Bulletin d'information ECA-N : Mars 2026

La souveraineté individuelle : réduire sa surface d’attaque

Données personnelles transformées en marchandise, surveillance étatique en expansion, vague d’enlèvements visant les détenteurs de cryptoactifs en France : la souveraineté individuelle est devenue un enjeu existentiel. Ce guide pratique propose une méthode complète et progressive pour reprendre le contrôle de son identité, de sa vie privée, de son patrimoine et de sa juridiction en restant strictement dans le cadre légal.

Table des matières

Introduction

Nous vivons dans un contexte inédit où les données personnelles sont devenues une ressource économique de première valeur. Elles sont collectées massivement par les entreprises, revendues par des courtiers en données, et parfois exploitées par des acteurs malveillants. Parallèlement, les États élargissent leurs capacités de surveillance et de contrôle des flux financiers. Dans ce paysage, votre visibilité l'ensemble des informations accessibles sur vous, détermine directement votre vulnérabilité.

Ce guide ne s'adresse pas exclusivement aux personnes fortunées, ni à ceux qui auraient quelque chose à cacher. Il s'adresse à toute personne souhaitant **reprendre le contrôle sur ses données**, mieux comprendre les leviers de coercition auxquels elle est soumise, et agir pour les réduire de façon **légale et raisonnée**.

Les entreprises qui gèrent vos données, les banques qui enregistrent vos transactions, les plateformes qui conservent vos publications : chacune constitue un point de contact potentiel avec des tiers — qu'il s'agisse d'un gouvernement, d'un concurrent, d'un criminel ou d'un simple curieux. Réduire ces points de contact, c'est ce que nous appelons **réduire sa surface d'attaque**.

La France est devenue, en 2025-2026, le premier pays européen en matière d'enlèvements et de séquestrations liés aux crypto-actifs. Plus de **vingt affaires** ont été recensées depuis janvier 2025. En juin 2025, une agente du fisc a vendu, via Western Union, les données fiscales de détenteurs de crypto-monnaies. En janvier 2026, trois gendarmes ont été condamnés à de la prison ferme pour avoir revendu des informations issues de fichiers judiciaires 160 000 € perçus pour plus de 6 500 opérations frauduleuses. Même les institutions censées protéger les données constituent un vecteur de risque.

Les chiffres clés de ce guide

20+ enlèvements et séquestrations recensés en France depuis janvier 2025

2 Français sur 3 déjà concernés par une fuite de données personnelles

130+ bases de données françaises piratées sur le seul mois de janvier 2026

45 millions de données françaises exposées dans une seule fuite

646,52 € : Solde Bancaire Insaisissable en 2026

6 surfaces d'attaque à neutraliser pour devenir un « individu désintermédié »

1. Comprendre le jeu : la surface d’attaque

Pourquoi ce guide ?

La question n’est pas tant de se soustraire à ses obligations légales que de comprendre les mécanismes en jeu. Un particulier dont tous les actifs sont saisissables et l’adresse publique figure dans plusieurs registres dispose de beaucoup moins de marge de manœuvre qu’une personne ayant structuré sa vie de façon plus discrète sans pour autant enfreindre la loi.

La leçon est claire : partir du principe que toute base de données sera un jour piratée ou vendue est l’hypothèse de travail la plus prudente.

La notion de surface d’attaque

Définition

La surface d’attaque est un concept issu de la cybersécurité. Elle désigne l’ensemble des points d’entrée qu’un attaquant peut exploiter pour atteindre une cible. Plus cette surface est large, plus le risque est élevé.

Appliqué à la vie personnelle, ce concept dépasse le seul cadre numérique. Votre surface d’attaque comprend :

- Votre adresse de domicile visible dans des registres publics,
- Vos comptes bancaires saisissables,
- Votre numéro de téléphone lié à votre identité civile,
- Vos réseaux sociaux indexés par les moteurs de recherche,
- Votre patrimoine immobilier ou financier connu des administrations,
- Votre visage identifiable par des moteurs de reconnaissance faciale,
- Vos empreintes et votre ADN (données biométriques).

Chacun de ces éléments est relativement anodin pris isolément. C'est leur **combinaison et leur accessibilité simultanée** qui créent le risque.

Qui peut vous cibler et pourquoi ?

Les États et administrations

L'État dispose d'un accès légal à de nombreuses informations : revenus déclarés, comptes bancaires (via le fichier FICOBA), biens immobiliers, domicile fiscal. Ces données sont utilisées à des fins légitimes recouvrement fiscal, enquêtes judiciaires mais aussi, comme les cas récents le montrent, potentiellement détournées par des agents corrompus ou utilisées par des gouvernements aux dérives autoritaires.

« Si demain tu as des caméras de reconnaissance faciale sur la voie publique avec des titres d'identité biométriques et que toute la population est dans cette base de données, tu n'as plus de droit de résistance à l'oppression. »

Estelle de Marco — Docteure en droit privé et sciences criminelles

Les cybercriminels et fraudeurs

Ce groupe représente la menace la plus concrète pour le particulier. Les attaques incluent le phishing, l'usurpation d'identité, le SIM swapping, et des escroqueries sophistiquées exploitant les données disponibles sur les réseaux sociaux. Les données proviennent souvent de fuites de bases de données, croisées avec des informations publiques. La visibilité en ligne peut faire d'un individu une cible **physique**, pas uniquement numérique.

Les data brokers et l'économie de la surveillance

Les courtiers en données sont des entreprises dont le modèle consiste à collecter, agréger et revendre des profils sur des millions de personnes. Ils opèrent légalement en exploitant des données publiques et des partenariats commerciaux. Ces profils sont achetés par des employeurs, des assureurs, des recruteurs, des annonceurs, mais aussi par des particuliers souhaitant en savoir plus sur une personne spécifique. En Europe, le RGPD encadre leur activité, mais ne l'interdit pas.

Les deux archétypes qui échappent au système

Les invisibles

Certaines personnes sans adresse fixe déclarée, sans compte bancaire identifiable, sans bien saisissable sont, pour un créancier ou un huissier, pratiquement insaisissables. Non pas parce qu'elles sont sophistiquées, mais parce qu'elles n'ont aucune surface d'attaque exploitable par les voies classiques. D'ailleurs, en France, **la moitié des amendes pénales ne sont jamais recouvrées**. Pour les amendes supérieures à un million d'euros, le taux chute à 17 %.

Les ultra-riches

Les grandes fortunes utilisent des structures juridiques complexes, holdings, trusts, fondations pour diluer la propriété apparente de leurs actifs dans plusieurs juridictions. Trouver et saisir de tels actifs requiert des ressources juridiques et judiciaires considérables, ce qui rend l'opération économiquement peu rentable.

La leçon

Que ce soient les individus sans surface d'attaque ou les grandes fortunes, tous ont compris un même principe : **il ne faut pas être la pomme la plus basse du pommier**. L'objectif n'est pas l'invisibilité totale qui est impossible mais d'être suffisamment peu exposé pour ne pas valoir le coût de l'effort.

> **ℹ Note**
>
> Ce principe s'applique sans qu'il soit nécessaire de se placer hors de la loi. La grande majorité des mesures présentées dans ce guide sont légales et pratiquées couramment par des professionnels, des journalistes, des militants des droits civiques, ou simplement des personnes soucieuses de leur vie privée.

L’objectif : devenir un « individu désintermédié »

L’objectif est de s’inspirer de ces deux archétypes pour devenir plus résilient, sans tomber dans l’illégalité et sans nécessiter les ressources des hyper-riches. La formule retenue est celle de « l’individu désintermédié » : ne pas exister dans la matrice de manière trop visible, tout en disposant d’actifs et de revenus.

Quand un individu n’a aucun bien saisissable apparent, aucune adresse de vie dans les registres publics et des revenus partiellement hors circuit bancaire classique, la capacité de coercition des tiers, États, créanciers, acteurs malveillants s’effondre mécaniquement.

« L’arbre tordu vit sa vie, l’arbre droit finit en bois. »

Les 6 surfaces d’attaque

Pour atteindre cet objectif, ce guide traite six dimensions de la vulnérabilité :

Ce que vous protégez	Contre quoi
Qui vous êtes & où vous êtes	Identification et localisation physique
Ce que vous faites en ligne	Traçage numérique
Votre argent	Saisie et surveillance financière
Votre travail	Dépendance géographique
Votre juridiction	Exposition à un seul État
Vos actions	L’attentisme et l’inaction

Chaque surface non protégée est une porte d'entrée. Ce guide va vous apprendre à les fermer, une par une.

La chasse à l'homme

Avant de passer à l'action, un constat s'impose : il faut partir du principe que **toute base de données en ligne sera un jour piratée ou vendue** à des acteurs malveillants. Ce n'est pas de la paranoïa : c'est une réalité statistique démontrée chaque semaine.

Les acteurs malveillants opèrent de la manière suivante : ils se procurent des bases de données issues de piratages, les recoupent pour identifier des individus disposant de cryptoactifs ou d'un patrimoine significatif, puis passent à l'action. Il n'est pas nécessaire d'être parfait. Il est nécessaire de **ne pas être le maillon le plus accessible**.

Principe de proportionnalité et progressivité

Toutes les mesures de ce guide ne s'appliquent pas à tous les profils de la même manière. Un employé salarié sans actifs crypto n'a pas les mêmes priorités qu'un entrepreneur détenant d'importants actifs numériques.

Le guide est organisé de manière progressive. Chaque partie peut être lue indépendamment. Leur efficacité est néanmoins maximale lorsqu'elles sont abordées comme un système cohérent. **N'attendez pas de pouvoir tout faire pour commencer.**

> ★ **Priorité**
> Si vous ne deviez faire qu'une chose aujourd'hui : rendez-vous sur **haveibeenpwned.com** et entrez votre adresse e-mail principale. Si elle apparaît dans des fuites connues, changez immédiatement les mots de passe des services concernés. C'est gratuit, cela prend cinq minutes, et c'est le point de départ le plus utile.

Synthèse — Ce qu'il faut retenir

Principe	Ce que cela signifie en pratique
Surface d'attaque	Plus vous êtes visible et traçable, plus vous êtes vulnérable. Chaque information supprimée ou rendue inaccessible est un gain de sécurité.
Pertinence	Adaptez le niveau de protection à votre profil réel. Tout le monde n'a pas les mêmes besoins, ni les mêmes ressources.
Légalité	La quasi-totalité des mesures recommandées sont légales. Là où une zone grise existe, elle est explicitement signalée.

