancaires ou, pire encore, venir vous envoyer un groupe de “petits anges” de cité cagoulés chez vous pour vous torturer et dérober vos cryptomonnaies.

Le Nicolas moyen est donc pris en étau entre l'État bolchévique qui a besoin de le ponctionner pour éviter la faillite, la grande majorité du peuple français qui veut prendre son argent pour le redistribuer aux improductifs, et les ingénieurs de la DZ mafia qui veulent s'emparer de son trésor de guerre.

Et comme si ça ne suffisait pas, l'État français multiplie les lois liberticides : interdiction des réseaux sociaux aux moins de 15 ans, surveillance vidéo algorithmique, et Macron qui formalise en juillet 2025 le concept de "sécurité cognitive" pour "protéger l'esprit des citoyens". Bienvenue en 1984.

Il est donc important de ne laisser aucune trace et de prendre son hygiène numérique au sérieux.

# Chapitre 5 : Téléphonie

Ton numéro de téléphone, c'est ton identifiant le plus critique. Plus encore que ton email. Pourquoi ? Parce qu'il est lié à ton identité civile. Pour acheter une carte SIM en France, il faut une pièce d'identité. Et ce numéro, tu le donnes partout : banque, réseaux sociaux, 2FA, livraisons, inscriptions en ligne. Contrairement à ton email que tu peux changer en 5 minutes, ton numéro de téléphone, tu es coincé avec pendant des années. C'est parfait pour te tracer.

Et devine quoi ? Les bases de données de numéros de téléphone sont les premières à fuiter. En janvier 2026, la fuite de 45 millions de données françaises incluant des millions de numéros de téléphone. Résultat : tu te fais appeler toute la journée par du démarchage, du spam et des arnaques. 97% des Français sont agacés par le démarchage téléphonique. 40% des Français ont déjà été victimes de smishing (SMS arnaque). En 2025, 18 000 signalements d'usurpation de numéro ont été enregistrés sur la plateforme de l'Arcep. Si tu reçois des appels spam tous les jours, c'est la preuve que ton numéro a fuité quelque part.

Mais le vrai problème, c'est le traçage. Ton opérateur télécom enregistre tous tes appels, tous tes SMS, et ta position géographique via les antennes relais. L'État peut demander ton historique complet à ton opérateur, et ce dernier est légalement obligé de fournir. Depuis janvier 2026, la France a même mis en place un système d'authentification des numéros via le protocole STIR/SHAKEN pour lutter contre l'usurpation. Traduction : encore plus de traçabilité.

Bref, ton numéro de téléphone, c'est une laisse que tu traînes partout. Voici comment la couper.

## Les 4 cas d'usage

Avant de te noyer dans les solutions, il faut comprendre qu'il n'existe pas UNE solution miracle. Tout dépend de ton besoin.

**Tu as besoin d'un numéro éphémère pour une vérification SMS ponctuelle ?** Un numéro jetable suffit (SMSPool, LNVPN Disposable). 0.50-2€ par SMS, anonymat maximal, mais le numéro meurt après réception.

**Tu as besoin de recevoir plusieurs SMS sur le même numéro ?** Il te faut un numéro longue durée (LNVPN Rental UK, Silent.link US). 5-15€ par mois, tu reçois des SMS, mais tu ne peux pas en envoyer ni passer d'appels.

**Tu as besoin d'envoyer des SMS ou de passer des appels ?** Une SIM prépayée au tabac (Lycamobile, Lebara, Syma). 5-20€ de recharge, KYC laxiste, tu peux tout faire : envoyer, recevoir, appeler, internet mobile en option.

**Tu veux juste de l'internet mobile sans numéro de téléphone ?** Une eSIM LNVPN ou Silent.link fait le job. Data uniquement, paiement Bitcoin, anonymat maximal, mais pas de SMS ni d'appels.

Maintenant, rentrons dans les détails.



Pour aller plus loin, rejoins Le ₿unker sur YouTube

## Numéros éphémères (vérification SMS unique)

**Cas d'usage :** Tu dois créer un compte sur un site qui demande un numéro de téléphone pour vérifier que tu es humain. Ça peut être pour créer un compte Mondial Relay par exemple, un site e-commerce, ou n'importe quel service en ligne. Tu n'as besoin de recevoir qu'un seul SMS avec le code de vérification, puis tu ne toucheras plus jamais à ce numéro.

**Solution : numéros jetables.**

Ces services recyclent les numéros. Le numéro que tu utilises aujourd'hui a peut-être déjà servi à créer un compte il y a 6 mois. Résultat : quand tu essaies de créer ton compte, le site te dit "ce numéro est déjà utilisé". Tu dois racheter un autre numéro et réessayer. C'est chiant, mais c'est le prix de l'anonymat.

**SMSPool**

SMSPool te loue un numéro pour recevoir un seul SMS. Tu choisis le pays et le service, tu paies en Bitcoin, et tu reçois un numéro. Le SMS arrive dans les secondes qui suivent. Le numéro meurt après.

**LNVPN Disposable**

LNVPN Disposable fonctionne exactement pareil. Tu paies en Bitcoin Lightning, tu choisis ton numéro, tu reçois le SMS, c'est terminé.

Attention : certains services détectent que c'est un numéro VoIP (pas une vraie SIM) et le refusent. Dans ce cas, il faut passer à la solution suivante.

## Numéros longue durée (recevoir plusieurs SMS sur le même numéro)

**Cas d'usage :** Tu as besoin de recevoir plusieurs SMS sur le même numéro. Par exemple, pour recevoir des notifications, ou pour un compte de réseau social que tu veux garder.

**Solution : numéros en location.**

**LNVPN Rental (UK)**

LNVPN Rental te loue un numéro britannique (indicatif +44) par abonnement mensuel. Tu paies en Bitcoin Lightning, et tu conserves le numéro tant que tu paies.

**Important :** Tu **reçois** des SMS uniquement. Tu ne peux ni en envoyer ni passer d'appels.

**Silent.link (US)**

Silent.link fonctionne pareil, mais avec un numéro américain (indicatif +1). Tu paies en Bitcoin Lightning, et le numéro reste actif tant que tu paies l'abonnement.

**Important :** Réception SMS uniquement, pas d'envoi ni d'appels.

**Bonus :** Silent.link inclut une eSIM pour la data mobile.

**Limite :** Certains services français refusent les numéros étrangers (+44 ou +1). Dans ce cas, il te faut un vrai numéro français, donc une SIM prépayée.

## SIM prépayée (envoyer SMS + appels + internet)

**Cas d'usage :** Tu as besoin d'envoyer des SMS (certaines vérifications demandent un SMS aller-retour), de passer des appels vocaux, ou d'avoir un numéro français pour un usage quotidien.

Par exemple, pour vérifier un compte sur X, c'est à toi d'envoyer un SMS vers un numéro en Angleterre. Cette solution s'y prête parfaitement.

**Solution : SIM prépayée au tabac.**

**Lycamobile, Lebara, Syma**

Tu achètes une carte SIM au tabac pour quelques euros. Ces opérateurs ont un **KYC laxiste** : ils demandent une pièce d'identité pour activer la SIM, mais le contrôle est sommaire. Leur fonds de commerce, c'est de fournir des numéros aux personnes qui n'ont pas forcément le profil idéal. Tu recharges ensuite en cash au tabac.

**Process :**

1. Achète la SIM au tabac (environ 5€)
2. Active en ligne : renseigne une adresse existante mais pas la tienne, et pour le numéro de CNI ou de passeport, il suffit d'être créatif
3. Recharge en cash au tabac

Tu peux envoyer des SMS et passer des appels. Numéro français (indicatif +33), accepté partout. Internet mobile en option.

## eSIM (internet mobile anonyme)

**Cas d'usage :** Tu veux de la data mobile sans numéro de téléphone. Pratique pour voyager anonymement (pas de SIM physique de ton pays), ou comme backup internet si ta SIM principale est compromise.

**Solution : eSIM LNVPN ou Silent.link.**

LNVPN eSIM et Silent.link te fournissent une eSIM payable en Bitcoin Lightning. **Data uniquement** : pas de numéro de téléphone, pas de SMS, pas d'appels. Multi-pays.

**Process :**

1. Commande l'eSIM sur le site LNVPN ou Silent.link
2. Paie en Bitcoin
3. Reçois un QR code
4. Scanne le QR code dans les paramètres de ton téléphone → eSIM activée

Anonymat maximal (paiement Bitcoin), pas de SIM physique (discret), activation instantanée.

**Important :** Nécessite un téléphone compatible eSIM (iPhone XS+, Android récents).

# Chapitre 6 : Emails

Si tu utilises le même email partout, tu te grilles tout seul. Un seul email sur 10 services = 10 points qui te relient. Les attaquants voient le pattern et reconstituent ton profil complet. Ton email Netflix + ton email LinkedIn + ton email salle de sport = ton nom complet, ton boulot, ton quartier, tes goûts. Un seul piratage suffit pour que tout fuite.

Dans la Partie II, je t'ai dit de créer un alter ego avec un email dédié. Maintenant, on va voir comment gérer tout ça concrètement.

## Pourquoi la corrélation est le vrai danger

Tu utilises jean.dupont@gmail.com pour t'inscrire sur 20 sites différents : Netflix, Amazon, des forums, LinkedIn, ta salle de sport, Leboncoin, X, Instagram.

Chacun de ces sites a une base de données avec ton email. Quand un de ces sites se fait hacker (et ça arrive tout le temps), ton email fuite. Les attaquants collectent ces fuites et les recoupent.

Résultat : ils voient que le même email apparaît dans 10 fuites différentes. Ils savent maintenant que jean.dupont@gmail.com a un compte LinkedIn (ton vrai nom, ton boulot), un abonnement Netflix (tes goûts), une inscription salle de sport (ton quartier), un compte X (tes opinions).

Avoir un seul email partout, c’est tendre la joue pour se faire hack.

## La solution : compartimenter

La solution, c'est de compartimenter.

Dans la Partie II, je t'ai dit : une adresse email pour ton alter ego, et des alias pour les besoins ponctuels. Voici comment faire concrètement.

**Structure minimum :**

**1. Ton identité réelle**
Un email pour banque, impôts, santé, famille. Les trucs où tu es obligé de donner ton vrai nom.
Exemple : jean.dupont@protonmail.com

**2. Ton alter ego pour les besoins récurrents et la règle du +**

Tu crées un email dédié à ton alter ego, et tu utilises le +tag pour les différents services.

Gmail et ProtonMail supportent le +tag : tu ajoutes +tag à ton email et tout arrive dans ta boîte principale.

Exemple :

- Email alter ego : jean.martin@protonmail.com
- Inscription salle de sport : jean.martin+sport@protonmail.com

Tous les emails arrivent dans jean.martin@protonmail.com. En bonus : tu verras qui a vendu tes données. Si tu reçois du spam sur jean.martin+sport@protonmail.com, tu sais que c'est la salle de sport qui a fuité ou vendu ta base.

**Limite du +** : Ça révèle ton email réelle (il suffit de retirer le +sport). Pour de l'anonymat réel, utilise des services d'alias.

**3. Les emails alias**

Un alias, c'est une adresse email secondaire qui redirige tous les messages vers ton inbox réelle, mais sans révéler ton email principal.

Tu t'inscris sur Netflix avec netflix-xyz123@simplelogin.com. Netflix t'envoie un email, il arrive dans ta vraie boîte jean.martin@protonmail.com. Mais Netflix ne connaît jamais ton vrai email. Si Netflix spam ou se fait hacker, tu désactives l'alias et c'est fini. Ton email principal reste protégé.

**Services d'alias :**

**SimpleLogin** : Plans gratuit (10 alias) et payant. Racheté par Proton, open source, domaine custom possible. Si tu as déjà ProtonMail payant, SimpleLogin premium est inclus. Tu peux répondre depuis l'alias.

**Addy.io** (ex-AnonAddy) : Alias illimités. Open source, support GPG. Tu peux répondre depuis l'alias.

**iCloud Hide My Email** : Requiert abonnement iCloud+. Alias illimités, intégré à Safari et Mail, pratique si tu es dans l'écosystème Apple. Tu peux répondre depuis l'alias.

**Firefox Relay** : Plans gratuit et payant. Service Mozilla, intégré au navigateur Firefox. Tu peux répondre depuis l'alias (plans payants).

**DuckDuckGo Email Protection** : Gratuit, alias illimités en @duck.com. Suppression automatique des trackers, requiert extension DuckDuckGo. Tu peux répondre depuis l'alias.

**Limite importante** : Ces services conservent le lien entre tes alias et ton email réelle dans leurs bases de données. Si SimpleLogin ou Addy.io se font pirater, un attaquant peut potentiellement relier tous tes alias à ton adresse principale. Ça reste quand même une protection solide. Le service qui t'envoie des emails ne connaît jamais ton vrai email. Et un attaquant doit d'abord pirater SimpleLogin ou Addy avant de faire le lien entre tes alias et ton adresse principale.

**4. Les emails jetables pour du one-time**

Même principe que les numéros éphémères du chapitre précédent. Tu ouvres le site, il te génère une adresse temporaire au hasard, tu reçois ton email, l'adresse meurt après quelques minutes ou heures.

**Services :**

**Guerrilla Mail** : Email jetable instantané, pas d'inscription, l'adresse meurt après 1 heure d'inactivité.

**10 Minute Mail** : Email qui meurt automatiquement après 10 minutes. Tu peux prolonger si besoin.

**Temp Mail** : Email jetable aléatoire, tu peux en générer autant que tu veux, durée de vie variable.

**TempMailo** : Email temporaire avec plusieurs domaines au choix.



Pour aller plus loin, rejoins Le ₿unker sur YouTube

Si tu veux aller plus loin, tu peux aussi séparer ton email pro, ton email shopping, ton email réseaux sociaux. Mais l'essentiel, c'est de ne jamais utiliser le même email pour ton identité réelle et ton alter ego.

## Où héberger tes emails

Maintenant que tu sais compartimenter tes emails, il faut choisir où les héberger.

Le problème avec Gmail, Outlook, Yahoo, c'est qu'ils lisent tous tes emails. Google scanne tes messages pour cibler ses pubs, Microsoft fait pareil. Tes emails sont stockés en clair sur leurs serveurs. Si un gouvernement demande accès à ton compte, ils donnent tout sans broncher.

**ProtonMail, c'est l'inverse.**

Proton ne peut pas lire tes emails, même s'ils le voulaient. Juridiction Suisse. Hors de portée des 5/9/14 Eyes. Pas de tracking. Pas de pub.