Principe	Ce que cela signifie en pratique
Progressivité	Commencez par les mesures les plus simples et les plus impactantes. N'attendez pas de pouvoir tout faire pour commencer.
Systémique	Une approche cohérente sur plusieurs dimensions vaut mieux que des mesures isolées dans un seul domaine.
Risque physique	La vie privée numérique a des implications physiques. Traiter les deux ensemble est indispensable.

Annexe — Glossaire des termes clés

Terme	Définition
Surface d'attaque	Ensemble des points d'accès qu'un tiers peut exploiter pour atteindre une cible.
Data broker	Entreprise qui collecte, agrège et revend des profils sur des individus.
RGPD	Règlement Général sur la Protection des Données. Législation européenne (2018).
Droit à l'effacement	Article 17 RGPD : droit de demander la suppression de ses données personnelles.
KYC	Know Your Customer. Procédures d'identification imposées aux établissements financiers.
SIM swapping	Fraude consistant à transférer un numéro de téléphone vers une SIM contrôlée par l'attaquant.
Phishing	Tentative d'usurpation par voie numérique pour obtenir des identifiants ou données bancaires.
FICOBA	Fichier national des comptes bancaires recensant tous les comptes ouverts en France.
SBI	Solde Bancaire Insaisissable : montant minimum laissé en cas de saisie (646,52 € en 2026).
Self-custody	Détention directe de crypto-monnaies via un portefeuille dont l'utilisateur contrôle les clés.

Terme	Définition
Multisig	Portefeuille protégé par plusieurs clés privées requises pour signer une transaction.
VPN	Virtual Private Network : service masquant l'adresse IP et chiffrant le trafic internet.
Domiciliation	Service permettant d'utiliser une adresse postale tierce comme adresse administrative.
Résidence fiscale	Pays dans lequel un individu est soumis à l'impôt sur ses revenus.
VoIP	Numéro de téléphone fonctionnant via internet plutôt que via le réseau classique.
Exit tax	Taxe française au transfert de résidence fiscale hors de France (patrimoines > 800 000 €).
RCS	Registre du Commerce et des Sociétés.
Reconnaissance faciale	Technologie d'identification biométrique permettant de retrouver des photos d'une personne.
Données biométriques	Propriétés physiques uniques à chaque individu (empreintes, ADN, visage, voix).

2. Qui vous êtes & où vous êtes

Votre identité et votre adresse constituent les fondations de votre surface d'attaque physique. Chaque fois que vous communiquez votre vrai nom, votre vraie date de naissance ou votre adresse réelle à un service commercial, vous créez un point d'ancrage. Ces données sont collectées par habitude, pas par nécessité et elles se retrouvent dans des bases revendues, piratées, ou accessibles pour quelques centimes. **En France, deux Français sur trois ont déjà été concernés par une fuite de données personnelles.**

Les deux règles fondamentales de cette partie :

- Votre vrai nom ne doit apparaître nulle part dans les bases de données commerciales.
- Il en va de même pour votre adresse personnelle.

Chapitre 1 — Créer un alter ego

La solution la plus efficace et la plus simple est de disposer d'une **identité d'emprunt** pour tous les usages quotidiens non officiels. La salle de sport, les commerces, les cartes de fidélité, les inscriptions en ligne : aucun de ces services n'a besoin de votre vraie identité.

ℹ Note

Utiliser un nom d'emprunt pour des inscriptions commerciales ne constitue pas une usurpation d'identité. L'usurpation consiste à se faire passer pour une personne qui existe réellement. Inventer un prénom et un nom fictifs n'est pas illégal dans ce contexte. Cette pratique ne doit pas être utilisée pour des engagements financiers ou des démarches officielles.

Comment construire son alter ego

Nom et prénom

Choisissez quelque chose de banal, simple à retenir. Évitez les noms trop exotiques ou trop mémorables. L'objectif est que cela sorte de manière spontanée à chaque fois qu'on vous demande de vous identifier. Apprenez-le par cœur jusqu'à ce qu'il devienne un réflexe.

Date de naissance

Prenez une date facile à retenir. Par exemple, ajoutez 1 jour et 1 mois à votre vraie date de naissance et changez l'année. L'important est que ça reste ancré dans votre mémoire sans être votre vraie date.

Adresse

Si vous avez besoin d'être recontacté par le service, utilisez votre **adresse de domiciliation** (voir chapitre 2). Sinon, donnez une adresse existante qui n'est pas la vôtre. Votre vraie adresse ne doit apparaître dans aucune base de données commerciale.

Adresse e-mail

Une adresse e-mail dédiée à votre alter ego pour le quotidien. Vous pouvez aussi créer des **alias** pour les inscriptions ponctuelles.

Numéro de téléphone

Si vous n'avez pas besoin d'être recontacté, donnez un faux numéro. Sinon, utilisez un numéro secondaire anonyme.

✓ Recommandation

À moins de traiter avec une administration officielle ou de souscrire un engagement financier où donner un nom d'emprunt pourrait entraîner des poursuites, vous utilisez votre alter ego.

Chapitre 2 — Domiciliation personnelle

Chaque fois que vous donnez votre adresse réelle, vous créez un point d'ancrage, un fil qu'on peut tirer pour vous retrouver. Pourtant, vous ne pouvez pas supprimer toute adresse : vous avez besoin d'une adresse pour votre courrier administratif, vos justificatifs de domicile, vos déclarations d'impôts.

La solution : **séparer votre adresse administrative de votre lieu de vie réel**.

Option A — Service de domiciliation postale

Pour quelques euros par mois, vous obtenez une adresse postale dans une autre ville, loin de votre lieu de vie réel. Votre courrier arrive, est scanné et envoyé en PDF par e-mail. Vous pouvez aussi demander la réexpédition physique.

Service	Prix/mois	Points forts	Remarques
Paperboy	à partir de 8,99 €	Scanning, réexpédition, multi-identités	Référence du secteur, pro disponible
SeDomicilier	à partir de 6 €	Réseau national, domiciliation juridique	Très bien pour les entreprises
Postes privées	variable	Présence physique dans de nombreuses villes	Moins orienté numérique
Chez un proche	gratuit	Simple	Expose l'adresse du proche
SAS / SASU perso	inclus	Sépare adresse pro et perso	Nécessite une structure existante

Option B — Domiciliation en mairie (gratuit)

Si vous n'avez pas de domicile stable, vous pouvez vous domicilier gratuitement via le **CCAS** (Centre Communal d'Action Sociale) de votre commune. Il suffit de remplir un des critères suivants : être hébergé chez quelqu'un, être nomade, être en transition résidentielle, ou avoir un lien avec la commune.

Processus : formulaire Cerfa 16029*01, dépôt au CCAS, entretien, domiciliation valable 1 an renouvelable.

Obtenir un justificatif de domicile officiel

Une fois votre adresse de domiciliation obtenue, connectez-vous sur **impots.gouv.fr** et changez votre adresse de correspondance. Elle apparaîtra sur votre prochain avis d'imposition, valable **12 mois** comme justificatif de domicile officiel — contrairement aux factures valables seulement 3 mois.

> ✓ **Recommandation**
>
> L'avis d'imposition est reconnu par la quasi-totalité des administrations et de nombreuses banques. C'est le document de référence à utiliser après un changement d'adresse de correspondance fiscale.

Chapitre 3 — Domiciliation entreprise

Si vous avez une entreprise, vous ne pouvez pas échapper au registre. L'adresse de votre activité sera visible publiquement sur Infogreffe et l'annuaire des entreprises. **L'erreur fatale** commise par de nombreux freelances est de déclarer leur adresse personnelle comme adresse d'entreprise. Leur adresse de domicile devient alors accessible à n'importe qui en 30 secondes.

- L'adresse de votre entreprise est toujours publique. Vous ne pouvez pas la masquer.
- Depuis août 2025, vous pouvez en revanche masquer votre adresse personnelle en tant que dirigeant sur le RCS.
- Si l'adresse de votre entreprise et votre lieu de vie sont identiques, votre adresse reste publique même après masquage.

La solution : externaliser l'adresse de votre entreprise

Service	Prix HT/mois	Points forts
Paperboy (pro)	à partir de 14,90 €	Scanning, réexpédition, juridique
SeDomicilier	à partir de 10 €	Réseau national, gestion en ligne
Kandbaz	à partir de 19 €	Adresses prestigieuses, gestion complète
Domiciliation.fr	variable	Large réseau de villes
Coworking local	variable	Double usage : bureau + domiciliation

Masquer votre adresse personnelle du RCS (Décret août 2025)

Depuis le 22 août 2025, vous pouvez demander à masquer votre adresse personnelle du RCS. Cette mesure a été prise pour donner suite à plusieurs enlèvements visant des dirigeants d'entreprise détenteurs de cryptoactifs.

- **Coût** : 53,38 € pour masquer tous les documents, ou 7,63 € par document. Gratuit si la demande est faite lors d'une formalité RCS.
- **Démarche** : en ligne sur formalites.entreprises.gouv.fr. Adresse masquée sous 5 jours ouvrés.

> ⚠ **Attention**
>
> Cette mesure masque votre adresse personnelle en tant que dirigeant, **pas l'adresse de votre entreprise**. Si ces deux adresses sont identiques, la protection est nulle. Externalisez l'adresse de l'entreprise en premier.

Option : non-diffusion SIREN (auto-entrepreneurs)

Si vous êtes auto-entrepreneur, au moment de votre déclaration, cochez la case « Je demande à ce que mes informations ne puissent pas être consultées ou utilisées par des tiers ». Vous pouvez également modifier ce choix ultérieurement en contactant l'INSEE. Résultat : votre nom, prénom et adresse exacte sont masqués sur les registres publics.

Le Registre des Bénéficiaires Effectifs (RBE)

Depuis le 31 juillet 2024, le RBE n'est plus accessible au grand public. Il reste consultable par les autorités, les professionnels soumis aux obligations anti-blanchiment, et certaines personnes justifiant d'un intérêt légitime. Vous n'êtes plus exposé publiquement comme avant.