**Important :** ProtonMail ne peut pas lire tes emails, mais ils peuvent être forcés de logger ton adresse IP si un tribunal suisse l'ordonne. La seule donnée qu'ils peuvent fournir aux autorités, c'est ton IP de connexion. Solution : accède toujours à ProtonMail via un VPN (ou Tor). Comme ça, l'IP loggée sera celle du serveur VPN, pas la tienne.

Plans gratuit et payant. Le gratuit suffit pour un usage basique. Le payant te donne plus de stockage, des alias illimités, et SimpleLogin premium inclus.

**Alternative : Tutanota.**

Chiffrement de bout en bout aussi, juridiction Allemagne, open source. Moins cher que ProtonMail. Interface plus simple mais moins de fonctionnalités.

## Vérifie si tes emails ont déjà fuité

Avant de passer à autre chose, vérifie si tes emails ont déjà fuité.

Va sur **haveibeenpwned.com**. Entre ton email. Le site te dit si ton email a fuité.

Si ton email a fuité, change les mots de passe de tous les services où tu utilises cet email. Active la 2FA partout (on verra ça au chapitre suivant). Et migre tes comptes critiques vers ProtonMail.

Tu peux aussi activer les alertes automatiques sur Have I Been Pwned. Comme ça, si ton email apparaît dans une future fuite, tu reçois une notification immédiatement. C'est gratuit.

Un email par identité, c'est pas de la parano. C'est de l'hygiène de base.

# Chapitre 7 : Mots de passe

Tu as probablement déjà entendu qu'il faut des mots de passe "forts" : 12 caractères minimum, majuscules, minuscules, chiffres, caractères spéciaux. Le problème, c'est que personne ne peut retenir 50 mots de passe différents qui ressemblent à ça : K9$mPz@3vL!qX. Donc tu fais comme tout le monde : tu réutilises le même mot de passe partout, ou tu en as 2-3 que tu alternes.

Et c'est exactement là que ça devient dangereux. Quand un site se fait pirater (et ils se font tous pirater un jour ou l'autre), ton mot de passe fuite. Si tu utilises le même mot de passe sur 15 sites, les 15 comptes tombent. Un seul piratage suffit pour tout perdre.

La solution, c'est pas de te forcer à retenir 50 mots de passe compliqués. C'est d'arrêter d'essayer de les retenir. Un gestionnaire de mots de passe, c'est un coffre-fort numérique qui génère et stocke tous tes mots de passe. Tu retiens un seul mot de passe maître, et lui retient les 50 autres. Chaque compte a un mot de passe unique, aléatoire, de 20+ caractères. Si un site fuite, un seul compte tombe, pas les 15 autres.

## 1. Gestionnaires de mots de passe

**Bitwarden**

Cloud chiffré de bout en bout. Quand tu tapes ton mot de passe maître, Bitwarden dérive une clé de chiffrement directement sur ton appareil. Tous tes mots de passe sont chiffrés avec cette clé **avant** d'être envoyés sur les serveurs de Bitwarden. Les serveurs stockent uniquement des blocs chiffrés illisibles. Même si Bitwarden se faisait pirater, les attaquants n'obtiendraient que du charabia. Même Bitwarden ne peut pas lire tes mots de passe.

**Important : si tu perds ton mot de passe maître, tu perds TOUS tes mots de passe.** Il n'y a aucune récupération possible. Note-le sur papier et range-le dans un endroit sûr.

**KeePass**

100% local, zéro cloud. Ta base de données de mots de passe est un fichier unique (.kdbx) qui reste physiquement sur ton appareil. Rien n'est jamais envoyé sur internet. Chiffrement AES-256 (standard militaire). Tu contrôles absolument tout : où est le fichier, qui y accède, comment il est sauvegardé.

100% gratuit, open source. Interface moins moderne que Bitwarden, mais ultra-fiable. Existe depuis 2003, utilisé par des millions de paranos.

**Important : tu dois sauvegarder ce fichier régulièrement** (sur une clé USB, un autre appareil, ou via un service de sync P2P comme Syncthing). Si tu perds ton fichier sans backup, tu perds tous tes mots de passe.

## 2. Double authentification (2FA)

Un mot de passe, même généré par Bitwarden, ça peut fuiter : piratage du site, keylogger sur ton PC, phishing bien ficelé. Si quelqu'un vole ton mot de passe, il peut accéder à tes comptes. Sauf si tu as activé le 2FA, et là, même avec ton mot de passe, l'attaquant ne peut pas se connecter parce qu'il lui manque un deuxième élément qu'il n'a pas.

**TOTP : le minimum syndical**

C'est une application qui génère des codes à 6 chiffres qui changent toutes les 30 secondes. Le code est calculé localement sur ton téléphone avec une clé secrète partagée au moment de l'activation, rien ne transite par internet. Contrairement au SMS (qui peut être intercepté ou détourné via une attaque SIM swap), le code TOTP ne peut pas être volé à distance. Même si quelqu'un intercepte tes communications ou clone ta SIM, il n'a pas la clé secrète stockée dans ton téléphone.

**Recommandation :** 2FAS (open source, iOS et Android) ou Aegis (open source, Android uniquement). Les deux permettent de sauvegarder tes clés TOTP.

**Important :** Ne stocke pas tes codes TOTP dans Bitwarden (où sont déjà tes mots de passe). Si quelqu'un accède à ton compte Bitwarden, il aura à la fois tes mots de passe ET tes codes 2FA. Utilise une app dédiée pour la 2FA, c'est plus sûr.

Attention par contre : si tu perds ton téléphone sans backup des clés TOTP, tu es bloqué. 2FAS et Aegis permettent de sauvegarder tes clés, donc pense à activer ça.

**Clés matérielles : pour les trucs qui comptent vraiment**

Clé physique USB ou NFC, genre YubiKey. Tu la branches ou tu la touches pour valider la connexion. Même si quelqu'un vole ton mot de passe ET ton téléphone, il ne peut rien faire sans ta clé physique. C'est inphishable : même si tu tapes ton mot de passe sur un faux site (phishing parfait, copie pixel-perfect de ta banque), l'attaquant ne peut pas se connecter parce que la clé vérifie le nom de domaine, et si c'est pas le bon site, elle refuse de signer.

C'est le seul 2FA qui résiste au phishing. Les codes TOTP, tu peux les taper sur un faux site sans t'en rendre compte, mais une clé matérielle, elle sait où elle est connectée.

Le problème, c'est que tous les sites ne supportent pas les clés matérielles. Mais pour ta banque, ton gestionnaire de mots de passe, ton email principal : si c'est possible, tu mets une clé. Prix : environ 30€ pour une YubiKey Security Key NFC compatible USB-A + NFC.

**Note importante :** Évite le 2FA par SMS. De toute façon, si t'as bien suivi le chapitre sur la téléphonie, tu n'as pas de numéro de téléphone durable et unique, donc TOTP ou clé matérielle, point.

**Règle simple :** Tout ce qui compte doit avoir du 2FA. Email, gestionnaire de mots de passe, banque : minimum TOTP. Si tu peux mettre une clé matérielle, tu mets une clé.

Un gestionnaire de mots de passe, c'est pas optionnel. Un mot de passe différent par compte, généré aléatoirement, et du 2FA partout où c'est possible. C'est 30 minutes de setup pour ne plus jamais avoir à te soucier d'une fuite de mot de passe ou d'un accès frauduleux à tes comptes.

# Chapitre 8 : Navigation

Chaque fois que tu ouvres un navigateur, tu laisses des traces. Ton adresse IP révèle ta localisation géographique et ton fournisseur d'accès internet. Ton FAI voit absolument tous les sites que tu visites. Et en France, les FAI sont légalement obligés de conserver ton historique de connexions pendant un an. Orange, Free, SFR : ils ont tous un dossier sur toi avec chaque site que tu as visité, horodaté, pendant 365 jours. Parce que l'État a besoin de savoir ce que tu mates en ligne, au cas où.

Ton navigateur, lui, dit aux sites que tu visites qui tu es : quel OS tu utilises, quelle résolution d'écran tu as, quelles polices sont installées sur ton PC. Ton moteur de recherche enregistre chaque requête que tu tapes et la lie à ton profil. Et si tu utilises Google Chrome (comme 65% des utilisateurs d'internet dans le monde), c'est encore pire : chaque clic, chaque recherche, chaque site que tu visites remonte directement à Google pour alimenter ton "profil publicitaire".

La solution : un VPN pour que ton FAI arrête de te surveiller, un navigateur qui ne te moucharde pas, un moteur de recherche qui ne logue pas chaque recherche, et Tor quand tu veux vraiment disparaître.

## 1. Navigateurs

Le navigateur que tu utilises détermine ce que tu laisses comme traces. Chrome envoie tout à Google, Edge envoie tout à Microsoft. Si tu veux reprendre le contrôle, il faut changer d'outil.

**Firefox**

C'est le navigateur open source que tu utilises au quotidien si tu veux de la privacy sans sacrifier la compatibilité. Firefox supporte toutes les extensions dont tu as besoin : bloqueur de pubs (uBlock Origin), bloqueur de trackers, gestionnaire de mots de passe (Bitwarden, dont on a parlé au chapitre précédent).

Par défaut, Firefox envoie de la télémétrie à Mozilla (statistiques d'utilisation). Tu dois désactiver ça dans les paramètres de Vie privée et sécurité.

Si tu veux une alternative prête à l'emploi sans configuration, il y a Brave.

**Brave**

Basé sur Chromium (le moteur open source derrière Chrome), mais dégooglé. Toutes les connexions à Google ont été retirées. Bloqueurs de pubs et de trackers intégrés par défaut, donc pas besoin d'installer des extensions. L'interface est identique à Chrome, donc la migration est facile si tu viens de Chrome.

**Tor Browser**

Pour les opérations sensibles. Tor Browser, c'est Firefox modifié avec le réseau Tor intégré. Quand tu visites un site, ton trafic passe par 3 relais chiffrés (nœuds Tor) avant d'arriver au site de destination. Le premier relai connaît ton IP mais pas où tu vas, le dernier relai sait où tu vas mais pas qui tu es. Personne ne peut voir à la fois qui tu es ET ce que tu consultes.

Plus lent qu'un navigateur classique (à cause des relais successifs), et certains sites bloquent les adresses IP Tor (parce qu'elles sont connues et listées publiquement).

## 2. Moteurs de recherche

Google Search enregistre chaque requête que tu tapes et la lie à ton compte Google (si tu es connecté) ou à ton profil publicitaire via cookies et fingerprinting. Ils savent ce que tu cherches, quand, depuis où.

**DuckDuckGo**

Le moteur de recherche privé par défaut. Pas de tracking, pas de profil utilisateur, pas de stockage de tes recherches. Les résultats sont corrects pour un usage quotidien, même s'ils sont parfois moins pertinents que Google (parce que Google a 20 ans d'historique et d'optimisation derrière lui).

**Startpage**

Startpage utilise les résultats de Google, mais de manière anonymisée. Tu obtiens la qualité de recherche Google sans que Google sache qui tu es. Startpage agit comme un proxy entre toi et Google : ils envoient ta requête à Google, récupèrent les résultats, et te les affichent sans transmettre ton IP ou tes cookies à Google.

Bonus : fonction "Anonymous View" qui te permet de visiter les sites depuis un proxy Startpage, donc le site ne voit pas ton IP.

**Brave Search**

Le moteur de recherche de Brave (le navigateur). Index propre, pas basé sur Google ou Bing. Pas de tracking. Résultats corrects, mais moins pertinents que Google. Alternative solide si tu utilises déjà Brave comme navigateur.

## 3. VPN

Ton FAI voit tous les sites que tu visites parce qu'il voit toutes les requêtes DNS que ton ordinateur envoie pour résoudre les noms de domaine en adresses IP. Quand tu tapes lebunker.net dans ton navigateur, ton ordinateur demande à un serveur DNS "c'est quoi l'IP de lebunker.net ?", et cette requête passe par ton FAI. Résultat : Orange, Free, SFR savent exactement quels sites tu visites, même si le contenu des pages est chiffré en HTTPS.

Un VPN (Virtual Private Network) masque ton trafic à ton FAI. Quand tu actives un VPN, tout ton trafic internet passe par un tunnel chiffré vers un serveur VPN, puis ressort de là pour aller sur internet. Ton FAI voit seulement que tu te connectes au serveur VPN, il ne voit plus les sites que tu visites. Et les sites que tu visites voient l'IP du serveur VPN, pas la tienne.

**Important :** Un VPN ne te rend pas anonyme. Il déplace juste ta confiance : au lieu de faire confiance à ton FAI (qui logue tout), tu fais confiance au provider VPN. Si le provider VPN logue tes connexions, tu n'as rien gagné. C'est pour ça qu'il faut choisir un provider no-logs audité de manière indépendante.

Une fois que tu as un VPN, reste connecté en permanence. Si tu l'actives seulement pour certaines opérations sensibles, tu fuis ta vraie IP partout le reste du temps. Le VPN doit être ton mode par défaut, pas une option ponctuelle.

**Notre recommandation : LNVPN**

Le VPN le plus anonyme du marché. Paiement Bitcoin Lightning uniquement, donc aucune trace bancaire, aucun lien avec ton identité réelle. Pas d'email requis, pas de compte à créer, pas de nom, pas d'adresse, rien. Tu paies via Lightning, ton service s'active automatiquement, tu te connectes, c'est terminé.

LNVPN ne conserve aucun log de connexion. Pendant que tu es connecté, ils gardent ton IP en mémoire (RAM), mais après 5 minutes d'inactivité ils l'effacent, et elle n'est jamais écrite sur disque. Les clés VPN WireGuard sont générées localement dans ton navigateur via JavaScript, elles ne passent jamais par leurs serveurs. LNVPN ne sait pas qui tu es, d'où tu viens, et ne peut pas relier ton paiement Lightning à ton utilisation du VPN.

Protocole WireGuard (le plus rapide et le plus sécurisé actuellement). Serveurs dans 14 pays. Pas de cookies, pas de tracking sur leur site. Lien affilié.

**Mullvad**

Le VPN recommandé si tu veux payer en cash. Tu peux littéralement leur envoyer une enveloppe avec des billets et l'identifiant du compte. Pas de compte email requis : tu

génères un numéro de compte aléatoire à 16 chiffres, c'est ton identifiant. Mullvad ne sait pas qui tu es.