Chapitre 4 — Colis et livraisons

Chaque colis commandé en ligne laisse une trace : nom complet, adresse exacte, numéro de téléphone, historique de commandes. Ces informations sont enregistrées par le vendeur et le transporteur, parfois pendant des années. **En France, au moins quatre affaires d'extorsion liées aux cryptoactifs ont commencé par une livraison à domicile surveillée.**

4.1 Recevoir des colis

Solution 1 — Mondial Relay Locker (recommandé)

Les Lockers Mondial Relay sont des casiers automatiques disponibles 24h/24, 7j/7, dans 10 pays européens. Aucune pièce d'identité, aucune interaction humaine, juste un code PIN. C'est la solution offrant le meilleur équilibre entre anonymat et praticité.

Si Mondial Relay n'est pas intégré : remplissez avec un faux nom, un faux numéro, et une adresse existante mais pas la vôtre. Choisissez un Locker proche de chez vous mais pas adjacent à votre domicile. Le code PIN est suffisant pour récupérer le colis — quelqu'un d'autre peut y aller à votre place.

Solution 2 — Amazon Locker

Principe identique aux Lockers Mondial Relay pour les commandes Amazon. Trois stratégies selon votre niveau d'exigence :

- **Option basique** : conserver votre compte Amazon habituel mais mettre une adresse Paperboy et un faux nom en livraison au Locker.
- **Option intermédiaire** : créer un compte alter ego long terme avec un e-mail dédié, un numéro anonyme, et une carte de paiement anonyme.
- **Option maximale** : comptes jetables par commande (moins stable — Amazon détecte les comptes multiples).

Solution 3 — Domiciliation postale (Paperboy et alternatives)

Pour les colis trop volumineux, les vendeurs n'acceptant pas Mondial Relay, ou les articles nécessitant votre vraie identité : faites-vous livrer à votre adresse de domiciliation. Le service réceptionne le colis, vous l'envoie en photo par e-mail, et vous pouvez demander une réexpédition physique.

Solution 4 — Mondial Relay Point Relais

Si le Locker n'est pas disponible, les Points Relais Mondial Relay (commerçants) permettent de retirer avec le code PIN sans pièce d'identité dans la majorité des cas. Risque : certains commerçants peuvent demander un document d'identification.

Solution 5 — Point Relais générique

En dernier recours (transporteur incompatible, zone non couverte). Votre adresse de vie reste protégée, mais une interaction humaine est inévitable.

4.2 Envoyer des colis

L'envoi pose plus de difficultés que la réception car vous n'avez pas le contrôle : il faut souvent passer par un guichet ou créer un compte en ligne.

Solution 1 — Mondial Relay Locker

Créez un compte en ligne avec un faux nom, e-mail dédié, numéro jetable et carte de paiement anonyme. Deux options pour déposer : imprimer l'étiquette et déposer directement au Locker, ou présenter le QR code dans un Point Relais.

Solution 2 — La Poste

Trois façons de procéder : au guichet en liquide (faux nom, adresse de retour fictive), étiquettes prépayées Colissimo achetées en cash chez un buraliste, ou via internet avec faux nom et carte anonyme.

> ⚠ **Règle absolue**
>
> Votre vrai nom et votre adresse de vie ne doivent **jamais** figurer sur un colis, que vous le receviez ou que vous l'envoyiez.

Chapitre 4 bis — Sécurité physique du domicile

La France est devenue l'épicentre européen des attaques physiques liées aux cryptoactifs. En 2025, **19 cas documentés** ont été recensés, dont l'enlèvement du cofondateur de Ledger à Vierzon en janvier 2025 (rançon de 10 M€, libération par le GIGN). Les tentatives sur les familles de dirigeants de Paymium et Binance France confirment un pattern : les agresseurs exploitent les fuites de bases de données pour localiser physiquement leurs cibles.

Alarmes télésurveillées

Pour un détenteur de cryptoactifs ou un patrimoine significatif, exiger la certification **APSAD P5** (norme française de référence pour la télésurveillance), la résistance au jamming radio et l'option d'intervention physique d'un agent. Références : Verisure (~49,90 €/mois), Homiris (~36,49 €/mois, APSAD P5), Sector Alarm (37,90 €/mois), Qiara (~20 €/mois sans engagement, APSAD P5).

Coffres-forts

Deux normes complémentaires encadrent les coffres domestiques : **EN 14450** (classes S1/S2 pour usage domestique courant) et **EN 1143-1** (classes 0 à VI pour usage professionnel et valeurs importantes). Pour une protection réelle, un minimum de classe III EN 1143-1 est recommandé. Associer une certification feu **EN 1047-1**. Fabricants : Hartmann Tresore, Fichet-Bauche, Burg-Wächter, Phoenix Neptune. Règle impérative : scellement dans une dalle béton ou un mur porteur.

Pièces fortes (safe rooms)

Pour les profils à patrimoine élevé. Entreprises spécialisées en France : Ultimium Protection (Paris/Genève), ICar'Safe, Fortalys (Île-de-France), Bunker Room (Dijon), Bunkerkit. Fourchette : **20 000 €** à **200 000 € et plus** (installation clé en main avec ventilation autonome, porte blindée, communications sécurisées et coffre intégré).

Caméras de surveillance à stockage local

Éviter les caméras imposant un stockage cloud (Ring/Amazon, Nest/Google). Privilégier les solutions locales : Ubiquiti UniFi Protect, Synology Surveillance Station, Reolink NVR, ou Frigate/Blue Iris (open source avancé).

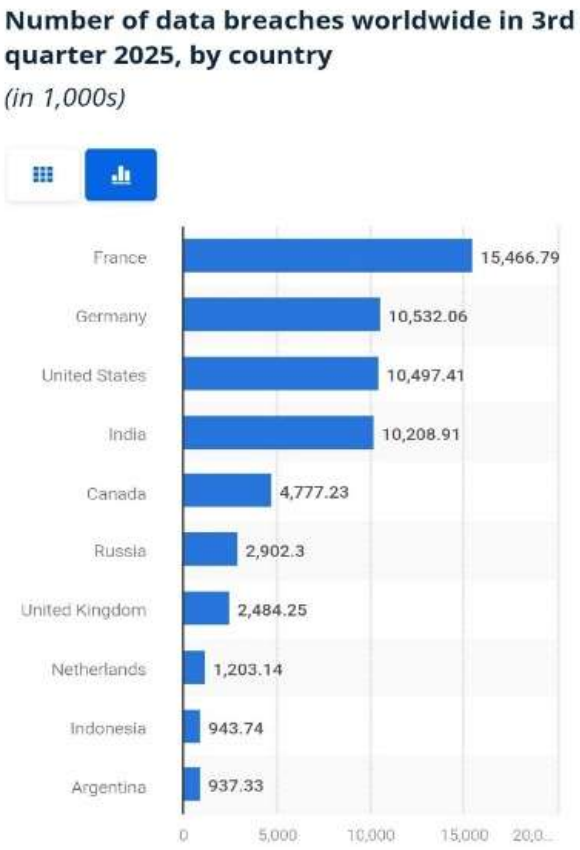
Assurances spécialisées

L'assurance multirisque habitation classique ne couvre pas les risques spécifiques liés aux cryptoactifs. Trois catégories à examiner : les **MRH haut de gamme** (Hiscox Clientèle Privée, AXA XL TailorMade) pour les patrimoines > 300 k€ ; les **Kidnapping and Ransom (K&R)** via Lloyd's (Hiscox, AIG, Chubb) pour les profils exposés (10 000 à 50 000 €/an) ; les **assurances crypto en self-custody** : AnchorWatch (Lloyd's, 0,55 à 2 %/an, exige un multisig), Coincover (159 à 749 $/an), Evertas.

> ✓ **Recommandation**
>
> Le couplage **multisig + assurance** est la stratégie la plus efficace : il réduit simultanément la surface d'attaque technique et le coût de la prime d'assurance.

3. Ce que vous faites en ligne

La surface d'attaque numérique est aujourd'hui la plus exposée et la moins défendue. Chaque inscription en ligne, chaque achat par carte, chaque recherche depuis un navigateur non sécurisé génère des traces persistantes, agrégées et revendues. **En France, en janvier 2026 seulement, plus de 130 bases de données nationales ont été piratées.** Le recoupement systématique de ces fuites permet à des acteurs malveillants de reconstituer des profils complets et d'en tirer des conséquences concrètes.



Liste des types d'attaques répertoriés

- **SIM Swapping** — un hacker convainc votre opérateur de transférer votre numéro sur sa carte SIM pour recevoir vos codes 2FA
- **Compromission du password manager** — votre coffre-fort de mots de passe est vulnérable si le mot de passe maître est réutilisé ailleurs
- **Chaîne de récupération email** — un vieux compte e-mail abandonné devient une porte d'entrée vers vos comptes principaux
- **Interception sur Wi-Fi public** — un attaquant capture vos cookies de session pour usurper votre identité
- **Shoulder surfing + vol de téléphone** — votre code PIN observé à la volée suffit à prendre le contrôle de votre appareil
- **OAuth / Sign in with Google** — une application tierce compromise devient un pont vers votre compte principal
- **Absence de verrouillage applicatif** — un téléphone déverrouillé donne accès direct aux applis bancaires ou crypto
- **Fuites de sauvegardes cloud** — des données chiffrées localement stockées en clair dans le cloud
- **Social engineering via questions de sécurité** — les réponses sont souvent trouvables sur les réseaux sociaux
- **Règle de transfert email cachée** — après un accès bref, un hacker installe une redirection silencieuse

- **Sessions actives sur appareils revendus** — un ancien appareil vendu sans déconnexion contient encore des tokens
- **Vol physique de SIM** — la carte SIM retirée et insérée ailleurs permet de recevoir les SMS de réinitialisation
- **Failles logicielles non patchées** — les mises à jour ignorées laissent des vulnérabilités exploitables
- **Phishing par lien frauduleux** — un SMS ou e-mail urgent redirige vers une fausse page pour voler les identifiants
- **Phishing avancé contournant la 2FA** — des attaques sophistiquées peuvent intercepter les codes en temps réel

Chapitre 5 — Téléphonie

Le numéro de téléphone personnel est l'identifiant le plus critique. Contrairement à une adresse e-mail que l'on peut remplacer en quelques minutes, un numéro de téléphone est lié à une pièce d'identité, communiqué à la banque, aux réseaux sociaux, aux services de livraison, aux authentifications à deux facteurs. Il suit un individu pendant des années et constitue un vecteur de traçage continu. L'opérateur enregistre chaque appel, chaque SMS et la position géographique via les antennes-relais.