Juridiction Suède. Mullvad ne logue rien, et cette politique a été auditée publiquement par Cure53. Tous leurs serveurs tournent 100% sur RAM, zéro disque dur. Ça veut dire quoi ? Quand un serveur redémarre, toutes les données stockées en mémoire volatile sont effacées automatiquement. Rien ne persiste sur disque. En 2023, la police suédoise a perquisitionné les bureaux de Mullvad et n'a saisi aucun équipement parce qu'ils ont réalisé qu'il n'y avait aucune donnée utilisateur stockée nulle part.

**IVPN**

Alternative solide basée à Gibraltar. Même philosophie que Mullvad : pas d'email requis, compte anonyme généré aléatoirement. Paiement cash possible. IVPN ne logue rien, et Cure53 a audité publiquement cette politique depuis 2019, avec des audits annuels répétés.

IVPN a déployé son infrastructure RAM-only à partir de 2025. Même principe que Mullvad : serveurs sans disque dur, tout tourne en mémoire volatile. Quand un serveur redémarre, toutes les données sont effacées. Open source complet : toutes leurs applications sont auditables publiquement.

## 4. Tor

Un VPN masque ton IP à ton FAI et aux sites que tu visites, mais le provider VPN voit tout : ton IP réelle, les sites que tu visites, quand tu t'y connectes. Tu déplaces ta confiance de ton FAI vers le provider VPN. Si tu veux de l'anonymat réel, il faut utiliser Tor.

**Comment fonctionne Tor**

Tor (The Onion Router) est un réseau décentralisé de milliers de relais bénévoles répartis dans le monde entier. Quand tu te connectes à un site via Tor, ton trafic passe par 3 relais successifs, chacun ne connaissant que le relai précédent et le relai suivant. Le premier relai (guard node) connaît ton IP réelle mais pas où tu vas. Le relai de sortie (exit node) sait où tu vas mais pas qui tu es. Personne ne peut relier ton IP réelle au site que tu visites.

Chaque connexion utilise un circuit différent (3 relais différents), et les circuits changent automatiquement toutes les 10 minutes. Même si quelqu'un contrôle un des relais, il ne peut pas voir à la fois qui tu es et ce que tu consultes.

**Quand utiliser Tor**

Pour des opérations sensibles où tu ne veux laisser aucune trace. Recherches sur des sujets sensibles, consultation de sites que tu ne veux pas voir apparaître dans ton historique, whistleblowing, journalisme. Si tu es un dissident politique, un journaliste dans un pays autoritaire, ou simplement quelqu'un qui veut un anonymat réel, Tor est la seule solution qui tient la route.

**Limites de Tor**

Tor est plus lent qu'un VPN (parce que ton trafic passe par 3 relais successifs au lieu d'un seul serveur VPN). Certains sites bloquent les adresses IP Tor parce qu'elles sont connues et listées publiquement. Cloudflare te demande de résoudre des CAPTCHAs à répétition. Les sites de streaming (Netflix, YouTube) bloquent Tor.

JavaScript est un vecteur d'attaque sur Tor. Un site malveillant peut exploiter JavaScript pour récupérer des infos sur ton système et te déanonymiser. Tor Browser a un mode "Safest" qui désactive JavaScript complètement, mais ça casse beaucoup de sites modernes.

Tu peux combiner VPN + Tor : tu te connectes à ton VPN, puis tu lances Tor Browser. Ton FAI voit que tu te connectes au VPN (pas à Tor), et le premier nœud Tor voit l'IP du VPN (pas ton IP réelle). Ça ajoute une couche de protection, mais c'est overkill pour 95% des cas.

Un navigateur qui ne te track pas, un moteur de recherche qui ne logue pas tes requêtes, un VPN activé en permanence, et Tor Browser quand tu veux vraiment disparaître. C'est tout ce qu'il faut pour ne plus laisser de traces à chaque clic.



Pour aller plus loin, rejoins Le Ƀunker sur YouTube

# Chapitre 9 : Nettoyer ses traces

Tu crois que personne ne sait qui tu es en ligne ? Tu te trompes. Des photos de toi prises il y a 10 ans lors d'un événement random, un commentaire sur un forum que tu as posté en 2012 sous ton vrai nom parce que tu ne savais pas encore que l'internet n'oublie jamais : tout ça circule quelque part, indexé par Google, archivé par des sites que tu as oubliés depuis longtemps, revendu par des data brokers, scraped par des moteurs de reconnaissance faciale, et accessible à n'importe qui qui sait où chercher.

Tu penses peut-être que ça ne concerne que les gens célèbres ou les cibles de harcèlement, mais tu te trompes encore. Tes données personnelles ont de la valeur. Pour un employeur qui veut savoir si tu as des casseroles avant de t'embaucher. Pour un ex qui veut savoir où tu habites maintenant. Pour un arnaqueur qui veut te cibler avec une attaque de social engineering bien ficelée parce qu'il a trouvé sur LinkedIn où tu bosses et sur Facebook le nom de tes enfants. Pour l'État qui veut surveiller tes opinions politiques et te mettre sur une liste quelque part au cas où tu deviendrais un problème.

Le pire, c'est que tu as toi-même laissé la majorité de ces traces. Tu t'es inscrit sur des sites avec ton vrai nom, ton vrai email, ton vrai numéro de téléphone. Tu as posté des photos sur Facebook avec la géolocalisation activée. Tu as créé un compte LinkedIn avec ton CV complet. Et maintenant, tout ça traine sur des serveurs que tu ne contrôles pas, dans des bases de données qui se font pirater régulièrement, et tu ne peux rien faire pour l'effacer. Sauf que si, justement.

Nettoyer ses traces, c'est long, c'est chiant, c'est fastidieux, mais c'est faisable. Et si tu veux vraiment réduire ta surface d'attaque, tu n'as pas le choix. Ce chapitre, c'est le mode d'emploi pour faire valoir ton droit à l'effacement auprès des sites qui stockent tes données, supprimer tes résultats Google, opt-out des moteurs de reconnaissance faciale, et faire le grand ménage sur tes réseaux sociaux avant qu'un connard ne le fasse à ta place.

## La CNIL et le droit à l'effacement : ton arme légale

Depuis 2018, tu as un droit légal inscrit dans le Règlement Général sur la Protection des Données (RGPD), Article 17 : le droit à l'effacement. En gros, n'importe quel site web, n'importe quelle entreprise, n'importe quel service en ligne qui stocke tes données personnelles est légalement obligé de les supprimer si tu le demandes. Ton nom, ton email, ton adresse, ton historique de commandes, tes messages sur un forum, ton compte inactif depuis 2015 : tout ça doit disparaître sur simple demande de ta part.

Le site a un mois maximum pour répondre. S'il refuse ou s'il ne répond pas, tu peux déposer une réclamation auprès de la CNIL, et là ça devient leur problème, pas le tien. La CNIL peut mettre des amendes qui vont jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires mondial de l'entreprise. Donc en général, les sites suppriment tes données quand tu le demandes poliment, parce qu'ils n'ont pas envie que la CNIL débarque.

**Comment faire concrètement :**

Tu identifies les sites sur lesquels tu as un compte ou qui ont tes données. Copains d'avant, un vieux forum sur lequel tu as posté en 2010, un site e-commerce où tu as commandé une fois, un réseau social que tu n'utilises plus. Tu leur envoies un email avec une demande formelle d'effacement.

La CNIL met à disposition des modèles de courrier gratuits sur leur site. Tu utilises leur modèle, tu remplaces les champs avec tes infos, tu envoies par email à l'adresse de contact du site (cherche "contact" ou "protection des données" ou "DPO" sur leur site). Si tu ne trouves pas d'email, envoie par courrier postal recommandé avec accusé de réception à leur siège social.

Le site a 30 jours pour répondre. Soit il supprime tes données et te confirme par email, soit il refuse avec une justification légale (par exemple, si tu as une commande en cours ou s'il doit conserver tes données pour des raisons comptables ou légales pendant un certain délai). Si tu n'as pas de réponse après 30 jours, ou si le refus ne te semble pas justifié, tu vas sur le site de la CNIL et tu remplis le formulaire de réclamation en ligne. La CNIL contactera le site directement et fera le sale boulot pour toi.

**Cas concrets où ça marche :**

**Copains d'avant** : Ce site de réseau social vintage que personne n'utilise plus mais qui affiche toujours ton profil avec ton vrai nom, ta ville, ton ancien lycée. Si tu t'es inscrit il y a plus de 2 semaines, tu peux demander la suppression par email à equipe@copainsdavant.com. Ils ont un délai de rétractation de 2 semaines après inscription, passé ce délai il faut faire une demande RGPD classique.

**Anciens employeurs** : Si une ancienne boîte conserve encore ton dossier RH avec tes données persos alors que tu es parti depuis 5 ans, tu peux demander l'effacement (sauf s'ils ont une obligation légale de conserver certaines données pendant un délai précis, genre bulletins de salaire).

**Sites e-commerce** : Tu as commandé une fois en 2017, tu n'as jamais racheté, mais le site garde toujours ton compte avec ton nom, adresse, historique de commandes. Demande d'effacement, ils suppriment tout sauf les données qu'ils doivent légalement conserver pour la comptabilité (factures, etc.).

**Forums et vieux comptes** : Un forum sur lequel tu as posté sous ton vrai nom il y a 10 ans. Demande d'effacement, ils anonymisent ou suppriment tes posts.

Le droit à l'effacement, c'est ton arme légale pour faire disparaître tes traces des bases de données que tu ne contrôles pas. Ça ne marche pas à 100% (certains sites ont des obligations légales de conserver certaines données pendant des délais précis), mais dans la majorité des cas, tu obtiendras gain de cause.

## Google et le droit à l'oubli : effacer tes résultats de recherche

Google indexe tout. Les articles de presse où ton nom apparaît, les vieux profils sur des forums que tu as oubliés, les photos que quelqu'un a posté il y a 10 ans lors d'un événement où tu étais présent, les mentions de ton nom dans des documents publics. Tape ton nom et ton prénom dans Google, et il y a de fortes chances que tu trouves des résultats que tu préférerais voir disparaître. Un article de presse sur une affaire judiciaire classée sans suite. Une photo embarrassante. Un commentaire que tu as posté en 2012 sous ton vrai nom et que tu regrettes aujourd'hui.

Le problème, c'est que même si tu supprimes le contenu à la source (tu contactes le site qui héberge la page, ils la suppriment), Google continue d'afficher le résultat pendant des semaines ou des mois parce que leur robot d'indexation n'est pas encore repassé sur le site. Et parfois, tu ne peux pas supprimer le contenu à la source parce que tu n'as aucun contrôle sur le site (article de presse, document public, etc.). Dans ce cas, ta seule option, c'est de demander à Google de supprimer le résultat de recherche.

### Le formulaire droit à l'oubli de Google

Google propose un formulaire en ligne pour demander la suppression de résultats de recherche te concernant, basé sur l'Article 17 du RGPD (droit à l'effacement). Tu remplis le formulaire, tu justifies pourquoi les résultats doivent être supprimés, Google examine ta demande, et si elle est valide, ils retirent les URLs de leurs résultats de recherche.

**Important :** La suppression est géolocalisée. Si Google accepte ta demande, les résultats disparaissent sur google.fr (et les autres domaines Google européens), mais ils restent visibles sur google.com (États-Unis) et les autres domaines hors Europe. Quelqu'un qui



Pour aller plus loin, rejoins Le Ƀunker sur YouTube

cherche ton nom depuis les États-Unis ou avec un VPN américain verra toujours les résultats. Ce n'est pas un effacement total, c'est un effacement pour les recherches effectuées depuis l'Union Européenne.

**Comment ça marche :**

Tu vas sur le formulaire de suppression Google (cherche "droit à l'oubli Google" ou "Google RTBF form"). Tu remplis :

- Ton nom, prénom, email
- Les URLs des résultats que tu veux supprimer
- La justification : pourquoi ces résultats sont obsolètes, non pertinents, ou excessifs

Google traite la demande sous plusieurs semaines. Soit ils acceptent et les URLs disparaissent des résultats de recherche européens, soit ils refusent avec une justification. Les critères de Google pour accepter une demande : l'information doit être obsolète (un vieux fait divers qui n'a plus d'intérêt public aujourd'hui), non pertinente (un résultat qui ne te concerne pas vraiment ou qui n'a aucun intérêt légitime), ou excessive (des données sensibles qui n'ont pas à être publiques).

**Si Google refuse :**

Si Google refuse ta demande et que tu penses qu'ils ont tort, tu peux déposer une réclamation auprès de la CNIL. La CNIL examinera ton dossier et pourra ordonner à Google de supprimer les résultats si elle estime que ta demande est légitime. Google a déjà été condamné plusieurs fois par la CNIL pour avoir refusé des demandes valides.

**Limite importante :**

Le droit à l'oubli ne s'applique pas si l'information a un intérêt public légitime. Si tu es une personnalité publique (politique, chef d'entreprise, artiste), ou si l'information concerne une affaire judiciaire récente ou d'intérêt général, Google refusera probablement ta demande. Le droit à l'oubli, c'est pour le Nicolas moyen qui a des vieux résultats embarrassants mais sans intérêt public, pas pour les gens qui veulent cacher des affaires graves.

## PimEyes : quand ton visage devient traçable

PimEyes, c'est un moteur de recherche par reconnaissance faciale. Tu upload une photo de toi, et il te trouve toutes les autres photos de toi qui circulent sur internet. Réseaux sociaux, articles de presse, sites web, forums, blogs : si une photo de ton visage est publique quelque part, PimEyes la trouve. La technologie utilise des algorithmes de reconnaissance faciale biométrique qui analysent les traits de ton visage et les comparent à des millions de photos indexées sur le web.

Tu penses peut-être que ça ne concerne que les gens célèbres ou les victimes de harcèlement, mais en réalité, n'importe qui peut utiliser PimEyes pour te retrouver. Un employeur qui veut vérifier si les photos sur ton profil LinkedIn correspondent bien à toi. Un stalker qui veut savoir où tu traînes en cherchant des photos de toi géolocalisées. Un ex qui veut savoir avec qui tu es maintenant. Ou pire : quelqu'un qui a récupéré une photo de toi sur un réseau social et qui l'utilise pour te traquer en ligne.

Le problème, c'est que la reconnaissance faciale, c'est une donnée biométrique. Et les données biométriques sont considérées comme des données sensibles par le RGPD. En théorie, leur traitement est strictement encadré et nécessite ton consentement explicite. En pratique, PimEyes indexe des millions de visages sans demander l'autorisation à personne.

**Opt-out gratuit disponible**

PimEyes propose un formulaire d'opt-out gratuit sur leur site. Tu upload une photo de toi, tu remplis le formulaire, et PimEyes retire ton visage de leur index. Une fois exclu, quand quelqu'un cherchera avec une photo de toi, PimEyes ne retournera plus de résultats te concernant.

**Important :** L'opt-out PimEyes te retire uniquement de l'index PimEyes. Ça ne supprime pas les photos de toi sur les sites sources. Si une photo de toi est publiée sur un blog random, elle reste sur ce blog. PimEyes arrête juste de la montrer dans ses résultats de recherche. Pour supprimer les photos à la source, il faut contacter chaque site individuellement et faire une demande RGPD Article 17 (voir section précédente sur la CNIL).

**Comment faire l'opt-out :**

Va sur le formulaire d'opt-out PimEyes, upload une photo claire de ton visage, remplis le formulaire avec ton email, et soumets la demande. PimEyes traite la demande sous quelques jours et te confirme par email que ton visage a été retiré de leur index.

**Limite de l'opt-out gratuit :**

L'opt-out gratuit retire ton visage de l'index, mais ne te protège pas des futures photos que tu pourrais poster. Si tu post une nouvelle photo de toi demain sur Instagram, PimEyes pourrait l'indexer de nouveau. Pour une surveillance continue et des alertes automatiques quand une nouvelle photo de toi apparaît en ligne, PimEyes propose des abonnements payants. Mais on ne recommande évidemment pas de payer un service de surveillance faciale pour te protéger d'un service de surveillance faciale.

**Alternative : ne pas poster de photos de ton visage**

La meilleure protection contre la reconnaissance faciale, c'est de ne pas poster de photos de ton visage en ligne. Utilise des avatars, des pseudos, des photos de profil qui ne montrent pas ton visage. Si tu dois poster une photo de toi (LinkedIn, CV), limite la diffusion au minimum et désactive l'indexation par les moteurs de recherche dans les paramètres de confidentialité du site.

## Les data brokers : ceux qui vendent tes données

Les data brokers, c'est des entreprises dont le business model repose entièrement sur la collecte, l'agrégation, et la revente de tes données personnelles. Ils récupèrent des infos sur toi depuis des sources publiques (annuaires, réseaux sociaux, registres publics, bases de données gouvernementales) et des sources privées (achats de bases de données auprès d'autres entreprises, scraping de sites web, partenariats avec des sites e-commerce). Ils recoupent tout ça pour créer un profil complet sur toi : ton nom, ton adresse, ton numéro de téléphone, ton âge, ta situation familiale, tes revenus estimés, tes centres d'intérêt, tes habitudes d'achat. Et ils vendent ce profil à qui veut l'acheter : annonceurs, recruteurs, assureurs, agences de recouvrement, détectives privés.

Le truc, c'est que tu n'as jamais donné ton consentement à ces entreprises. Tu ne les connais même pas. Elles existent dans l'ombre, collectent tes données sans te demander ton avis, et les revendent sans que tu le saches. Aux États-Unis, c'est complètement légal et l'industrie pèse des milliards de dollars. En Europe, c'est censé être encadré par le RGPD, mais en pratique, les data brokers continuent d'opérer en exploitant des zones grises de la législation.

**En France et en Europe : moins de brokers, mais ils existent**

Le RGPD limite sérieusement l'activité des data brokers en Europe. Ils ne peuvent pas collecter et revendre tes données sans base légale, et tu as le droit de demander l'effacement (Article 17). Résultat : il y a beaucoup moins de data brokers actifs en France qu'aux États-Unis. Mais ils existent quand même : agrégateurs de données marketing, annuaires professionnels enrichis, bases B2B qui vendent des fichiers de contacts.

Le problème, c'est qu'ils sont difficiles à identifier. Tu ne sais pas qui a tes données, où elles sont stockées, à qui elles ont été vendues. Et les contacter un par un pour demander l'effacement, c'est un travail de titan.

**Solutions automatisées : Incogni et DeleteMe**

Des services comme Incogni et DeleteMe automatisent le processus de suppression. Tu leur paies un abonnement (environ 100€ par an), et ils envoient des demandes d'effacement RGPD en ton nom à des centaines de data brokers. Incogni revendique 420+ data brokers contactés, DeleteMe revendique 850 (mais seulement 181 pratiques en Europe, le reste étant des brokers américains qui ne sont pas soumis au RGPD).

**Attention : tu fais confiance à Incogni ou DeleteMe avec tes données**

Pour qu'Incogni ou DeleteMe puissent envoyer des demandes d'effacement en ton nom, tu dois leur fournir tes données personnelles : nom, prénom, adresse, email, numéro de téléphone. Tu leur donnes exactement les mêmes infos que celles que tu veux supprimer des data brokers. Le problème, c'est que tu déplaces ta confiance : au lieu de faire confiance à des data brokers inconnus, tu fais confiance à une entreprise privée qui centralise tes données pour te "protéger". Si Incogni ou DeleteMe se font pirater, ou s'ils décident de revendre tes données (ce qui serait illégal, mais pas impossible), tu te retrouves dans la même situation qu'avant, voire pire.

Ces services fonctionnent bien pour les data brokers connus et référencés. Ils envoient des demandes d'effacement régulièrement, surveillent que les brokers respectent la suppression, et renvoient des demandes si tes données réapparaissent. C'est pratique si tu n'as pas le temps ou l'énergie de le faire manuellement. Mais il faut comprendre le trade-off : tu gagnes du temps en échange de la confiance que tu accordes à ces services.

**Limite en France et en Europe :**

Ces services sont beaucoup moins efficaces en Europe qu'aux États-Unis parce qu'il y a structurellement moins de data brokers actifs. Incogni et DeleteMe ont été conçus pour le marché américain où des centaines de brokers opèrent ouvertement. En Europe, avec le RGPD, beaucoup de ces entreprises ne peuvent légalement pas opérer ou ont dû fermer. Donc tu paies 100€ par an pour contacter des brokers dont la majorité ne sont pas vraiment actifs en France.

**Alternative manuelle gratuite :**

Si tu veux économiser les 100€ par an et ne pas donner tes données à un tiers, tu peux faire le boulot toi-même. Google ton nom complet + "data broker" ou "annuaire professionnel", identifie les sites qui affichent tes données, envoie des demandes d'effacement RGPD Article 17 (utilise les modèles CNIL dont on a parlé plus haut). C'est long, fastidieux, tu vas passer plusieurs heures à envoyer des emails, mais c'est gratuit et légalement, les brokers sont obligés de répondre. Et surtout, tu ne confies tes données à personne d'autre.

**Vérifie si tes données ont fuité :**

Avant de t'attaquer aux data brokers, vérifie si tes données ont déjà fuité dans des piratages de bases de données. Va sur Have I Been Pwned, entre ton email, et le site te dira si ton email est apparu dans des fuites connues. Si c'est le cas, change immédiatement les mots de passe des comptes concernés (et utilise un gestionnaire de mots de passe comme on a vu au Chapitre 3).

Les data brokers, c'est l'ennemi invisible. Tu ne les vois pas, tu ne sais pas ce qu'ils ont sur toi, mais ils existent. Les services automatisés comme Incogni ou DeleteMe peuvent aider, mais ils comportent un risque de confiance et en Europe, leur efficacité est limitée par le fait qu'il y a moins de brokers actifs. L'alternative manuelle (Google + demandes RGPD) fonctionne, mais demande du temps.

## Réseaux sociaux : le grand ménage

Facebook, Instagram, X (Twitter), LinkedIn, TikTok, Snapchat : tu as probablement des comptes sur plusieurs de ces plateformes, et tu as probablement posté des centaines ou des milliers de publications, photos, commentaires au fil des années. Le problème, c'est que tout cet historique reste accessible indéfiniment. Tes vieux posts de 2015 où tu avais des opinions politiques que tu ne partages plus aujourd'hui. Les photos de soirées embarrassantes que tu as posté à 20 ans. Les commentaires impulsifs que tu as laissé sous des articles polémiques. Tout ça est encore là, indexable, searchable, et utilisable contre toi par un employeur, un recruteur, un ex, ou n'importe qui qui veut te nuire.

Les réseaux sociaux, c'est la plus grosse source de fuites volontaires de tes données personnelles. Tu as toi-même posté ces infos. Tu as accepté les conditions d'utilisation. Tu as cliqué sur "Publier". Et maintenant, tu ne contrôles plus rien. Facebook, Instagram, X, LinkedIn : ils possèdent tes données, et même si tu supprimes un post, il reste dans leurs bases de données et dans les archives de sites tiers qui ont scraped ton profil.

**Stratégie : supprimer, verrouiller, ou disparaître**

Tu as trois options pour réduire ta surface d'attaque sur les réseaux sociaux :

**1. Supprimer les vieux posts**

Si tu veux garder ton compte actif mais nettoyer ton historique, il existe des outils automatisés qui suppriment tes anciens posts en masse. Sur X (Twitter), des services comme TweetDelete ou Redact scannent ton historique et suppriment tous les tweets de plus de X mois/ans. Sur Facebook et Instagram, c'est plus compliqué parce que Meta ne propose pas d'API publique pour la suppression en masse, mais des outils comme Social Book Post Manager (extension Chrome) permettent de supprimer des posts par batch.

**Attention :** Ces outils nécessitent l'accès à ton compte (connexion via OAuth ou extension navigateur avec tes identifiants). Tu leur fais confiance avec tes identifiants de connexion. Lis bien les conditions d'utilisation et vérifie que l'outil est open source ou audité avant de l'utiliser.

**2. Verrouiller les paramètres de confidentialité**

Si tu veux garder ton compte et tes posts mais limiter qui peut les voir, passe en profil privé. Sur Instagram, active "Compte privé" dans les paramètres : seuls tes abonnés approuvés peuvent voir tes posts. Sur Facebook, limite la visibilité de tes posts aux "Amis uniquement" (pas "Public"). Sur X, active "Protéger vos posts" pour que seuls tes abonnés approuvés voient tes tweets. Sur LinkedIn, désactive "Rendre mon profil public" pour que seuls tes contacts puissent voir ton profil complet.

Vérifie aussi les paramètres d'indexation par les moteurs de recherche. Sur Facebook, va dans Paramètres > Confidentialité > Souhaitez-vous que les moteurs de recherche en dehors de Facebook renvoient vers votre profil ? → Désactive. Sur LinkedIn, désactive "Autoriser les recherches publiques" pour que ton profil ne soit pas indexé par Google.

**3. Supprimer les comptes inutilisés**

Si tu n'utilises plus un réseau social, supprime ton compte complètement. Attention : suppression ≠ désactivation. Quand tu "désactives" un compte Facebook ou Instagram, ton profil disparaît temporairement mais toutes tes données restent stockées sur les serveurs de Meta, et tu peux réactiver ton compte à tout moment. Quand tu "supprimes" ton compte, Meta a un délai de 30 à 90 jours pour effacer définitivement tes données (en théorie).

Pour supprimer un compte définitivement :

- **Facebook** : Paramètres > Vos informations Facebook > Désactivation et suppression > Supprimer définitivement le compte. Délai : 30 jours avant suppression définitive.
- **Instagram** : Compte > Supprimer votre compte (via navigateur web, pas l'app). Délai : 30 jours.
- **X (Twitter)** : Paramètres > Votre compte > Désactiver votre compte. Délai : 30 jours avant suppression définitive.
- **LinkedIn** : Paramètres > Gestion du compte > Fermer le compte. Délai : 14 jours.
- **TikTok** : Gérer le compte > Supprimer le compte. Délai : 30 jours.

Pendant le délai de grâce (30 jours en général), si tu te reconnectes, le compte est réactivé et la suppression est annulée. Passé ce délai, le compte et tes données sont censés être supprimés définitivement. Censés.

**Important :** Même après suppression, il est possible que des archives de tes posts circulent encore sur des sites tiers qui ont scraped ton profil (Internet Archive, bases de données de scraping, etc.). La suppression sur la plateforme ne garantit pas l'effacement total de tes traces sur internet.

Nettoyer ses traces, c'est pas un projet qu'on finit en une après-midi. C'est long, c'est répétitif, c'est chiant. Tu vas passer des heures à envoyer des emails de demande d'effacement, à remplir des formulaires, à vérifier que les sites ont bien supprimé tes données, à contacter la CNIL quand un site refuse de coopérer. Tu vas découvrir que ton nom apparaît sur des dizaines de sites dont tu ne te souvenais même plus. Tu vas réaliser que tes données ont circulé pendant des années sans que tu le saches.

Mais c'est nécessaire. Chaque trace que tu effaces, c'est un point de vulnérabilité en moins. Un employeur qui ne trouvera pas ton vieux commentaire politique sur un forum. Un ex qui ne pourra pas te localiser via PimEyes. Un arnaqueur qui n'aura pas ton adresse pour te cibler avec du social engineering. Un data broker qui ne pourra pas revendre ton profil à une agence de recouvrement.

Tu ne seras jamais complètement invisible. Il restera toujours des traces quelque part, des archives que tu ne pourras pas atteindre, des sites qui ignoreront tes demandes d'effacement, des données qui circuleront dans des bases privées inaccessibles. Mais tu auras réduit ta surface d'attaque. Et dans un monde où tes données personnelles sont une marchandise qui se vend et se revend sans ton consentement, réduire ta surface d'attaque, c'est déjà une victoire.

# PARTIE IV : TON ARGENT

Bitcoin, c'est LA pierre angulaire de toute stratégie de réduction de ta surface d'attaque.

Le pécore moyen pense que Bitcoin est risqué et stressant. C'est tout l'inverse. Avec Bitcoin, tu n'as pas de partie tierce qui va bloquer ton argent, te demander des preuves de provenance des fonds ou te geler ton épargne. Bitcoin te permet d'organiser ton insolvabilité. Tu deviens ce fameux SDF capitaliste dont on parle depuis le début.

Pourquoi les gens consentent-ils à l'impôt ? Parce que s'ils refusent, ils redoutent que l'État vienne saisir leurs biens. Bitcoin dénoyaute cette peur. Il casse le levier que les bolchéviques ont sur toi.

Reprends l'exemple des amendes Covid. Que se passe-t-il si quelqu'un qui a son épargne en Bitcoin et des revenus hors salariat refuse de payer ? Rien. Comme le Gitan, comme le mec de cité, comme le milliardaire, Bitcoin te donne accès à l'insolvabilité. Il remet au centre la notion de consentement et de choix.