En janvier 2026, une fuite de **45 millions de données françaises** incluait des millions de numéros de téléphone. En 2025, **18 000 signalements** d'usurpation de numéro ont été enregistrés auprès de l'Arcep. (L'Autorité de régulation des communications électroniques, des Postes et de la distribution de la presse)

Les quatre cas d'usage

Cas 1 — Vérification SMS ponctuelle

Coût : 0,50 à 2 € par SMS.

- SMSPool (smspool.net) : paiement en Bitcoin, large choix de pays.
- LNVPN Disposable (lnvpn.net) : paiement en Bitcoin Lightning. Activation quasi instantanée.
- ReceiveSMS.cc: alternatives grand public, paiement possible en crypto.
- OnlineSIM.io : autre alternative avec large couverture.

> ⚠ **Attention**
> Certaines plateformes détectent les numéros VoIP et les rejettent. En cas de refus, basculer sur une SIM prépayée.

Cas 2 — Numéro longue durée

- **LNVPN Rental UK** : numéro britannique (+44), abonnement mensuel, paiement Bitcoin Lightning.

- Silent.link US: numéro américain (+1), paiement Bitcoin Lightning. Inclut une eSIM data.

Cas 3 — Envoi de SMS et appels vocaux

Solution : SIM prépayée achetée en tabac-presse. Les opérateurs MVNO à bas coût (Lycamobile, Lebara, Syma Mobile) ont un KYC sommaire.

- Acheter la SIM en tabac (~5 €).
- Activer en ligne avec une adresse existante mais pas la vôtre.
- Recharger exclusivement en espèces.

Cas 4 — Data mobile anonyme

- **LNVPN eSIM** : eSIM data-only, paiement Bitcoin Lightning, multi-pays.
- **Silent.link eSIM** : même principe. Inclut un numéro US pour les SMS.
- Airalo : eSIM internationale, paiement par carte, moins anonyme mais très pratique.

Chapitre 5 bis — Systèmes d'exploitation et téléphones sécurisés

Le système d'exploitation de votre téléphone est la couche la plus fondamentale de votre sécurité numérique. Android stock (Google) et iOS (Apple) collectent en permanence des données de localisation, d'usage et de diagnostic.

GrapheneOS — la référence

GrapheneOS est un système d'exploitation Android entièrement dé-googlisé, conçu pour la sécurité et la vie privée. Compatible uniquement avec les téléphones Google Pixel (6 à 10). Prix d'un Pixel 9a en France : ~353 €. Profils utilisateurs séparés (un profil « quotidien », un profil « crypto » isolé). Sandbox Google Play optionnelle. Revendeurs clé en main : europe-connection.fr, Nitrokey NitroPhone, lab312.

Alternatives

CalyxOS : similaire à GrapheneOS, avec microG intégré par défaut. Plus grand public, légèrement moins durci.

Pour les ordinateurs : **Qubes OS** (virtualisation Xen, 16 Go RAM minimum, cloisonnement maximal) ou **Tails** (système amnésique sur clé USB pour les sessions jetables).

Chapitre 5 ter — Messageries chiffrées

Les messageries grand public (WhatsApp, Telegram en mode non-secret, iMessage) exposent des métadonnées exploitables : qui parle à qui, quand, combien de temps. Les alternatives chiffrées de bout en bout éliminent cette surface, mais toutes ne se valent pas.

Signal — le standard

Chiffrement de bout en bout par défaut pour tous les messages et appels. Protocole Signal (référence académique). Sealed Sender (l'expéditeur masqué même pour les serveurs Signal). Un numéro de téléphone reste nécessaire à l'inscription. Gratuit.

SimpleX Chat — aucun identifiant

Seule messagerie fonctionnant sans aucun identifiant (pas de numéro, pas d'email, pas de pseudonyme). Les connexions utilisent des files de messages anonymes. Routage à deux sauts par défaut depuis la version 6.0. Audit Trail of Bits (juillet 2024). Gratuit et open source.

Briar — résilience hors réseau

Communication pair-à-pair via Tor, Bluetooth ou WiFi Direct. Fonctionne même sans connexion internet. Conçue pour les journalistes et activistes en zone hostile. Android et Linux desktop uniquement.

Meshtastic, la messagerie post-apocalyptique fonctionnant sur radio LoRa, sans dépendance à internet.

✓ **Recommandation**

Pour les communications sensibles liées à la gestion de patrimoine crypto, privilégier **SimpleX** (aucun identifiant) ou **Signal** (avec un numéro anonyme obtenu via silent.link ou SIM prépayée). Éviter Telegram pour tout échange confidentiel : le chiffrement de bout en bout n'est pas activé par défaut.

Chapitre 6 — E-mails

L'utilisation d'une adresse e-mail unique sur l'ensemble des services en ligne est l'un des vecteurs de vulnérabilité les plus sous-estimés. Chaque inscription relie le même identifiant à un service différent. Lorsqu'une de ces bases est piratée, l'attaquant ne dispose pas seulement d'un mot de passe : il reconstitue un profil complet en recoupant les fuites.

Pourquoi la corrélation est le vrai danger

Votre e-mail Netflix + votre e-mail LinkedIn + votre e-mail salle de sport = votre nom complet, votre employeur, votre quartier, vos goûts. Un seul piratage suffit pour que tout fuite. Avoir un seul e-mail partout revient à relier tous vos profils à un seul identifiant traçable.

La solution : compartimenter

Niveau 1 — Identité réelle

Une adresse e-mail utilisée exclusivement pour les démarches officielles : banque, impôts, santé, famille, organismes d'État. Cette adresse ne doit jamais figurer sur un forum, un service commercial ou un réseau social.

Niveau 2 — Alter ego pour usages récurrents

Une adresse dédiée à l'alter ego, utilisée pour toutes les inscriptions commerciales régulières. L'usage du tag « + » permet de tracer quelle source a fuité (exemple : jean.martin+amazon@protonmail.com). Limite : le tag est visible et facilement supprimable.

Niveau 3 — Alias

Un alias est une adresse de transfert qui redirige les messages vers l'inbox principale sans la révéler. Chaque service reçoit un alias différent. En cas de fuite, l'alias est désactivé en un clic.

- **SimpleLogin** : open source, rachetée par Proton. Plan gratuit (10 alias) et payant.
- Addy.io (ex-AnonAddy) : alias illimités, open source, chiffrement GPG.
- **iCloud Hide My Email** : alias illimités intégrés à Safari et Mail. Requiert un abonnement iCloud+.
- Firefox Relay: plans gratuit et payant. Intégration native Firefox.
- DuckDuckGo Email Protection : gratuit, alias illimités en @duck.com.

> ⚠ **Attention**
>
> Ces services conservent la correspondance entre alias et adresse réelle. Une compromission de SimpleLogin ou Addy.io permettrait de relier tous les alias à l'adresse principale.

Niveau 4 — Adresses jetables

- Guerrilla Mail : adresse instantanée sans inscription, expire après 1h.
- 10 Minute Mail : expire après 10 minutes, prolongeable.
- Temp Mail : adresse aléatoire, durée variable.
- Mailnesia : alternative simple et rapide.

Où héberger ses e-mails

Gmail, Outlook et Yahoo scannent le contenu des e-mails à des fins publicitaires et transmettent les données aux autorités sur demande. Les alternatives chiffrées de bout en bout éliminent cette surface.

- ProtonMail (proton.me) : chiffrement de bout en bout, juridiction suisse, hors des accords Five/Nine/Fourteen Eyes. Utiliser un VPN en permanence lors de l'accès.
- **Tutanota /** Tuta (tuta.com) : chiffrement de bout en bout, juridiction allemande, open source. Moins cher que ProtonMail.
- Skiff Mail : alternative récente, open source, chiffrée.

> ✓ **Recommandation**
>
> Accédez systématiquement à votre service e-mail via un VPN. L'adresse IP est la seule donnée que ces services peuvent transmettre sous contrainte légale.

Vérifier si vos e-mails ont déjà fuité

Rendez-vous sur **Have I Been Pwned** (haveibeenpwned.com). Le service est gratuit, recense des milliers de bases de données piratées et propose des alertes automatiques. Toute adresse compromise impose la mise à jour immédiate des mots de passe et l'activation du 2FA.

Chapitre 7 — Mots de passe

La réutilisation de mots de passe est aussi une cause de piratage en cascade. Lorsqu'un service est piraté, les attaquants testent automatiquement les identifiants obtenus sur des dizaines d'autres plateformes (credential stuffing). Un seul mot de passe réutilisé peut provoquer la subtilisation simultanée de tous les comptes qui le partagent.

1. Gestionnaires de mots de passe

La solution n'est pas de mémoriser des mots de passe complexes, mais d'utiliser les outils adéquats. Un gestionnaire génère et stocke des mots de passe uniques et aléatoires de 20+ caractères pour chaque compte. Vous ne retenez qu'un mot de passe maître.

Gestionnaire	Stockage	Open source	Prix	Points forts
Bitwarden	Cloud chiffré E2E	Oui	Gratuit / ~10 €/an	Toutes plateformes
KeePass	Local uniquement	Oui	Gratuit	Zéro cloud, AES-256
KeePassXC	Local uniquement	Oui	Gratuit	Version moderne, multiplateforme
1Password	Cloud chiffré	Non	~3 €/mois	Interface soignée
Proton Pass	Cloud chiffré E2E	Oui	Gratuit / Proton+	Intégré à Proton

> ⚠ **Attention**
>
> La perte du mot de passe maître entraîne la **perte irréversible** de l'accès à l'ensemble des comptes. Le noter sur papier et le conserver dans un endroit physiquement sécurisé est impératif. Pour KeePass : sauvegarder régulièrement le fichier .kdbx sur une clé USB ou via *synchronisation P2P* (Syncthing).

2. Double authentification (2FA)

Un mot de passe solide et unique ne suffit pas : il peut fuiter via un piratage de la plateforme, un keylogger ou une attaque de phishing. La double authentification ajoute un second facteur inaccessible à l'attaquant.

TOTP — Standard recommandé

Le TOTP (Time-based One-Time Password) génère un code à 6 chiffres renouvelé toutes les 30 secondes, calculé localement. Contrairement au 2FA par SMS, il ne transite pas par le réseau téléphonique et ne peut pas être intercepté via un SIM-swap.

- 2FAS : open source, iOS et Android. Sauvegarde chiffrée des clés.
- Aegis : open source, Android uniquement. Exportation et sauvegarde des clés.
- Raivo OTP : iOS uniquement, open source.