Le but n'est pas de te pousser à frauder. Mais de te faire comprendre qu'adopter Bitcoin te permet de briser les chaînes qui t'attachent au système. Ça réduit drastiquement la capacité de coercition que la structure a sur toi.

Contrairement à ce que beaucoup voudraient faire croire, Bitcoin permet aussi de transacter de manière pseudonyme en gardant ta privacy. Les gens qui disent qu'il n'y a pas d'anonymat dans Bitcoin sont des incultes qui n'ont jamais mis les mains dans le cambouis. Il suffit d'avoir une bonne hygiène numérique.

Si tu es recherché par la CIA, quelle que soit la monnaie que tu utilises, tu finiras par faire une erreur et te faire gauler. Mais pour le commun des mortels qui ne veulent pas que Big Brother scrute leur activité financière, tout en ayant une réserve de valeur qui croît plus vite que l'inflation et que la plupart des classes d'actifs, Bitcoin est parfait.



Pour aller plus loin, rejoins Le ₿unker sur YouTube

# Chapitre 10 : Pourquoi Bitcoin

## Ton salaire doit passer par un compte bancaire

Ce n'est pas un hasard si l'État oblige les employeurs à payer ton salaire par virement bancaire dès que tu gagnes plus de 1 500 € net par mois. En dessous, tu peux demander à être payé en espèces, mais la plupart des employeurs refuseront. Au-dessus, c'est virement obligatoire.

Pourquoi ? Pour que ton argent transite par un compte bancaire. Comme ça, quand l'État a besoin de se servir, il sait où aller.

## Comment fonctionne la saisie

Tu dois de l'argent. Impôts, amendes, loyer, pension alimentaire, crédit. Peu importe. L'huissier ou l'État envoie un ordre à ta banque. Ta banque bloque ton compte. Elle garde 646,52 € (le Solde Bancaire Insaisissable, le montant du RSA), et vire le reste au créancier.

Tu ne reçois aucun avertissement. Un jour tu vérifies ton solde, il reste 646,52 €. Le reste est parti.

## Multiplier les comptes ne sert à rien

Tu penses que répartir ton argent sur plusieurs comptes va te protéger ? L'huissier et l'État ont accès au fichier FICOBA. C'est la liste de tous les comptes bancaires ouverts à ton nom en France. Ils saisissent tout d'un coup. Le SBI de 646,52 € est calculé sur l'ensemble de tes comptes, pas par compte.

## La solution

Ne jamais garder plus de 646,52 € sur l'ensemble de tes comptes bancaires. Tout le reste, tu le sors. En Bitcoin, en self-custody. Tes clés, tes bitcoins. Personne ne peut les saisir. Personne ne peut les geler.

## Tu ne possèdes rien

Pose-toi la question : est-ce que tu possèdes vraiment ton appartement, tes actions, ton assurance-vie ?

La réponse est non. Ce que tu as, ce sont des droits inscrits dans un registre contrôlé par l'État, et il peut les modifier quand il veut.

Ton appartement ? Tu es propriétaire tant que ton titre figure au cadastre. Si demain l'État décide de réquisitionner ton bien pour loger des migrants ou des sinistrés, il le fait. Si tu



Pour aller plus loin, rejoins Le ₿unker sur YouTube

ne paies pas tes impôts fonciers, il saisit. Tu ne détiens pas un bien physique inaliénable, tu détiens un droit révocable.

Tes actions ? Des lignes dans un fichier chez Euroclear. Tu as le droit de percevoir des dividendes, le droit de vendre tes parts, mais ces droits peuvent disparaître du jour au lendemain : nationalisation, taxation exceptionnelle, blocage des ventes. Ça s'est déjà vu.

Ton assurance-vie, ton PEL, ton Livret A ? Tu prêtes ton argent à une institution financière ou à l'État, et en échange ils te promettent de te le rendre avec des intérêts. Une promesse, rien de plus.

## Les précédents historiques

Si tu penses que l'État ne touchera jamais à l'épargne privée, l'histoire te donne tort.

Chypre, 2013. Les deux principales banques du pays sont au bord de la faillite. L'État et l'Union européenne élaborent un plan de sauvetage où tous les comptes sont gelés. Les dépôts de plus de 100 000 € servent à recapitaliser les banques : à la Bank of Cyprus, 47,5% disparaissent, et à Laiki, jusqu'à 80%. Les retraits sont limités à 100 € par jour pendant des semaines. Les Chypriotes se réveillent un matin et découvrent que leur épargne a fondu.

Grèce, 2015. Le gouvernement ferme les banques pour éviter un bank run et instaure un contrôle des capitaux. Les Grecs ne peuvent retirer que 60 € par jour, les virements à l'étranger sont interdits, et ils ne peuvent plus accéder à leur propre argent pendant des mois.

France, 1789. La Révolution nationalise les biens du clergé, soit entre 10% et 20% du territoire. En 1936, le Front populaire prend les industries d'armement et crée la SNCF. En 1945, nationalisation de Renault, des charbonnages, des quatre grandes banques (Crédit Lyonnais, Société Générale, Comptoir national d'escompte de Paris, Banque nationale pour le commerce et l'industrie), du gaz et de l'électricité. En 1982, Mitterrand nationalise Thomson, Saint-Gobain, Rhône-Poulenc, Paribas, Suez et plus de trente banques.

L'histoire montre une constante : quand l'État a besoin d'argent, il se sert, toujours au nom de l'intérêt général, de la justice sociale ou de la crise.

## Bitcoin change les règles

Bitcoin, c'est différent. Si tu détiens tes clés toi-même, tu as la capacité technique de recevoir et d'envoyer des bitcoins sans demander la permission à quiconque et sans intermédiaire. Personne ne peut geler ton wallet. Personne ne peut confisquer tes bitcoins sans tes clés privées.

Avec Bitcoin, tu contrôles vraiment ton argent au lieu d'avoir un simple droit révocable sur un fichier administratif. C'est la première fois dans l'histoire moderne qu'un actif financier échappe complètement au contrôle étatique, et c'est pour ça que Bitcoin est LA pierre angulaire de ta stratégie de réduction de surface d'attaque.

L'immobilier, les actions, l'épargne bancaire : ce ne sont que des permissions. Bitcoin, c'est de la propriété.

# Chapitre 11 : Acheter du Bitcoin

## Le pair-à-pair d'abord

Si tu en as la possibilité, le mieux pour obtenir des bitcoins c'est le pair-à-pair. Pas d'intermédiaire, pas de plateforme qui enregistre tes données. Tu échanges de l'argent contre des bitcoins avec quelqu'un, et personne d'autre n'a besoin de le savoir.

## Meetups Bitcoin et cash

La méthode la plus simple et la plus propre : tu vas à un meetup Bitcoin local et tu achètes en cash directement à quelqu'un. Pas de trace bancaire, pas de plateforme, pas de KYC. Juste un échange de billets contre des sats.

Tu trouves ton meetup sur btcmap.org ou en rejoignant les groupes Telegram de ta région. Tu te pointes, tu discutes avec d'autres bitcoiners, et si quelqu'un vend, tu achètes.

C'est aussi l'occasion de construire ton réseau. Ces personnes-là, tu pourras les recontacter plus tard pour acheter ou vendre directement. Le layer social est sous-estimé mais c'est la méthode la plus résiliente à long terme.

## Vendre un service en Bitcoin

Si tu es freelance, développeur, designer, rédacteur, consultant, propose d'être payé en Bitcoin. Pas besoin d'acheter, tu reçois directement des sats pour ton travail. C'est du Bitcoin 100% no-KYC et tu développes un side hustle en même temps.

Tu peux trouver des clients sur bitcoinerjobs.com ou workinbitcoin.com, ou mentionner que tu acceptes Bitcoin dans ta bio.

## Plateformes P2P sans KYC

Si tu ne peux pas acheter en cash ou via ton réseau, il existe des plateformes peer-to-peer qui permettent d'acheter sans donner ton identité. Le principe : tu es mis en relation avec quelqu'un qui vend du Bitcoin, vous vous mettez d'accord sur le prix et le mode de paiement, les fonds sont bloqués dans un escrow pendant l'échange, et une fois que le vendeur confirme avoir reçu ton paiement, les bitcoins sont libérés et arrivent dans ton wallet.

Tu paies généralement une prime de 5% à 10% au-dessus du cours des plateformes KYC. C'est le prix de l'anonymat.

Les principales solutions : **@lnp2pBot** (bot Telegram pour échanger en Lightning), **RoboSats** (accessible uniquement via Tor, Lightning Network, parfait pour les petits

montants), **Peach Bitcoin** (application mobile, virement SEPA ou Revolut), et **Bisq** (logiciel desktop 100% décentralisé, plus lent mais ultra-résilient).

## Acheter via une plateforme

Parfois tu n'as pas le choix. Tu veux acheter un gros montant et tu ne trouves personne en P2P qui vend autant. Ou tu n'as pas accès aux meetups dans ta région. Ou tu as besoin d'acheter rapidement et les plateformes P2P prennent trop de temps.

Dans ce cas, tu passes par une plateforme d'achat. Le problème des grandes plateformes généralistes (celles qui vendent 50 cryptos différentes), c'est qu'elles gardent tes bitcoins en custody. Tes coins restent chez eux, tu n'as pas les clés, et tu dépends de leur bon vouloir pour retirer. Si demain la plateforme fait faillite, gèle ton compte ou se fait pirater, tes bitcoins disparaissent.

La solution : privilégier les plateformes Bitcoin-only et non-custodial. Ces plateformes ne gardent pas tes bitcoins, elles te permettent d'acheter et de retirer immédiatement dans ton propre wallet. Tu contrôles tes clés dès l'achat.

## Retirer via Lightning ou Liquid

Lightning et Liquid sont des layer 2 de Bitcoin, des surcouches qui permettent des transactions plus rapides et plus confidentielles que sur la blockchain principale. Quand tu retires tes bitcoins via Lightning ou Liquid au lieu de la blockchain classique, tu bénéficies d'un haut niveau d'anonymat. Les montants et les adresses sont masqués, et personne ne peut suivre la vie de tes coins après l'achat.

Résultat : même si tu achètes avec KYC sur une plateforme, dès que tu retires via Lightning ou Liquid, le lien entre ton identité et tes bitcoins est cassé. La plateforme sait que tu as acheté, mais elle ne sait pas ce que tu fais avec tes coins après.

C'est pour ça que retirer via Lightning ou Liquid est systématiquement préférable à un retrait classique on-chain. Tu coupes la traçabilité dès la sortie de la plateforme.

**Notre recommandation : Bull Bitcoin**

Plateforme Bitcoin-only et non-custodiale qui te permet d'acheter du Bitcoin et de retirer instantanément via Lightning ou Liquid. Tu achètes, tu retires en 45 secondes, et tes bitcoins arrivent directement dans ton wallet.

→ 0,25 % de réduction sur tous tes achats et ventes à vie avec ce lien

# Chapitre 12 : Sécuriser tes bitcoins

## Self-custody

Tu as acheté du Bitcoin. Maintenant il faut le sécuriser. Si tu le laisses sur une plateforme d'achat, tu ne possèdes rien, tu as juste une promesse qu'ils te le rendront. Promesse qui peut disparaître du jour au lendemain si la plateforme fait faillite, se fait pirater, ou décide de geler ton compte.

La solution : retirer tes bitcoins dans un wallet où tu contrôles les clés privées. C'est ce qu'on appelle le self-custody, et c'est la seule manière de posséder vraiment tes bitcoins.

## Hot wallet vs cold wallet

Il existe deux types de wallets : les hot wallets, connectés à internet, et les cold wallets, qui ne le sont jamais.

Un **hot wallet** est une application sur ton téléphone ou ton ordinateur, pratique pour dépenser au quotidien mais moins sécurisée parce que ton appareil peut être piraté, infecté ou volé.

Un **cold wallet** est un appareil physique dédié (un hardware wallet) qui stocke tes clés hors ligne. Pour dépenser, tu dois physiquement connecter l'appareil à ton ordinateur et valider la transaction sur son écran. Même si ton ordinateur est infecté, le hacker ne peut rien faire parce que les clés ne quittent jamais le hardware wallet.

Hot wallet pour les petits montants du quotidien, cold wallet pour ton épargne.

## Le problème Ledger

Ledger est le hardware wallet le plus vendu, mais il a un gros problème : les fuites de données à répétition. 14 juillet 2020, 23 décembre 2020, 4 janvier 2026. À chaque fois, des centaines de milliers d'adresses complètes (nom, prénom, adresse postale, téléphone) finissent sur des forums. Ces bases de données sont dans la nature, accessibles à tout le monde, et les ingénieurs buveurs de Capri-Sun qui cherchent des cibles pour leurs crypto-rapts savent exactement qui a un Ledger chez lui.

Le problème n'est pas le hardware wallet en lui-même, mais le fait que si tu achètes un Ledger en donnant ton identité, tu deviens une cible. Des vagues de phishing par email, SMS, et même par courrier postal vont te tomber dessus pour te faire peur et te voler ta seed phrase.



Pour aller plus loin, rejoins Le ₿unker sur YouTube

## La solution : Bitcoin Bazar

Achète ton hardware wallet sans donner ton identité. La meilleure option en France et en Europe : Bitcoin Bazar, une boutique physique à Paris qui vend des hardware wallets en cash. Tu te déplaces, tu paies en espèces, tu repars avec ton appareil. Pas de nom, pas d'adresse, pas de trace.

Si tu ne peux pas te déplacer à Paris, commande en ligne et paie en Bitcoin. Demande une livraison en Locker Mondial Relay sous un faux nom (comme expliqué dans la Partie II). Tu récupères ton colis avec le code PIN, toujours sans donner ton identité.

# Chapitre 13 : Dépenser tes bitcoins

Tu as acheté du Bitcoin, tu l'as sécurisé dans ton hardware wallet. Très bien. Maintenant il faut pouvoir le dépenser. Parce que si ton Bitcoin reste bloqué dans ton cold wallet sans que tu puisses t'en servir pour payer ton loyer, tes courses ou ton billet d'avion, ça ne sert à rien.

Le problème, c'est que très peu de commerces acceptent Bitcoin directement. Tu ne vas pas chez Carrefour avec ton wallet Lightning pour payer tes courses. Le boucher du coin ne prend pas Bitcoin. Ton propriétaire veut un virement SEPA, pas des satoshis.

Donc il te faut des solutions pour pouvoir le dépenser.