> ✓ **Recommandation**
>
> Ne pas stocker les codes TOTP dans le même outil que les mots de passe. Si le gestionnaire est compromis, l'attaquant ne doit pas obtenir à la fois le mot de passe et le second facteur.

Clés matérielles — Protection maximale

Une clé matérielle est un dispositif physique USB ou NFC qui valide une connexion par contact physique. Sa particularité : elle vérifie le nom de domaine du site avant de signer. Un faux site de

phishing, même parfaitement reproduit, ne peut pas obtenir la signature. C'est la seule méthode de second facteur résistant au phishing.

- YubiKey Security Key NFC : référence du marché. Compatible USB-A et NFC. ~30 €.
- **YubiKey 5 Series** : version étendue, supporte TOTP et d'autres protocoles. ~55-75 €.
- OnlyKey : alternative open source avec stockage de mots de passe intégré.

> ⚠ **Attention**
> Utiliser le 2FA par SMS est la pire option : le SIM-swap est une attaque documentée et relativement accessible qui permet de détourner un numéro pour intercepter les codes.

Chapitre 8 — Navigation

Chaque session de navigation laisse des traces à plusieurs niveaux : l'adresse IP communique la localisation géographique ; le navigateur transmet une empreinte unique (OS, résolution, polices) ; le moteur de recherche conserve un historique des requêtes ; le fournisseur d'accès voit tous les domaines visités. **En France, les FAI sont légalement tenus de conserver cet historique un an.**

1. Navigateurs

- **Firefox** : open source, très configurable. Désactiver la télémétrie. Compléter uBlock Origin.
- Brave : basé sur Chromium mais dégooglé. Bloqueurs intégrés par défaut. Migration facile depuis Chrome.
- LibreWolf : copie de Firefox pré-configuré pour la vie privée.
- Tor Browser : Firefox modifié avec le réseau Tor intégré. Réservé aux opérations sensibles.

2. Moteurs de recherche

- DuckDuckGo : pas de profil utilisateur, pas de stockage des requêtes.
- Startpage : résultats Google mais anonymisés.
- **Brave Search** : index propre, indépendant de Google et Bing.
- SearXNG : méta-moteur open source auto-hébergeable.
- Qwant : moteur français sans tracking, dans l'UE.

3. VPN

Un VPN chiffre le trafic internet et le fait transiter par un serveur intermédiaire. Le FAI ne voit plus que la connexion au serveur VPN — plus les sites visités. Un VPN ne procure pas d'anonymat : il déplace la confiance du FAI vers le fournisseur VPN. Critères : politique no-logs auditée indépendamment, infrastructure RAM-only, paiement sans identification.

Fournisseur	Paiement	Logs	Juridiction	Prix/mois
LNVPN	Bitcoin Lightning	Aucun (RAM, 5 min)	International	~5 €
Mullvad	Cash / BTC / carte	Aucun (audité)	Suède	~5 €
IVPN	Cash / BTC / Monero	Aucun (audité)	Gibraltar	~6 €
ProtonVPN	Carte / crypto	Aucun (audité)	Suisse	~5-10 €
NYM	Cash / Crypto + ZK	Aucun par design	Suisse	~2,4-8 €

✓ **Recommandation**

Le VPN doit être activé en permanence, pas seulement lors d'opérations sensibles. Utiliser le VPN ponctuellement revient à révéler sa vraie IP tout le reste du temps.

4. Tor

Tor (The Onion Router) est un réseau décentralisé de milliers de relais bénévoles. Le trafic transite par trois relais successifs, chacun ne connaissant que le relai précédent et le suivant. Aucun relai ne détient les deux informations simultanément.

Cas d'usage : opérations exigeant un anonymat réel. Limites : lenteur, blocage par certains sites, JavaScript exploitable pour la désanonymisation (utiliser le mode Safest).

✓ **Recommandation**

La combinaison VPN + Tor masque au FAI l'utilisation de Tor, et masque au premier nœud Tor l'IP réelle. Utile dans les contextes à risque élevé.

Chapitre 8 bis — DNS sécurisés et réseau domestique

Le VPN protège le trafic en transit, mais il ne couvre qu'une partie du problème. Une couche de défense souvent négligée concerne la configuration de votre réseau domestique et de votre **DNS**.

Le DNS est l'annuaire d'Internet : chaque fois que vous tapez un nom de site, votre appareil envoie une requête DNS pour traduire ce nom en adresse IP. Le problème : par défaut, ces requêtes transitent en clair. Votre FAI voit chaque site que vous consultez. C'est comme envoyer une carte postale : le contenu est peut-être illisible, mais tout le monde peut lire l'adresse du destinataire.

La solution : remplacer le DNS de votre FAI par un DNS chiffré qui ne journalise pas vos requêtes.

Quel DNS chiffré choisir ?

Quatre critères : absence de journalisation, chiffrement du transport (DNS-over-HTTPS ou DNS-over-TLS), juridiction (hors 5/9/14 Eyes), fiabilité du service.

- **Quad9** (9.9.9.9) : juridiction suisse, aucune journalisation, bloque les domaines malveillants connus.
- **Mullvad DNS** (100.64.0.4 via DoH) : aucun log, bloqueur publicités intégrées en option.
- **NextDNS** (1,99 €/mois) : interface très complète avec filtres personnalisables. Hébergement disponible en France.
- **DNS0.eu / DNS4EU** : hébergé dans l'UE, sans but lucratif, alternative souveraine européenne.

Pour un contrôle total : installer un serveur DNS local (AdGuard Home ou Pi-hole sur Raspberry Pi, NAS Synology, ou vieux PC) qui filtre toutes les requêtes DNS de votre foyer.

Segmentation du réseau domestique

Un réseau domestique non segmenté, c'est un appartement sans portes : si un appareil est compromis, tous les autres sont accessibles. Une caméra connectée piratée peut servir de passerelle vers votre ordinateur.

La **segmentation VLAN** consiste à créer des réseaux virtuels isolés au sein de votre box ou routeur. Segmentation minimale recommandée pour un détenteur de cryptoactifs : un réseau de confiance (ordinateurs et téléphones), un réseau IoT isolé (caméras, domotique — accès internet uniquement), un réseau invité, et un réseau « crypto » dédié (accès sortant restreint au nœud Bitcoin ou à Tor).

Trois options : **Turris Omnia NG** (~400 €, open source), **UniFi Dream Machine Pro** (450 à 650 €), ou **OPNsense/pfSense** sur matériel dédié.

Trois réglages à appliquer immédiatement sur votre routeur actuel : désactiver WPS (vulnérable), désactiver UPnP (ouvre des ports automatiquement), et activer WPA3.

Chapitre 9 — Nettoyer ses traces

Les données passées constituent une surface d'attaque souvent négligée. Des profils sur des forums abandonnés, des photos géolocalisées sur d'anciens réseaux sociaux, des inscriptions avec adresse réelle : tout cela circule dans des bases de données revendues, piratées et agrégées.

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

Depuis 2018 l'article 17 du RGPD vous confère un droit à l'effacement. N'importe quel site qui stocke vos données personnelles est légalement obligé de les supprimer si vous le demandez. Délai : 30 jours maximum. En cas de refus, vous pouvez déposer une réclamation auprès de la CNIL, qui dispose de pouvoirs d'injonction et d'amendes jusqu'à **4 % du chiffre d'affaires mondial**.

Procédure : identifier les sites concernés (vieux forums, anciens e-commerces, réseaux sociaux abandonnés, anciens employeurs), utiliser les modèles de courrier disponibles sur cnil.fr, envoyer par e-mail à l'adresse de contact ou au DPO. En l'absence de réponse, saisir la CNIL en ligne.

Google et le droit à l'oubli

Google propose un formulaire en ligne pour supprimer des résultats de recherche vous concernant. La suppression est limitée aux domaines européens — les résultats restent visibles sur google.com. Critères : information ancienne, sans intérêt public légitime, concernant une personne privée.

PimEyes : quand votre visage devient traçable

PimEyes est un moteur de recherche par reconnaissance faciale qui indexe des millions de photos publiques. Il permet à quiconque de retrouver toutes vos photos à partir d'une seule image. PimEyes propose un formulaire d'opt-out gratuit : votre visage est retiré de leur index. La protection la plus efficace reste préventive : ne pas publier de photos de votre visage.

Les data brokers

Deux approches : **services automatisés** (Incogni ~100 €/an, DeleteMe) qui envoient des demandes d'effacement RGPD en masse — mais vous remplacez une exposition diffuse par une exposition concentrée sur un tiers ; **approche manuelle gratuite** : recherchez votre nom sur Google, identifiez les sites qui affichent vos données, envoyez des demandes RGPD individuelles. Chronophage mais gratuit et efficace.

Réseaux sociaux : le grand ménage

1 — Supprimer les anciens contenus

Sur X (Twitter) : TweetDelete ou Redact. Sur Facebook / Instagram : Social Book Post Manager. Vérifiez que ces outils sont open source ou audités.

2 — Verrouiller les paramètres de confidentialité

Profil privé sur Instagram, restreindre la visibilité aux amis sur Facebook, protéger les posts sur X. Désactiver l'indexation par les moteurs de recherche dans les paramètres.

3 — Supprimer les comptes inutilisés

- Facebook : Paramètres → Informations → Suppression définitive. Délai : 30 jours.
- Instagram : Via navigateur web. Délai : 30 jours.
- X / Twitter : Désactiver le compte. Délai : 30 jours.
- LinkedIn : Fermer le compte. Délai : 14 jours.
- TikTok : Gérer le compte → Supprimer. Délai : 30 jours.

> ⚠ **Attention**
>
> Distinguer la **désactivation** (données conservées, compte réactivable) de la **suppression** (irréversible après le délai de grâce). Même après suppression, des archives tierces (Internet Archive, bases de scraping) peuvent conserver des copies.

Nostr — Notes and Other Stuff Transmitted by Relays

Une alternative intéressante émerge avec **Nostr**, une nouvelle infrastructure qui permet de reprendre le contrôle total sur le contenu que l'on publie. Nostr est un réseau social libre, décentralisé et résilient, basé sur un protocole ouvert créé en 2022 par fiatjaf. Votre identité repose sur une paire de clés cryptographiques, à la manière de Bitcoin : pas besoin d'adresse e-mail ni de mot de passe. **Personne ne peut supprimer votre compte ni vous censurer durablement.**

Les publications sont diffusées via des relais que vous choisissez librement (Démarrer son relai Nostr sur Nym). Vous pouvez changer de client (Amethyst, Damus, Primal) à tout moment, sans perdre vos données ni vos abonnés. Nostr permet aussi de recevoir des paiements en Bitcoin via Lightning (« zaps ») directement sur vos contenus. Nous avons rédigé des newsletters dédiées à NOSTR.

Chapitre 9 bis — OSINT défensif : auditer sa propre exposition

Avant de payer un service pour supprimer vos données ou de passer des heures à envoyer des e-mails RGPD, posez-vous une question simple : qu'est-ce qu'un inconnu peut trouver sur vous en 30 minutes avec un moteur de recherche ?

L'**OSINT défensif**, c'est utiliser les mêmes méthodes que ceux qui voudraient vous cibler, mais pour votre propre compte. L'objectif n'est pas de devenir expert en cybersécurité, mais de savoir ce qui est exposé avant de décider quoi protéger en priorité.

Étape 1 : Cherchez-vous sur Google (10 minutes)

Tapez votre prénom et nom entre guillemets dans Google. Ajoutez votre ville, votre entreprise, votre ancien lycée. Essayez aussi votre numéro de téléphone, votre adresse e-mail. Tout ce qui apparaît est accessible à n'importe qui.

Étape 2 : Vérifiez si vos données ont déjà fuité (5 minutes)

Rendez-vous sur **haveibeenpwned.com** et entrez chacune de vos adresses e-mail. Si elles figurent dans des fuites, changez immédiatement les mots de passe et activez la 2FA.

Étape 3 : Cherchez votre visage (5 minutes)

Allez sur **PimEyes** et téléchargez une photo de vous. Le moteur vous montre toutes les autres photos de votre visage qu'il trouve en ligne. Si vous trouvez des résultats, faites l'opt-out gratuit. Vous pouvez aussi effectuer une recherche d'image inversée sur Yandex (le moteur le plus efficace pour retrouver des photos).

Étape 4 : Vérifiez vos pseudonymes (10 minutes)

Si vous utilisez le même pseudo sur plusieurs plateformes, un attaquant peut recouper vos comptes. Des outils gratuits comme Sherlock ou WhatsMyName vérifient automatiquement si un pseudonyme est enregistré sur des centaines de sites.

Bonus : protéger ses photos avant publication

Fawkes est un logiciel gratuit (Université de Chicago) qui modifie imperceptiblement vos photos avant publication. Les modifications sont invisibles à l'œil humain mais empêchent les moteurs de reconnaissance faciale de vous identifier. Efficacité documentée supérieure à 95 %.

En résumé : le bon ordre

D'abord s'auditer soi-même (les quatre étapes ci-dessus, 30 minutes). Ensuite seulement, décider où agir : effacement RGPD, opt-out PimEyes, changement de pseudonymes, nettoyage de comptes. Répéter l'exercice tous les six mois.

4. Votre argent

La surface d'attaque financière est celle qui détermine, en dernière instance, le niveau de coercition qu'un tiers peut exercer. Tant que l'épargne et les revenus transitent exclusivement par le système bancaire traditionnel, ils sont **saisissables, gelables et traçables sans délai**. Bitcoin constitue la réponse structurelle à cette vulnérabilité : détenu en self-custody, aucun tiers ne peut le saisir ou en restreindre l'usage.

Chapitre 10 — Pourquoi Bitcoin

Votre salaire doit passer par un compte bancaire

L'État oblige les employeurs à payer les salaires supérieurs à 1 500 € nets par virement bancaire. Objectif : faire transiter l'argent par un compte identifiable. Quand l'État a besoin de se servir, il sait où aller.

Comment fonctionne la saisie

Un créancier obtient un titre exécutoire. L'huissier ou l'État envoie un ordre à votre banque. La banque bloque votre compte. Elle maintient le **Solde Bancaire Insaisissable (SBI, 646,52 € en 2026)** et vire le reste au créancier. Vous n'êtes informé qu'après l'opération.

Multiplier les comptes ne sert à rien

Le fichier **FICOBA** recense tous les comptes bancaires ouverts à votre nom en France. L'ensemble est saisi simultanément. Le SBI de 646,52 € est calculé sur la globalité des avoirs, pas par compte.

> ✓ **Recommandation**
>
> Règle opérationnelle : ne jamais conserver plus de **646,52 €** sur l'ensemble des comptes bancaires. Tout excédent est transféré en Bitcoin, en self-custody.

Vous ne possédez rien

Votre appartement ? Vous êtes propriétaire tant que votre titre figure au cadastre. L'État peut réquisitionner votre bien. Vos actions ? Des lignes dans un fichier chez Euroclear. Votre assurance-vie, votre PEL, votre Livret A ? Vous prêtez votre argent à une institution, qui vous promet de vous le rendre. Une promesse.

Les précédents historiques

Chypre, 2013 : les dépôts supérieurs à 100 000 € ont été confisqués à hauteur de 47,5 % à la Bank of Cyprus pour recapitaliser le système bancaire. **Grèce, 2015** : fermeture des banques, retrait limité à 60 € par jour pendant des semaines. **France** : nationalisations de 1945 et 1982 touchant des dizaines d'entreprises et de banques. L'histoire montre une constante : quand l'État a besoin d'argent, il se sert.

Bitcoin change les règles

Si vous détenez vos clés vous-même (**self-custody**), vous avez la capacité technique de recevoir et d'envoyer des bitcoins sans demander la permission à quiconque. Personne ne peut geler vos avoirs. Personne ne peut confisquer vos bitcoins sans vos clés privées. C'est la première fois dans l'histoire moderne qu'un actif financier échappe structurellement au contrôle étatique.

Chapitre 11 — Acheter du Bitcoin

L'objectif est d'acquérir du Bitcoin en minimisant le lien entre l'identité civile et les coins obtenus.

Méthode 1 — Pair-à-pair avec paiement en espèces

C'est la méthode la plus propre : aucun intermédiaire, aucune plateforme, aucune trace bancaire. Un acheteur et un vendeur se rencontrent physiquement, échangent des espèces contre des satoshis. Les meetups Bitcoin locaux (btcmap.org, groupes Telegram régionaux) sont le canal le plus accessible.

Méthode 2 — Percevoir des revenus directement en Bitcoin

Pour les freelances et consultants, proposer d'être rémunéré en Bitcoin est une source de coins 100 % sans KYC. Plateformes : bitcoinerjobs.com, workinbitcoin.com.

Méthode 3 — Plateformes P2P sans KYC

Ces plateformes mettent en relation acheteurs et vendeurs sans exiger de vérification d'identité. Les fonds sont bloqués dans un escrow pendant la transaction. Prime de 5 à 10 % par rapport au cours des plateformes KYC.

- RoboSats : accessible via Tor, transactions sur Lightning. Idéal pour les petits montants. Anonymat maximal.
- Peach Bitcoin : application mobile, virement SEPA ou Revolut. Interface accessible.
- Bisq : logiciel desktop 100 % décentralisé. Plus lent, plus complexe, mais le plus résilient.
- @lnp2pBot (Telegram) : bot pour échanges Lightning rapides. Adapté aux petits montants.
- HodlHodl : plateforme P2P multi-monnaies avec escrow multi-sig. Pas de KYC obligatoire.

Méthode 4 — Plateformes d'achat avec retrait immédiat

Quand le P2P n'est pas praticable, acheter sur une plateforme et retirer via le **Lightning Network** ou le **réseau Liquid**. Ces couches secondaires masquent les montants et les adresses, coupant le lien traçable entre l'achat et la destination finale.

- Bull Bitcoin : Bitcoin-only, non-custodial. Retrait en 45 secondes via Lightning ou Liquid. Permet aussi des virements SEPA depuis un portefeuille Bitcoin.
- Relai : application suisse, Bitcoin-only, DCA automatisable. Retrait immédiat dans le portefeuille.
- Swan Bitcoin : orienté épargne programmée (DCA).

> ✓ **Recommandation**
>
> Retirer via **Lightning ou Liquid** depuis une plateforme KYC brise la traçabilité on-chain. La plateforme sait que vous avez acheté, mais ne peut pas suivre le parcours des coins après le retrait.

Chapitre 12 — Sécuriser ses bitcoins

Self-custody

Laisser des bitcoins sur une plateforme d'échange, c'est détenir une créance sur cette plateforme, **pas de la monnaie**. Une faillite, un piratage ou une décision réglementaire peut rendre cette créance inexigible. Le self-custody — détention des clés privées — est la seule forme de propriété réelle.

Hot wallet vs Cold wallet

Un **hot wallet** est une application connectée à internet. Pratique pour les transactions courantes, exposé aux menaces informatiques. Réservé aux montants du quotidien.

Un **cold wallet** est un appareil physique dédié (hardware wallet) qui stocke les clés privées hors réseau. La validation d'une transaction exige une interaction physique. Même un ordinateur compromis ne peut pas extraire les clés.

Modèle	Prix	Open source	Remarques
Ledger Nano X	~150 €	Partiel	Fuites de données 2020, 2026. Acheter anonymement.
Ledger Nano S Plus	~80 €	Partiel	Moins cher, même problème de données.
Trezor Model T	~180 €	Total	Firmware et hardware open source.
Trezor Safe 3	~80 €	Total	Puce sécurisée. Bon rapport qualité/prix.
Coldcard Mk4	~150 €	Total	Le plus avancé pour utilisateurs exigeants.
Foundation Passport	~200 €	Total	100 % open source. Pas de connexion USB.
Blockstream Jade	~55 €	Total	Excellent rapport qualité/prix.

> ⚠ **Attention**
>
> Ledger a connu plusieurs fuites massives de données clients (noms, adresses, numéros de téléphone) en 2020 et 2026. Ces bases circulent librement. Si vous utilisez un Ledger, **l'acheter anonymement** (en espèces ou livré sous faux nom en consigne automatique) est impératif.

Acheter un Hardware wallet

- Bitcoin Bazar, Boulanger (Paris) : boutique physique, paiement en espèces. Aucune trace.
- Commande en ligne payée en Bitcoin, livrée sous faux nom dans une consigne Mondial Relay.
- Achat auprès d'un particulier lors d'un meetup Bitcoin, contre espèces.