## Vendre contre du cash

La méthode la plus propre et la plus résiliente pour convertir tes bitcoins en pouvoir d'achat, c'est de les vendre directement contre du cash. Pas de plateforme, pas d'intermédiaire, pas de données personnelles, pas de trace bancaire. Tu rencontres quelqu'un, tu lui envoies des bitcoins, il te donne des billets. Transaction terminée.

Cash is king comme on dit en anglais. Avec du liquide en poche, tu paies ton loyer, tes courses, ton essence, ton resto, sans laisser aucune trace.

Où trouver des acheteurs ? Meetups Bitcoin locaux (btcmap.org) ou directement dans ton réseau si tu connais des bitcoiners. Cette méthode est adaptée aux petits montants (quelques centaines d'euros) et doit toujours se faire dans des lieux publics et fréquentés : café, centre commercial, gare. Pour les gros montants, oublie le P2P cash, c'est trop risqué.



Pour aller plus loin, rejoins Le ₿unker sur YouTube

## Les cartes de paiement anonymes

Le problème avec le cash, c'est que tu ne peux pas payer tes abonnements en ligne (sauf ton VPN Mullvad ou IVPN comme vu en Partie III), commander sur Amazon, réserver un billet d'avion ou un Airbnb. Pour ça, il te faut une carte de paiement, et si tu passes par ta banque classique, chaque transaction laisse une trace consultable par l'administration fiscale et les huissiers.

La solution, ce sont les cartes Visa virtuelles rechargeables en Bitcoin. Le principe est simple : tu envoies du Bitcoin, la carte convertit instantanément en fiat, et tu dépenses partout où Visa est accepté. Amazon, Fnac, Netflix, Spotify, billets d'avion, réservations d'hôtel, tout fonctionne exactement comme avec une carte bancaire classique, sauf que ces cartes ne sont pas reliées à ton identité réelle.

**Maintenant, règle critique : ne jamais laisser des mille et des cents sur ces services. Les cartes de paiement anonymes peuvent se faire shutdown du jour au lendemain, et quand ça arrive, tu te réveilles un matin avec le site down et ton argent disparu. Ça s'est déjà vu des dizaines de fois. Donc tu recharges juste avant de dépenser, ne jamais laisser plus que nécessaire dessus.**

**Notre recommandation : FREEDOMIA**

Carte Visa virtuelle rechargeable en Bitcoin, acceptée partout où Visa fonctionne. Compatible Google Pay pour payer en tap-to-pay dans les commerces physiques. 2 mois offerts avec ce lien.

## Les cartes cadeau

Si tu veux dépenser tes bitcoins sans passer par une carte de paiement et sans donner ton identité, il existe une solution encore plus simple : acheter des cartes cadeau en Bitcoin. Tu paies en Bitcoin, tu reçois un code de carte cadeau par email en 30 secondes, et tu utilises ce code sur le site du marchand comme n'importe quelle carte cadeau classique. Aucun KYC, aucune donnée personnelle à fournir, aucun intermédiaire bancaire.

Bitrefill, c'est la plateforme de référence pour ça. Amazon, Fnac, Carrefour, Leclerc, Decathlon, SNCF, Uber Eats, Netflix, Spotify, PlayStation, Steam, tout y est. Tu veux faire tes courses alimentaires ? Tu achètes une carte cadeau Carrefour ou Leclerc pour 100 €, tu paies en Bitcoin, tu reçois ton code en 30 secondes, et tu vas faire tes courses. Tu veux commander sur Amazon ? Pareil, carte cadeau Amazon, tu paies, tu reçois le code, et tu commandes ce que tu veux.

C'est totalement anonyme, et ça ne laisse aucune trace dans le système bancaire classique. Tu dépenses directement tes bitcoins sans les convertir en euros sur un

compte bancaire, sans passer par une carte de paiement qui peut se faire shutdown, et personne ne peut relier ces achats à ton identité. Pour les courses, le carburant, les billets de train, les livraisons de resto, les abonnements streaming, c'est la méthode la plus propre.

Le seul inconvénient, c'est que tu es limité aux marchands disponibles sur Bitrefill, et que les reliquats sur les cartes sont difficilement dépensables. Si tu achètes une carte de 100 € et que tu dépenses 87 €, il te reste 13 € bloqués sur la carte que tu devras utiliser plus tard ou perdre. Mais pour 80% de tes dépenses quotidiennes, ça fonctionne parfaitement.

## Virement bancaire

Parfois, tu n'as pas le choix : tu ne peux payer ni par carte ni en cash. Ton propriétaire veut un virement SEPA pour le loyer, tu dois payer une facture, ou tu as un service à régler qui n'accepte que les virements bancaires, mais ton argent est en Bitcoin et tu ne veux pas passer par le circuit classique qui laisse des traces partout.

La solution, c'est Bull Bitcoin. Tu leur envoies des bitcoins, tu leur donnes les coordonnées IBAN du bénéficiaire (ton propriétaire, ton fournisseur, n'importe qui qui accepte les virements SEPA), et ils envoient directement le virement en euros à cette personne sans que les euros ne transitent jamais par ton compte bancaire. Tu paies en Bitcoin, le bénéficiaire reçoit des euros par virement classique, et si tu envoies tes bitcoins via Lightning avec un SEPA instant, c'est ultra rapide, quelques secondes entre ton envoi et la réception.

C'est une plateforme non-custodiale et Bitcoin-only, donc tu gardes le contrôle de tes bitcoins jusqu'au moment où tu décides de les envoyer pour faire le paiement, et les frais sont transparents.

**Notre recommandation : Bull Bitcoin**

Plateforme Bitcoin-only et non-custodiale pour payer par virement bancaire directement en Bitcoin.

→ 0,25% de réduction à vie avec ce lien

### Lightning : paiements directs

Quelques rares commerces acceptent Bitcoin en paiement direct, et la plupart du temps c'est via Lightning Network. Lightning, c'est une surcouche de Bitcoin qui permet des paiements instantanés avec des frais dérisoires, moins de 0,01 € par transaction, et contrairement à Bitcoin on-chain, Lightning est privé : les transactions ne sont pas enregistrées sur la blockchain publique, donc personne ne peut suivre ton historique de paiements ou connaître ton solde. Parfait pour payer un café, un resto, ou acheter en ligne sur un site qui accepte Bitcoin sans laisser de trace.

Le problème, c'est que très peu de commerces acceptent Lightning en France. Tu trouveras quelques cafés et restos dans les grandes villes comme Paris, Lyon ou Marseille, mais ne compte pas dessus pour tes achats quotidiens. Pour trouver les commerces qui acceptent Bitcoin, va sur btcmap.org, une carte mondiale qui référence tous les points de vente physiques et en ligne où tu peux payer en Bitcoin.

Lightning est surtout utile pour payer des services en ligne (Mullvad, IVPN, Bitcoin Bazar) ou pour les paiements entre particuliers.

La réalité du terrain, c'est que Lightning reste marginal en France pour l'instant. Utile si tu fréquentes des meetups Bitcoin où les gens acceptent Lightning pour vendre des objets ou des services, ou si tu achètes régulièrement sur des sites qui acceptent Bitcoin, mais pas assez répandu pour couvrir tes besoins quotidiens.

## Conclusion

Cette partie n'est pas là pour t'inciter à frauder. Elle est là pour te redonner le contrôle. La déclaration fiscale des plus-values Bitcoin est une obligation déclarative : c'est à toi de déclarer tes gains, pas aux plateformes ou aux intermédiaires de jouer les flics à ta place. Même avec les nouvelles règles de 2026 où les plateformes transmettront automatiquement tes transactions au fisc, la responsabilité de la déclaration reste sur toi. Il est temps de remettre cet aspect au centre : le consentement et le choix individuel, pas la surveillance automatique par des tiers.

Tu as maintenant tous les outils pour organiser ton insolvabilité et réduire drastiquement la capacité de coercition que la structure a sur toi.



Pour aller plus loin, rejoins Le ₿unker sur YouTube

# PARTIE V : TON TRAVAIL

Ton travail détermine ton niveau de liberté.

Si tu as un business physique ou un CDI en présentiel, tu es prisonnier d'une juridiction. Tu mets le gouvernement en position de monopole sur ta personne. Sans possibilité de mettre les États en concurrence, tu deviens la vache à traire pour financer le train de vie décadent de l'État.

Prends l'exemple d'un restaurateur. Il est coincé dans sa juridiction. Son local est là, ses équipements sont là, ses clients sont là. Il ne peut pas partir. Et l'État le sait. C'est pour ça que les restaurants et les entreprises du BTP sont les cibles privilégiées des contrôles fiscaux. Ils ne peuvent pas délocaliser, et leurs biens sont saisissables. Ils sont captifs.

Pendant le Covid, on a vu la même chose avec les salariés en présentiel. Tu voulais garder ton job ? Tu devais accepter la vaccination obligatoire. Tu n'avais pas le choix. Ceux qui travaillaient en remote ou qui avaient un business en ligne pouvaient dire non. Toi, tu courbais l'échine ou tu perdais ton revenu.

C'est pour ça qu'il faut “s'internetiser”. Développer du cash-flow en ligne. Pas nécessairement pour t'expatrier demain, mais pour ne pas être la pomme la plus basse du pommier. Pour avoir l'option de partir si le contrat social de l'endroit où tu vis ne te convient plus.

Parce que les États sont des agents rationnels. Ils se comportent comme des entreprises. Ils tondent les captifs qui sont sur leur territoire, et ils font les yeux doux aux mobiles qui peuvent partir. Regarde l'Article 155 B en France, le régime des impatriés. Si tu viens de l'étranger avec du capital mobile, tu bénéficies de 30% de ton salaire transformé en prime d'impatriation non imposée, et de 50% d'exonération sur tes revenus financiers étrangers. Pendant huit ans. Tout ça parce que tu es mobile. C'est ça, mettre les gouvernements en concurrence.

Quand tu n'es pas dépendant d'un seul pays, tu ne te fais plus un nœud à l'estomac chaque fois que tu vois une manifestation pour taxer les riches ou un politicien collectiviste qui fait une déclaration. Tu observes le cirque médiatico-politique avec légèreté, en sachant qu'ils ont une capacité de nuisance quasiment nulle sur toi.



Pour aller plus loin, rejoins Le Ƀunker sur YouTube

# Chapitre 14 : Le piège de l'attentisme

Maintenant que tu as compris que ton travail détermine ta liberté, on va parler du piège dans lequel tombent 90% des gens : attendre que quelqu'un d'autre résolve le problème à leur place.

Tu les connais, ces Nicolas qui passent leurs soirées devant BFM ou CNews, qui scrollent sur Twitter pour commenter la dernière déclaration de Macron, qui écoutent des podcasts politiques pendant deux heures par jour. Ils sont devenus des experts en analyse politique, ils savent exactement ce qui ne va pas dans le pays, ils peuvent te réciter par cœur les chiffres du déficit, les scandales du gouvernement, les déclarations des députés. Et à chaque élection, ils se disent la même chose : cette fois, c'est la bonne, si X passe, tout va changer, on va enfin pouvoir respirer.

Et puis X passe, ou X ne passe pas, et rien ne change. Ou pire, ça empire. Alors ils recommencent, ils attendent la prochaine élection, ils suivent les sondages, ils débattent sur les forums, ils partagent des articles, ils s'indignent, ils espèrent. Et pendant ce temps, leur vie n'avance pas.

Consommer du contenu politique, c'est un sédatif émotionnel. Ça te donne l'illusion que tu fais quelque chose, que tu es engagé, que tu comprends les enjeux, mais en réalité, tu ne fais rien. Tu délègues ta responsabilité à un politicien providentiel qui va tout régler à ta place, sauf que ce politicien n'existe pas. Même si par miracle quelqu'un de bien arrivait au pouvoir, le système est structurellement cassé : la dette est trop élevée, les engagements sociaux sont trop lourds, la machine administrative est trop obèse. Personne ne peut inverser la tendance sans provoquer une révolution.

Pendant que tu passes deux heures par jour à t'énerver devant des talk-shows, tu aurais pu utiliser ces deux heures pour apprendre une compétence qui te rapporte de l'argent en ligne. Développement web, design, rédaction, montage vidéo, consulting, n'importe quoi. En un an, à raison de deux heures par jour, tu peux devenir suffisamment compétent pour facturer tes premiers clients. En deux ans, tu peux remplacer ton salaire. En trois ans, tu peux être complètement mobile.

Mais non, à la place, tu attends que Zemmour, Bardella, Asselineau ou n'importe quel autre sauveur providentiel vienne tout régler, et pendant ce temps, l'État continue de te tondre, les taxes augmentent, les contrôles se multiplient, et tu restes coincé au même endroit avec le même boulot que tu détestes.

La vérité, c'est qu'aucun politicien ne viendra te sauver. Le système est trop ancré, les intérêts sont trop puissants, les engagements sont trop lourds. La seule personne qui peut te sortir de là, c'est toi, et la seule manière de le faire, c'est de devenir mobile. Pas en déménageant demain à Dubaï, mais en développant des sources de revenus qui ne



Pour aller plus loin, rejoins Le Ƀunker sur YouTube

dépendent pas d'un lieu physique, comme ça, si demain le contrat social devient insupportable, tu as l'option de partir. Et cette option, c'est ce qui change tout.



Pour aller plus loin, rejoins Le Ƀunker sur YouTube

# Chapitre 15 : Business en ligne

Maintenant qu'on a compris qu'il faut devenir mobile, parlons concret. Comment tu développes du cash-flow en ligne quand tu pars de zéro, que tu as un CDI à temps plein, et que tu ne sais pas coder ?

La bonne nouvelle, c'est qu'en 2026, tu n'as jamais eu autant d'opportunités pour gagner de l'argent en ligne. La mauvaise nouvelle, c'est que 99% des gens n'en profiteront jamais parce qu'ils préfèrent attendre que leur situation se dégrade plutôt que d'agir.

## Les modèles qui marchent

Il existe quatre grandes catégories de business en ligne qui permettent de générer du cash-flow sans être attaché à un lieu physique.

**Le freelance.** Tu vends ton temps et tes compétences à des clients qui paient. Développement web, design graphique, rédaction de contenu, montage vidéo, consulting en marketing, traduction, gestion de réseaux sociaux. La liste est infinie. Tu n'as besoin de rien d'autre qu'un laptop et une connexion internet. Les plateformes comme Upwork, Fiverr, Malt ou Codeur te mettent directement en contact avec des clients qui cherchent exactement ce que tu proposes. Le problème du freelance, c'est que tu échanges ton temps contre de l'argent, donc tu restes limité par le nombre d'heures dans une journée. Mais c'est un excellent point de départ pour remplacer ton salaire.