Sauvegarde de la seed phrase

La **seed phrase** (12 ou 24 mots) est la sauvegarde maîtresse permettant de récupérer l'accès sur n'importe quel appareil compatible. **Sa perte ou sa divulgation est irréversible.**

- Ne jamais photographier ni stocker numériquement la seed phrase.
- La noter sur papier (au minimum deux copies) dans des lieux physiquement distincts et sécurisés.
- Envisager une **passphrase** (25e mot) : même en cas de découverte physique de la seed, les fonds sont inaccessibles sans elle.

Chapitre 12 (suite) — Custody avancée : multisig et stockage métal

Un hardware wallet unique constitue un point de défaillance unique : en cas de vol, de perte, de destruction ou de contrainte physique, les fonds sont perdus ou compromis. **Pour tout patrimoine Bitcoin supérieur à 25 000 €, le standard en 2026 est le multisig** (multi-signatures).

Principe du multisig

Un portefeuille multisig exige plusieurs clés privées pour autoriser une transaction. Un schéma **2-of-3** signifie que sur trois clés existantes, deux sont nécessaires pour signer. Si une clé est volée, perdue ou détruite, les fonds restent inaccessibles à l'attaquant et récupérables par le détenteur. Pour les patrimoines supérieurs à 500 k€, privilégier un schéma **3-of-5**.

Services de multisig assisté

Nunchuk Honey Badger (480 $/an) : 2-of-4 avec clé d'héritage dormante, timelocks on-chain, et open source. **Casa** (250 à 2 100 $/an) : 2-of-3 à 3-of-5, plan d'héritage intégré, welcome kit avec hardware wallets. **Sparrow Wallet** : gratuit, open source, pour configuration DIY.

Règles d'or du multisig

Utiliser au minimum deux à trois fabricants différents de hardware wallets (protection contre les vulnérabilités de la chaîne d'approvisionnement). Distribuer les clés sur au moins deux juridictions géographiques distinctes. Ne jamais stocker deux clés au même endroit physique. Sauvegarder les **output descriptors** (BIP 380-384) avec chaque seed : sans eux, la récupération d'un portefeuille multisig est impossible.

Stockage métal de la seed phrase

Le papier est vulnérable à l'incendie, à l'eau et à la dégradation. Les supports métalliques en acier inoxydable 316 ou en titane résistent aux températures d'un incendie domestique. Après six séries de tests de destruction par Jameson Lopp, **les plaques individuelles gravées par poinçon** (Blockplate, Bitplates, CodlKeys) se révèlent les plus résistantes. Éviter les systèmes à tuiles insérables (Billfodl et similaires) : les tuiles se libèrent sous l'effet de la chaleur. **Ne jamais acheter un support dont le fabricant connaît la clé** (pré-gravée).

Chapitre 12 bis — Succession et héritage crypto

En France, la **loi du 12 mars 2024** confirme que les crypto-actifs sont des biens meubles incorporels soumis à la réserve héréditaire. La valorisation se fait au cours du jour du décès. Le barème standard des droits de succession s'applique (5 à 45 % en ligne directe, abattement de 100 000 € par enfant et par parent tous les 15 ans). Si les crypto-actifs sont découverts post-décès sans avoir été déclarés, une **majoration de 60 %** s'applique.

Risque majeur : la volatilité

Les droits de succession sont calculés sur la valeur au jour du décès. Si le cours chute entre le décès et la vente par les héritiers, ceux-ci peuvent devoir payer des droits supérieurs à la valeur réalisée. L'**anticipation successorale** (donation de son vivant, assurance-vie avec unités de compte crypto, protocoles d'héritage on-chain) est indispensable.

Solutions techniques d'héritage

Liana, **Casa Inheritance** et **Nunchuk Honey Badger** permettent de débloquer l'accès aux fonds après une période d'inactivité sans intervention d'un tiers. **Vault12 Guard** (365 $/an) utilise un système de récupération sociale Shamir.

Cabinets d'avocats fiscalistes spécialisés crypto en France : ORWL, Haas Avocats, Revo, JBLA.

> ✓ **Recommandation**
>
> Rédiger un protocole successoral avec un notaire ou un avocat spécialisé. Ce document doit préciser l'existence des actifs numériques, le mécanisme d'accès (multisig, timelocks), et la localisation des sauvegardes, **sans révéler les seeds elles-mêmes**.

Chapitre 13 — Dépenser ses bitcoins

La capacité à convertir ou dépenser des bitcoins sans faire transiter les fonds par le circuit bancaire est indispensable à l'utilité pratique de la stratégie.

Canal 1 — Vente contre espèces

Méthode la plus propre pour obtenir du cash. Rencontrer un acheteur dans un lieu public, envoyer les bitcoins, recevoir les billets. Adapté aux montants faibles à modérés. Via meetups Bitcoin (btcmap.org) ou réseau personnel.

> ⚠ **Attention**
>
> Pour les montants importants, cette méthode expose à un risque physique. Se limiter aux lieux très fréquentés et aux montants raisonnables.

Canal 2 — Cartes de paiement rechargées en Bitcoin

Des cartes Visa virtuelles permettent de convertir des bitcoins en euros pour dépenser partout où Visa est accepté.

- Freedomia : carte Visa virtuelle rechargeable en Bitcoin, compatible Google Pay.
- Bitsa : carte prépayée rechargeable en crypto, utilisable dans les commerces.
- Paybis Card : carte Visa émise après conversion crypto, utilisable à l'international.

> ⚠ **Attention**
>
> Ces services peuvent fermer sans préavis. Ne jamais y conserver de solde significatif. Recharger uniquement pour le montant de la dépense prévue.

Canal 3 — Cartes cadeaux

Acheter une carte cadeau en Bitcoin pour le montant exact de la dépense prévue. Aucun KYC, aucune trace bancaire, livraison instantanée par e-mail.

- Bitrefill : Amazon, Fnac, Carrefour, Leclerc, Decathlon, SNCF, Uber Eats, Netflix, Spotify, PlayStation, Steam, et des centaines d'autres.
- CoinsBee : alternative européenne avec bonne couverture de marchands français.
- The Bitcoin Company : orienté marché américain, nombreux services internationaux.

> ✓ **Recommandation**
>
> Pour les courses alimentaires, le carburant, les billets SNCF et les abonnements streaming, les cartes cadeaux couvrent la quasi-totalité des besoins courants sans aucune interaction avec le circuit bancaire.

Canal 4 — Virements bancaires

Pour les paiements contraints par virement SEPA (loyer, factures), il est possible d'envoyer des bitcoins ou stablecoins à un service intermédiaire qui émet le virement en euros. Les euros ne transitent jamais par votre compte bancaire personnel.

- Swapin : service européen réglementé (uniquement B2B) qui permet d'accepter/envoyer des cryptos et de régler en SEPA.
- Monerium : service réglementé émettant des euros tokenisés sur blockchain permettant des virements SEPA depuis un portefeuille crypto.

Canal 5 — Paiements Lightning directs

Le **Lightning Network** permet des transactions instantanées avec des frais inférieurs à 0,01 €. Contrairement aux transactions on-chain, les paiements Lightning ne sont pas enregistrés sur la blockchain publique. En France, le réseau de commerces acceptant Lightning reste limité mais croît (btcmap.org). Principal intérêt actuel : services en ligne (VPN, outils SaaS acceptant Bitcoin).

Chapitre 13 bis — eCash : confidentialité maximale

Les protocoles **eCash** (Fedimint, Cashu) représentent une avancée majeure pour la confidentialité des transactions Bitcoin. Ils utilisent des **signatures aveugles** (blind signatures) pour découpler l'identité de l'émetteur de celle du bénéficiaire, rendant les paiements structurellement intraçables.

Fedimint (custody fédérée)

Fedimint permet à un groupe de confiance (famille, communauté, meetup Bitcoin) de constituer une fédération gardienne de bitcoins. Les membres émettent et échangent des jetons eCash adossés aux bitcoins de la fédération, avec une confidentialité totale entre membres. Application : **Fedi** (fedi.xyz).

Cashu (mint centralisé)

Cashu fonctionne avec un « mint » unique (serveur de confiance) qui émet des jetons eCash contre du Bitcoin Lightning. Les transactions entre utilisateurs sont totalement anonymes même pour le mint. Applications : **Nutstash, Minibits, Cashu.me**. Idéal pour les micro-paiements et les pourboires Nostr.

> **⚠ Attention**
>
> Le mint constitue un point de défaillance unique. Ne confiez à un mint Cashu que les montants que vous acceptez de perdre. Ce n'est pas une solution d'épargne, mais un outil de paiement confidentiel pour le quotidien.

5. Votre travail

La nature de l'activité professionnelle conditionne directement le niveau de liberté. Celui qui exerce une activité physiquement ancrée — restaurant, commerce, emploi salarié en présentiel — place l'État en situation de monopole sur sa personne. Sans possibilité de mise en concurrence des juridictions, il devient la cible privilégiée de toute politique fiscale ou réglementaire contraignante.

La période pandémique l'a illustré clairement : les salariés contraints au présentiel n'ont eu d'autre choix que de se soumettre aux injonctions administratives. Ceux dont l'activité était exercée à distance ou en ligne disposaient d'une marge de manœuvre significative. **La mobilité professionnelle est une forme de résilience à part entière.**

Les États se comportent en agents rationnels. Ils exercent une pression maximale sur les captifs et font des concessions aux mobiles. En France, l'**article 155 B du CGI** (régime des impatriés) le démontre : les personnes venant de l'étranger avec un capital mobile bénéficient d'exonérations substantielles pendant huit ans. Le mobile est valorisé ; le captif est tondu.

En France, la police utilise des drones thermiques pour aller traquer les vaches que les éleveurs planquent pour éviter qu'elles soient vaccinées.

Chapitre 14 — Le piège de l'attentisme

L'obstacle le plus commun à la construction de cette mobilité n'est pas technique : c'est l'**attentisme**. Beaucoup d'individus conscients des dysfonctionnements du système reportent toute action personnelle dans l'attente d'une solution politique. Ils suivent l'actualité avec assiduité, analysent les programmes électoraux. Et leur vie n'avance pas.

Consommer du contenu politique est un substitut émotionnel à l'action. Il procure une illusion d'engagement sans produire aucun résultat tangible. La délégation de sa souveraineté à un acteur politique providentiel est une stratégie perdante par réalisme structurel : aucun gouvernement ne peut inverser en un mandat les déséquilibres accumulés sur plusieurs décennies.