**L'e-commerce et le dropshipping.** Tu vends des produits physiques sans jamais toucher de stock. Tu crées une boutique en ligne, tu trouves un fournisseur qui s'occupe de l'entreposage et de la livraison, et tu te concentres uniquement sur le marketing et les ventes. Shopify, WooCommerce, Amazon FBA. Les outils existent, ils sont accessibles, et des milliers de gens gagnent leur vie avec ça. Le piège, c'est de croire que c'est facile. Ça demande du boulot, de la discipline, et une bonne compréhension du marketing digital. Mais une fois que ça tourne, tu peux scaler sans limite géographique.

**La création de contenu.** YouTube, podcast, newsletter, blog. Tu crées du contenu sur un sujet que tu maîtrises, tu construis une audience, et tu monétises via la publicité, les sponsors, l'affiliation, ou la vente de tes propres produits digitaux. Le problème, c'est que ça prend du temps avant de générer du cash. Mais une fois que ta base est construite, tu peux gagner de l'argent pendant que tu dors. Des milliers de créateurs vivent uniquement de ça, sans jamais avoir besoin d'un bureau physique ou d'un patron.

**Les produits digitaux et le SaaS.** Tu crées un logiciel, une formation en ligne, un template, un ebook, n'importe quel produit numérique que tu vends en ligne. Une fois créé, tu peux le vendre à l'infini sans coût de production supplémentaire. C'est le modèle le plus scalable qui existe. Si tu sais coder, tu peux créer un SaaS (Software as a Service) et facturer un abonnement mensuel. Si tu ne sais pas coder, tu peux créer une formation sur



Pour aller plus loin, rejoins Le Ƀunker sur YouTube

un sujet que tu maîtrises et la vendre sur des plateformes comme Système.io, Podia ou Skool.

## Recevoir des paiements

Une fois que tu as un business en ligne, il faut pouvoir encaisser l'argent. Et là, tu as deux options : fiat ou crypto.

**Pour le fiat classique**, tu as Stripe pour accepter les paiements par carte bancaire, Wise pour recevoir des virements internationaux sans te faire plumer par les frais bancaires, et PayPal si tu n'as vraiment pas le choix, mais à éviter si possible parce qu'ils adorent bloquer les comptes sans raison.

**Pour le Bitcoin**, tu as BTCPay Server, qui est une solution auto-hébergée, open-source, et sans frais. Tu peux accepter des paiements Lightning instantanés, et personne ne peut te bloquer ton argent. Si tu vends à une audience internationale, accepter Bitcoin te permet de diversifier géographiquement ta base de clients sans te soucier des frais de change ou des restrictions bancaires. Un client en Argentine, au Liban ou au Nigeria peut te payer en Bitcoin sans friction, alors qu'un virement bancaire classique prendrait des jours et coûterait une fortune en frais.

La stratégie intelligente, c'est de proposer les deux. Fiat pour les clients qui n'ont pas encore adopté Bitcoin, et Bitcoin pour ceux qui veulent éviter les intermédiaires bancaires.

## La structure juridique

Maintenant, parlons de comment tu structures tout ça légalement.

Si tu débutes et que tu es en France, tu peux commencer en auto-entrepreneur. C'est simple, rapide à mettre en place, et tu paies tes cotisations sur ton chiffre d'affaires. Par contre, tu as un plafond : 77 000 € pour les services, 188 000 € pour la vente de marchandises. Une fois que tu dépasses ça, tu dois passer en société.

Si tu vises international ou que tu veux optimiser ta fiscalité, tu peux créer une société étrangère. Une LLC aux États-Unis (Wyoming ou Delaware), une société offshore au Panama, en Uruguay, ou ailleurs. Mais attention, créer une société étrangère ne signifie pas que tu échappes automatiquement à l'impôt. Si tu es résident fiscal en France, tu dois déclarer tes revenus en France, peu importe où ta société est enregistrée. La structure étrangère devient intéressante si tu changes aussi de résidence fiscale.

Le moment où ça commence à avoir du sens de basculer en société étrangère, c'est quand tu dépasses les 100 000 € de chiffre d'affaires par an, ou quand tu veux structurer ton patrimoine de manière plus résiliente. À ce stade-là, tu consultes un fiscaliste qui connaît l'optimisation internationale, et tu mets en place une structure propre.

## Par où commencer

Si tu es salarié à temps plein et que tu veux développer un side hustle, la première étape est de choisir un modèle qui correspond à tes compétences actuelles ou à celles que tu veux acquérir. Tu ne vas pas te lancer dans le dropshipping si tu détestes la logistique, et tu ne vas pas faire du freelance en développement web si tu n'as aucune appétence pour le code.

Commence par une compétence que tu peux monétiser rapidement. Rédaction, design, montage vidéo, consulting, traduction, gestion de réseaux sociaux. Quelque chose où tu peux facturer tes premiers clients dans les trois à six mois. Les plateformes comme Upwork, Malt, Fiverr, LinkedIn sont là pour ça. Tu proposes tes services, même si au début tu facturas moins cher parce que tu n'as pas encore de portfolio.

Une fois que tu as tes premiers clients et que tu génères du cash régulier, tu peux scaler ou pivoter vers un modèle plus scalable : création de contenu, produits digitaux, SaaS. Mais l'erreur que font 99% des gens, c'est de vouloir tout faire en même temps. Ils lancent un YouTube, un podcast, un ebook, un cours en ligne, et au final, ils ne finissent rien. Commence par un seul modèle, maîtrise-le, puis diversifie.

La plupart des gens ne le feront jamais. Ils préféreront rester coincés dans leur CDI, à se plaindre de leur patron, à râler contre le gouvernement, à attendre que quelqu'un d'autre vienne les sauver. Et dans dix ans, ils seront exactement au même endroit.

Toi, tu as le choix. Soit tu continues comme avant, soit tu décides qu'aujourd'hui, c'est le jour où tu commences à construire ta mobilité. Et dans un an, ta vie aura complètement changé.

S'internetiser, ce n'est pas une fin en soi. C'est la première étape.

Une fois que tu as développé du cash-flow en ligne, que tu as compris comment fonctionne le freelance, l'e-commerce, la création de contenu ou les produits digitaux, tu débloques une nouvelle liberté : celle de choisir où tu vis, où tu paies tes impôts, et sous quelle juridiction tu places tes actifs.

Mais devenir mobile ne suffit pas. Il faut maintenant structurer cette mobilité de manière intelligente. Parce qu'avoir un business en ligne tout en restant résident fiscal en France, c'est comme avoir une Ferrari dans un garage fermé : tu as l'outil, mais tu ne l'utilises pas à son plein potentiel.

# PARTIE VI : TA JURIDICTION

Les Américains disent souvent que "if Bitcoin is king, passport is queen". Et ils n'ont pas tort. Avoir un deuxième ou un troisième passeport, établir des résidences dans plusieurs pays, et choisir stratégiquement ta résidence fiscale, c'est l'attirail du nomade capitaliste.

Ton passeport détermine où tu peux voyager. Ta résidence détermine où tu vis. Ta résidence fiscale détermine où tu paies tes impôts. Et ces trois éléments peuvent être dans trois pays différents.

Mon ami iranien ne me contredira pas : il ne peut aller que dans 35 pays dans le monde sans visa. Donc, s'il veut se déplacer à l'étranger, il doit prendre rendez-vous à l'ambassade, expliquer son projet, prouver qu'il a une situation financière stable. Ça prend des mois, et bien souvent, c'est refusé.

Un second passeport fait partie de ton patrimoine que tu légueras à tes enfants. Il te permettra peut-être de quitter le territoire quand nos politiciens européens partiront en guerre en Russie ou imposeront un confinement écologique. Et optimiser où tu paies tes impôts, c'est la différence entre garder 70% ou 30% de ce que tu gagnes.

Nous ne sommes pas les premiers à nous poser ces questions de résilience et d'équilibre de force. La théorie des drapeaux a été conceptualisée par l'auteur libertarien Harry D. Schultz dans les années 60-70 avec trois drapeaux, puis étendue à cinq drapeaux par WG Hill, et aujourd'hui certains parlent même de sept drapeaux. L'idée : répartir les différents aspects de ta vie (nationalité, résidence, résidence fiscale, business, actifs, lifestyle) dans plusieurs pays pour gagner en résilience et éviter de subir les sauts d'humeur fiscaux du gouvernement.

C'est comme en entrepreneuriat. Si ton business n'a qu'un seul et unique client, tu te mets en position de vulnérabilité. Si jamais tu le froisses ou s'il te prend en grippe, c'est tout ton business qui risque de s'effondrer. Donc tu fais des concessions, tu courbes l'échine, et tu acceptes tous ses caprices. Mais si tu as plusieurs clients, tu as de la flexibilité.



Pour aller plus loin, rejoins Le ₿unker sur YouTube

# Chapitre 16 : Les passeports comme patrimoine

Un passeport, ce n'est pas juste un document pour passer les contrôles à l'aéroport. C'est un actif à vie, transmissible à tes enfants, qui garantit ta mobilité et ta sécurité dans un monde de plus en plus instable.

Pendant le COVID, certains ne pouvaient pas quitter leur pays. Leurs frontières étaient fermées, leurs passeports ne valaient plus rien. Pendant ce temps, d'autres jonglaient entre leurs deux ou trois nationalités pour circuler librement. La mobilité est devenue un luxe rare, et ceux qui avaient investi dans un second passeport ont compris la valeur de cet actif.

Un second passeport te donne accès à des systèmes consulaires différents. Si un pays te bloque, tu peux utiliser l'autre. Si une zone géopolitique devient hostile à ta nationalité, tu peux jongler. C'est de l'assurance. Et comme toute assurance, tu espères ne jamais en avoir besoin, mais quand tu en as besoin, elle vaut de l'or.

Maintenant, parlons concret. Comment tu obtiens un second passeport ?

**Par filiation ou ascendance.** Si tu as des grands-parents italiens, polonais, irlandais, portugais ou espagnols, tu peux potentiellement demander la nationalité par droit du sang. Ça demande de la recherche généalogie, des documents administratifs, et de la patience. Ça prend entre un et trois ans selon le pays, mais une fois que c'est fait, c'est pour la vie. Et tes enfants en héritent automatiquement.

**Par résidence.** Tu vis dans un pays pendant un certain nombre d'années, tu apprends la langue, tu passes un test de culture générale, et tu obtiens la nationalité. Uruguay et Paraguay te demandent trois ans. Panama, cinq ans. Portugal, cinq ans. Espagne, dix ans. C'est long, mais si tu prévois de t'installer quelque part, autant en profiter pour obtenir le passeport.

**Par investissement.** Les pays des Caraïbes comme Saint-Kitts, la Dominique ou Antigua te vendent un passeport pour 100 000 à 200 000 dollars. Malte te le vend pour 600 000 à un million d'euros. C'est rapide, entre six et douze mois, mais c'est coûteux. Et attention, certains de ces passeports sont moins respectés. Tu auras parfois besoin d'un visa pour entrer dans l'Union Européenne ou aux États-Unis, alors que ton passeport français te donne déjà cet accès.

**Par mariage.** Tu épouses un(e) national(e) d'un pays cible, et après quelques années, tu peux demander la nationalité. Ça dépend du pays, mais c'est une voie classique.

Tous les passeports ne se valent pas. Évite les pays en guerre, sous sanctions internationales, ou les dictatures. Un passeport russe, chinois, nord-coréen ou



Pour aller plus loin, rejoins Le Ƀunker sur YouTube

vénézuélien peut devenir un boulet qui t'empêche de voyager plutôt qu'un actif qui te facilite la vie.

Si tu es français, tu as déjà accès à 27 pays de l'Union Européenne sans visa. Un passeport italien, espagnol ou portugais serait redondant, sauf si tu as des raisons spécifiques. Par contre, un passeport d'Amérique du Sud comme l'Uruguay ou le Paraguay, c'est facile à obtenir avec trois ans de résidence, et ça te donne accès au Mercosur. Un second passeport idéal, c'est celui qui complète géographiquement ton passeport français. Turc, brésilien, argentin. Des zones où les Européens ont plus de difficulté à circuler.



Pour aller plus loin, rejoins Le ₿unker sur YouTube

# Chapitre 17 : La résidence fiscale

Ta résidence fiscale, c'est le pays où tu es considéré comme résident aux yeux du fisc. Et c'est ce pays qui détermine combien d'impôts tu paies, sur quels revenus, et à quel taux.

C'est différent de ta nationalité et de ta résidence administrative. Tu peux être français de nationalité, vivre six mois par an au Portugal, et être résident fiscal au Panama. Les trois sont indépendants.

La règle générale, c'est que si tu passes 183 jours par an dans un pays, tu deviens résident fiscal de ce pays. Mais ce n'est pas le seul critère. Certains pays considèrent que tu es résident fiscal si tu y as ton centre d'intérêts économiques, ou si tu y as ton foyer familial permanent. En France, les critères sont alternatifs : un seul suffit pour être considéré résident fiscal français. Tu n'as pas besoin de passer 183 jours en France pour être considéré résident fiscal français si ta famille y vit ou si tes intérêts économiques y sont.

Le problème avec la France, c'est que si tu es résident fiscal français, tu paies l'impôt sur ton revenu mondial. Peu importe que tu aies gagné cet argent au Panama, en Uruguay ou à Dubaï. Si tu es résident fiscal français, le fisc français veut sa part. Et si tu as plus de 800 000 euros d'actifs et que tu décides de partir, tu paies une exit tax sur les plus-values latentes de tes actifs. C'est une taxe de sortie. Tu paies l'impôt sur des gains que tu n'as pas encore réalisés, juste parce que tu as décidé de partir.

Changer de résidence fiscale, ce n'est pas juste prendre un billet d'avion et dire au revoir. Il y a des étapes administratives à respecter.

Première étape : tu déclares ton départ aux impôts français. Tu remplis un formulaire, tu expliques où tu pars, et tu prouves que tu établis ta résidence ailleurs.

Deuxième étape : tu établis ta résidence dans ton pays cible. Ça veut dire un bail de location ou un achat immobilier, des factures d'électricité, d'internet, des preuves que tu es physiquement présent. Certains pays te demandent d'ouvrir un compte bancaire local, de t'inscrire à la sécurité sociale locale, bref, de prouver que tu vis vraiment là-bas.

Troisième étape : tu obtiens un certificat de résidence fiscale du nouveau pays. Ce document prouve au fisc français que tu es maintenant résident fiscal ailleurs.

Les pièges à éviter : garder un compte bancaire français avec des centaines de milliers d'euros dessus, c'est un signal que ton centre d'intérêts économiques est encore en France. Revenir trop souvent en France, plus de 183 jours par an, ça pose problème. Et si ta famille reste en France, le fisc peut considérer que ton foyer permanent est encore en France, donc tu restes résident fiscal français.



Pour aller plus loin, rejoins Le Ƀunker sur YouTube

L'exit tax s'applique si tu as plus de 800 000 euros d'actifs : crypto, actions, parts de société, tout ce qui peut générer une plus-value. Le fisc français calcule la plus-value latente au jour de ton départ et te demande de payer l'impôt dessus, même si tu n'as pas vendu. Il existe un sursis de paiement si tu pars dans un pays de l'Union Européenne ou de l'Espace Économique Européen, mais si tu pars au Panama, en Uruguay ou à Dubaï, tu paies immédiatement.

Maintenant, parlons des pays à fiscalité attractive pour les entrepreneurs digitaux.

Le Panama ne taxe pas les revenus étrangers. Si tu gagnes de l'argent en ligne en facturant des clients hors du Panama, tu ne paies pas d'impôt au Panama. Tu peux obtenir un visa de résidence facilement via le programme Friendly Nations, et la qualité de vie est correcte. Le coût de la vie est modéré.

L'Uruguay a changé son système en 2026. Depuis janvier 2026, les revenus de capital étrangers sont taxés à 12%. Mais si tu deviens résident fiscal uruguayen à partir de 2026, tu peux bénéficier du Tax Holiday 2.0 qui te donne dix ans d'exonération sur tes revenus étrangers, à condition d'investir 2 millions de dollars en immobilier uruguayen ou 100 000 dollars par an dans un fonds d'innovation gouvernemental. La résidence est facile à obtenir, et après trois ans, tu peux demander le passeport. La qualité de vie est élevée, mais le coût de la vie aussi.

Le Paraguay applique un impôt territorial. Seuls les revenus générés localement sont taxés. Si tu gagnes de l'argent en ligne en facturant des clients étrangers, tu ne paies rien. La résidence est très facile à obtenir, et le coût de la vie est très bas.

Dubaï, c'est zéro pour cent d'impôt sur le revenu. Par contre, il y a une TVA de 5%, et le coût de la vie est élevé. Tu peux obtenir un visa de résidence en montant une société ou en devenant freelance. Le climat est rude, surtout l'été.

Le Portugal avait un régime fiscal avantageux pour les nouveaux résidents, le NHR, Non-Habitual Resident. Mais ce régime a été supprimé en 2024. Ne compte plus dessus.

Certaines îles comme l'île Maurice offrent aussi une fiscalité attractive, mais l'isolement géographique peut être un problème.

Disclaimer : avant de changer de résidence fiscale, consulte un fiscaliste qui connaît l'optimisation internationale. Chaque situation est unique, et une erreur administrative peut te coûter cher.



Pour aller plus loin, rejoins Le ₿unker sur YouTube

# Chapitre 18 : La théorie des 5 drapeaux

Maintenant qu'on a parlé des passeports et de la résidence fiscale, on va voir comment tout ça s'articule dans une stratégie globale. C'est là qu'intervient la théorie des drapeaux.

L'idée, c'est de répartir les différents aspects de ta vie dans plusieurs juridictions pour maximiser ta liberté et ta résilience. Au lieu de tout concentrer dans un seul pays, tu divises : ta nationalité dans un pays, ta résidence fiscale dans un autre, ton business dans un troisième, tes actifs dans un quatrième, et tu vis dans un cinquième.

Voilà les cinq drapeaux.

**Premier drapeau : la nationalité.** C'est ton passeport. Idéalement, tu en as deux ou trois, complémentaires géographiquement. Un passeport européen pour circuler en Europe, un passeport d'Amérique du Sud pour le Mercosur, peut-être un passeport turc ou du Moyen-Orient pour d'autres régions. Plus tu as de passeports, plus tu as de liberté de mouvement.

**Deuxième drapeau : la résidence fiscale.** C'est le pays où tu paies tes impôts. L'idéal, c'est un pays à fiscalité basse ou nulle pour les entrepreneurs digitaux. Panama, Uruguay, Paraguay, Dubaï. Tu ne paies pas d'impôt sur tes revenus étrangers, et tu peux vivre ta vie sans que le fisc te prenne la moitié de ce que tu gagnes.

**Troisième drapeau : le business.** C'est le pays où est immatriculée ta société. L'idéal, c'est un pays stable, avec une administration efficace, un accès à un marché de clients riches, et zéro pour cent de taxe sur les profits. Par exemple, une LLC aux États-Unis, dans le Wyoming ou le Delaware. Si tu n'es pas résident fiscal américain, tu ne paies pas d'impôt aux États-Unis sur les profits de ta LLC. Et tu bénéficies de la crédibilité d'une société américaine pour facturer des clients internationaux.

**Quatrième drapeau : les actifs.** C'est le pays où tu détiens tes biens. Actions, immobilier, Bitcoin. L'idéal, c'est un pays qui respecte la sacralité de la propriété, avec une situation politique stable, et où une prise de pouvoir socialo-communiste n'est pas envisageable. La Suisse, Singapour. Ou alors, Bitcoin. Parce que Bitcoin n'a pas de juridiction. Ton Bitcoin n'est physiquement nulle part. Il est dans la “blockchain” et pour y accéder, tu possèdes un secret qui est dans ta tête si tu as mémorisé ta phrase de récupération (peu recommandé, la mémoire est faillible), ou sur ton Hardware Wallet et tes backups. Aucun gouvernement ne peut le saisir sans ta coopération.

**Cinquième drapeau : le lifestyle.** C'est le pays où tu vis au quotidien, sans être résident fiscal. Tu y passes moins de 183 jours par an, tu ne détiens rien là-bas, tu n'as aucun point de contact avec le gouvernement local. Tu es libre comme l'air. Thaïlande, Bali,



Pour aller plus loin, rejoins Le ₿unker sur YouTube

Portugal, Espagne. Des endroits où la sécurité est correcte, le coût de la vie est bas ou modéré, la qualité de vie est élevée, et personne ne te demande rien.

Maintenant, des exemples concrets.

**Le freelance nomade.** Nationalité : France, passeport européen. Résidence fiscale : Panama, zéro pour cent sur les revenus étrangers. Business : auto-entrepreneur français tant qu'il est sous le plafond de 77 000 euros, ou LLC aux États-Unis s'il dépasse. Actifs : Bitcoin plus un compte Wise pour recevoir les paiements en dollars ou en euros. Lifestyle : nomade digital. Il passe trois mois à Bali, trois mois en Thaïlande, trois mois en Amérique du Sud, trois mois en Europe de l'Est. Il ne reste jamais plus de 183 jours dans un seul pays, sauf au Panama où il est résident fiscal.

**L'entrepreneur qui scale.** Nationalité : France plus Uruguay en cours d'obtention après trois ans de résidence. Résidence fiscale : Uruguay, dix ans d'exonération via Tax Holiday 2.0 avec investissement requis. Business : LLC aux États-Unis pour accéder au marché américain et européen sans payer de taxe. Actifs : Bitcoin plus actions américaines via Interactive Brokers. Lifestyle : il passe six mois en Uruguay pour maintenir sa résidence, et six mois en Europe pour voir sa famille et ses amis.

**La famille expatriée.** Nationalité : France, plus un second passeport en cours d'obtention. Résidence fiscale : Portugal ou Espagne pour la qualité de vie et les écoles. Business : société locale ou travail en remote pour une entreprise européenne. Actifs : diversifiés, immobilier local, Bitcoin, actions. Lifestyle : stable dans le pays de résidence parce que les enfants sont scolarisés et qu'il faut un minimum de stabilité.

Est-ce que tout le monde peut appliquer cette théorie ? Non.

Si tu es entrepreneur digital, freelance en remote, investisseur ou rentier, célibataire ou en couple sans enfants, c'est facile. Tu as de la mobilité, tu peux vivre où tu veux, et tu peux structurer ta vie comme tu veux.

Si tu es salarié en présentiel, si tu as un business physique ancré dans un lieu, si tes enfants sont scolarisés, ou si tu as des parents âgés dépendants, c'est beaucoup plus compliqué. Ta mobilité est limitée.

Mais même si tu ne peux pas appliquer les cinq drapeaux à cent pour cent, connaître les principes te permet de les appliquer partiellement. Même deux ou trois drapeaux, c'est un gain énorme de liberté comparé à tout concentrer dans un seul pays.

Maintenant que tu as compris les principes des passeports, de la résidence fiscale et de la théorie des drapeaux, sois réaliste : ces sujets sont complexes et les erreurs coûtent cher.



Pour aller plus loin, rejoins Le ₿unker sur YouTube

Si tu envisages sérieusement de changer de résidence fiscale ou de structurer ta vie selon plusieurs juridictions, consulte un professionnel. Fiscaliste international ou conseiller en gestion de patrimoine. Ces deux professions sont devenues, ni plus ni moins, des spécialistes de l'expatriation. Ils accompagnent les Français qui veulent partir, déterminent leur résidence fiscale, structurent leurs actifs, et optimisent leur fiscalité.

# PARTIE VII : PASSER À L'ACTION

## Introduction

Tu as compris le jeu. Tu sais maintenant quelles sont tes surfaces d'attaque et comment les réduire. Reste une question : par où tu commences ?

On va découper ça en 4 blocs temporels :

1. **Aujourd'hui** - Ce que tu fais là, maintenant
2. **Cette semaine** - Les fondations solides
3. **Ce mois-ci** - Sécuriser ton argent et lancer ton side hustle
4. **La roadmap long terme** - 6 mois à 3 ans pour devenir un SDF capitaliste

Tu n'es pas obligé de tout faire. Mais au minimum, fais le bloc "Aujourd'hui". Ça changera déjà tout.



Pour aller plus loin, rejoins Le Ƀunker sur YouTube

## Aujourd'hui

1. Installe un gestionnaire de mots de passe → Partie III Chapitre 7
2. Check si tes emails ont fuité → Partie III Chapitre 6
3. Crée ton alter ego → Partie II Chapitre 1, Partie III Chapitre 5
4. Installe un VPN → Partie III Chapitre 8

## Cette semaine

1. Souscris à Paperboy → Partie II Chapitre 2
2. Nettoie tes traces en ligne → Partie III Chapitre 9
3. Configure un navigateur propre → Partie III Chapitre 8
4. Achète ton premier Bitcoin no-KYC → Partie IV Chapitre 11

## Ce mois-ci

1. Achète un hardware wallet → Partie IV Chapitre 12
2. Lance ton side hustle → Partie V Chapitre 15

## La roadmap long terme

À toi de la construire.

Tu as maintenant tous les éléments. Les passeports, la résidence fiscale, la flag theory, le business en ligne, Bitcoin. Comment tu assembles tout ça, dans quel ordre, avec quelles priorités, ça dépend de ta situation, de tes objectifs, de ton budget.

Certains vont d'abord chercher un deuxième passeport par filiation avant même de quitter leur CDI. D'autres vont scaler leur business en ligne jusqu'à 10k€/mois avant de penser à changer de résidence fiscale. D'autres vont mettre 80% en Bitcoin dès la première année et vivre comme des moines.

Il n'y a pas de chemin unique. Il y a juste des principes : réduire ta surface d'attaque, diversifier tes juridictions, ne pas mettre tous tes œufs dans le même panier, construire de la résilience.



Pour aller plus loin, rejoins Le Ƀunker sur YouTube

→ Partie V et VI

## Conclusion

**Aujourd'hui :** Gestionnaire mots de passe, check fuites, alter ego, VPN

**Cette semaine :** Paperboy, nettoyer traces, navigateur propre, premier Bitcoin no-KYC

**Ce mois-ci :** Hardware wallet, solutions dépenses Bitcoin, side hustle, compte Wise, DCA Bitcoin

**Roadmap long terme :** À toi de la construire

Chaque action compte. Chaque surface d'attaque réduite te rend plus libre.

Tu n'as pas besoin d'être parfait. Tu as juste besoin de ne pas être la pomme la plus basse du pommier.

Maintenant, arrête de procrastiner. Commence par le bloc "Aujourd'hui". Dans 6 mois, tu ne reconnaîtras plus ta vie.

Le système ne va pas se réformer. La seule personne qui peut te sauver, c'est toi.

Maintenant, tu sais quoi faire. À toi de jouer.

⚠ *Rappel: Les informations contenues dans ce guide ne constituent pas un conseil juridique ou fiscal. L'auteur décline toute responsabilité quant aux conséquences de l'application de ces informations. Respectez les lois en vigueur dans votre pays.*



Pour aller plus loin, rejoins Le ₿unker sur YouTube

# COMMENT NOUS SUIVRE

Tu as terminé ce guide. Si tu veux aller plus loin, reste connecté.

**Nos contenus**

- X (Twitter) : https://x.com/LeBunkerBtc
- YouTube : https://www.youtube.com/@leBunkerBTC
- Spotify : https://open.spotify.com/show/4eGWQrZFGnU4nJG8aa5Mx2?si=332f83fb0d0f4d71
- Instagram : https://www.instagram.com/lebunkerbtc/

**Nous soutenir**

Si ce guide t'a aidé et que tu veux soutenir notre travail, tu peux faire un don en Bitcoin Lightning :

Adresse Lightning : don@btcpay.lebunker.live

# SERVICES RECOMMANDÉS

Voici les services que nous recommandons et utilisons personnellement. Les liens ci-dessous sont des liens affiliés : si tu t'inscris via ces liens, tu bénéficies d'avantages (réductions, mois offerts) et tu nous soutiens sans surcoût.

## Domiciliation

**Paperboy**
Domiciliation personnelle et professionnelle en France.

→ https://getyourpaperboy.com/ref/BUNKER/

## VPN et téléphonie

**LNVPN**

→ https://lnvpn.net/vpn?ref=LeBunkerBTC

**Silent.link**

→ https://silent.link/lebunker

**SMSPool**

→ https://smspool.net/?r=LeBunker

## Bitcoin

**Bull Bitcoin**
La meilleure plateforme Bitcoin-only et non-custodiale.

→ https://app.bullbitcoin.com/registration/lebunker

**FREEDOMIA**
Carte Visa virtuelle rechargeable en Bitcoin.

→ https://freedomia.io/a/bunker