Le temps consacré quotidiennement à la consommation passive d'information politique serait mieux investi dans l'**acquisition de compétences monétisables**. En un an, à raison de deux heures par jour, il est possible de maîtriser suffisamment une discipline pour facturer ses premiers clients. En deux ans, un revenu complémentaire substantiel est accessible. **En trois ans, une indépendance géographique complète devient réaliste.**

Chapitre 15 — Business en ligne

Les modèles qui marchent

Le freelance

La vente de compétences à des clients distants est le point d'entrée le plus accessible. Développement web, design graphique, rédaction, traduction, consulting, gestion de présence numérique. Les plateformes d'intermédiation (Upwork, Malt, Fiverr, Codeur.com) facilitent la mise en relation. Contrainte : le freelance échange ses heures contre des revenus, ce qui plafonne la croissance. Excellent point de départ.

Le commerce en ligne et le dropshipping

Vendre des produits physiques sans gérer de stock. Le commerçant se concentre sur le marketing et les ventes, un fournisseur gère la logistique. Outils : Shopify, WooCommerce, Amazon FBA. La rentabilité exige une discipline marketing rigoureuse, mais une fois le système opérationnel, il peut croître sans contrainte géographique.

La création de contenu

YouTube, podcast, newsletter, blog. Production de contenu sur un domaine de compétence, construction d'une audience, monétisation via publicité, parrainage, affiliation ou vente de produits numériques. Délai avant rentabilité plus long, mais revenus récurrents progressivement décorrélés du temps investi.

Les produits numériques et le SaaS

Logiciel par abonnement, formation en ligne, modèle de document, guide numérique. Coût de production initial uniquement : une fois créés, ces produits peuvent être vendus à l'infini sans coût marginal. **Le modèle le plus scalable.** Plateformes : Système.io, Podia, Skool, Gumroad, Teachable.

Recevoir des paiements

Deux canaux complémentaires à combiner.

En monnaie fiduciaire : Stripe pour les paiements par carte bancaire, Wise pour les virements internationaux sans frais excessifs, PayPal en dernier recours (blocages de comptes fréquents).

En Bitcoin : **BTCPay Server** offre une solution auto-hébergée, sans frais de plateforme et sans possibilité de gel par un tiers. Un client en Argentine, au Liban ou au Nigeria peut payer en Bitcoin sans friction, contrairement à un virement bancaire classique.

Contrairement à BitPay (1 % + KYC) ou OpenNode (1 %), BTCPay vous donne un **contrôle total** : les bitcoins arrivent directement dans votre portefeuille, sans intermédiaire. Options d'hébergement : Umbrel sur Raspberry Pi 5 (~150 €), Start9 (350 à 800 €), LunaNode (~15,80 $/mois, accepte Bitcoin), ou tout VPS Docker. Intégrations disponibles : Shopify, WooCommerce.

> ✓ **Recommandation**
>
> Pour les freelances facturant à la fois en Bitcoin et en monnaie fiduciaire, **Zaprite** (25 $/mois) offre une interface unifiée intégrant BTCPay Server avec Stripe et Square.

La structure juridique

Si vous débutez en France, le statut d'**auto-entrepreneur** est adapté aux phases de démarrage : plafonds de 77 000 € pour les prestations de services et 188 000 € pour la vente. Au-delà, ou pour optimiser la structure fiscale, la création d'une société étrangère mérite d'être envisagée.

- **LLC américaine** (Wyoming ou Delaware) : zéro imposition pour les non-résidents fiscaux américains, crédibilité internationale, administration simple.
- **Société offshore** (Panama, Uruguay, etc.) : fiscalité territoriale. Pertinente seulement en combinaison avec un changement de résidence fiscale.

> ⚠ **Attention**
>
> Une société étrangère ne suffit pas à exonérer d'impôt un résident fiscal français. **La résidence fiscale reste le critère déterminant.** Consulter un fiscaliste avant toute démarche.

Par où commencer

Choisir un modèle correspondant aux compétences actuelles ou à celles que vous voulez acquérir. Commencer par une compétence monétisable rapidement. Les plateformes (Upwork, Malt, Fiverr, LinkedIn) facilitent les premières mises en relation. Une fois les premiers clients générés, pivoter vers un modèle plus scalable si souhaité.

> ✓ **Recommandation**
>
> Ne démarrer qu'**un seul modèle à la fois**. La dispersion entre plusieurs projets simultanés est la principale cause d'échec. Maîtriser, générer les premiers revenus, puis diversifier.

6. Votre juridiction

Votre passeport détermine où vous pouvez voyager. Votre résidence détermine où vous vivez. Votre résidence fiscale détermine où vous payez vos impôts. **Ces trois éléments sont juridiquement indépendants et peuvent être dans trois pays différents.** La théorie des drapeaux est un cadre stratégique qui exploite cette indépendance pour maximiser la résilience et minimiser l'exposition à tout acteur institutionnel unique.

Chapitre 16 — Les passeports comme patrimoine

Un passeport n'est pas un simple document administratif. C'est un **actif transmissible** qui garantit la mobilité dans un environnement géopolitique incertain. La pandémie a rappelé que la liberté de circulation peut être suspendue en quelques heures. Ceux qui disposaient de nationalités multiples ont conservé des options inaccessibles aux autres.

Un second passeport constitue aussi une assurance contre les aléas propres à une nationalité : sanctions, zones de tension, traités bilatéraux défavorables. Il se transmet aux descendants et constitue un patrimoine immatériel de premier ordre.

Les quatre voies d'obtention

1 — Par filiation ou ascendance

Si vous avez des grands-parents italiens, polonais, irlandais, portugais ou espagnols, vous pouvez potentiellement demander la nationalité par droit du sang. Délai : 1 à 3 ans selon le pays. Une fois obtenu, l'actif est transmis à vos enfants automatiquement.

2 — Par résidence

Après plusieurs années de présence effective et d'intégration.

- **Uruguay et Paraguay** : 3 ans
- **Panama** : 5 ans
- **Portugal** : 5 ans
- **Espagne** : 10 ans

3 — Par investissement

Les Caraïbes (Saint-Kitts, Dominique, Antigua) proposent des programmes de citoyenneté par investissement entre **100 000 et 200 000 $**. Malte entre 600 000 et 1 000 000 €. Délai : 6 à 12 mois. Attention : certains de ces passeports peuvent nécessiter un visa pour entrer dans l'UE ou aux États-Unis, contrairement à votre passeport français.

4 — Par mariage

Après quelques années de vie commune avec un(e) ressortissant(e) du pays cible. Dépend des législations.

Pour un ressortissant français qui bénéficie déjà d'un accès libre à l'Union européenne, un second passeport apporte le plus de valeur s'il complète géographiquement : **Turquie, Brésil, Argentine** ou tout pays du Mercosur ouvrent des zones où la mobilité européenne est plus restreinte.

Mises à jour réglementaires 2025-2026 — points de vigilance

Italie — Le décret-loi n°36/2025 du 28 mars 2025, entré en vigueur immédiatement et confirmé par la loi n°74/2025 du 23 mai, restreint l'accès à la citoyenneté par descendance. Désormais, elle est limitée aux personnes ayant un parent ou un grand-parent né en Italie. La transmission sur plusieurs générations, auparavant possible, est supprimée. Cette réforme exclut environ **80 millions de descendants potentiels**.

Malte — Par son arrêt C-181/23 du 29 avril 2025, la Cour de justice de l'Union européenne a jugé illégal le programme de citoyenneté par investissement maltais (MEIN), estimant qu'il contrevient à l'article 20 du TFUE. Le dispositif est en cours de démantèlement. En revanche, le régime de résidence « non-dom » reste accessible.

Vanuatu — Le règlement (UE) 2025/11 du 3 février 2025 instaure une suspension permanente de l'accès sans visa à l'espace Schengen pour les citoyens du Vanuatu (inscription à l'annexe I). Ce passeport perd ainsi une grande partie de son intérêt pour les résidents européens.

Espagne — La loi 20/2022, dite « Ley de Nietos », a pris fin le 23 octobre 2025 après avoir enregistré **876 000 demandes**. Cette voie d'accès à la citoyenneté n'est désormais plus disponible.

Chapitre 17 — La résidence fiscale

La résidence fiscale détermine le pays où un individu est soumis à l'impôt sur ses revenus. En France, les critères sont **alternatifs** : il suffit d'un seul pour être considéré résident fiscal français.

- Foyer familial permanent en France
- Centre d'intérêts économiques en France
- Présence physique supérieure à 183 jours par an en France

Tant que la résidence fiscale est française, l'imposition porte sur le **revenu mondial**, quelle que soit la localisation des revenus.

Changer de résidence fiscale

Changer de résidence fiscale n'est pas une démarche symbolique. Trois étapes structurées :

1. Déclarer son départ aux impôts français. Remplir un formulaire, expliquer où vous partez, prouver que vous établissez votre résidence ailleurs.
2. Établir une présence effective dans le pays cible : bail de location ou achat immobilier, factures locales, inscription à la sécurité sociale locale si nécessaire.
3. Obtenir un certificat de résidence fiscale du nouveau pays. Ce document prouve au fisc français que vous êtes maintenant résident fiscal ailleurs.

Pièges à éviter

- Conserver un compte bancaire français avec des avoirs importants (signal d'intérêts économiques en France).
- Revenir plus de 183 jours par an en France.
- Laisser la famille en France (le fisc peut considérer le foyer permanent en France).

L'exit tax

Si vous avez plus de **800 000 €** d'actifs (crypto, actions, parts de société), une exit tax s'applique au départ. Le fisc calcule la plus-value latente au jour du départ et vous demande de payer l'impôt, même si vous n'avez pas vendu. Sursis de paiement pour les départs vers l'UE ou l'EEE. Paiement immédiat pour le Panama, l'Uruguay ou Dubaï.

Destinations à fiscalité favorable

Pays	Règle fiscale	Revenus étrangers	Résidence	Passeport	Remarques
Panama	Territoriale	Exonérés	Friendly Nations	5 ans	Coût de vie modéré
Paraguay	Territoriale	Exonérés	Très facile	3 ans	Coût de vie très bas
Uruguay	Territoriale + Tax Holiday 2.0	Exonérés 10 ans*	Facile	3 ans	Qualité de vie élevée
Dubaï (EAU)	0 % IR	Exonérés	Société/freelance	Non applicable	TVA 5 %, coût élevé
Portugal NHR	Supprimé 2024	Ne s'applique plus	/	/	À ne plus considérer
Île Maurice	Attractive	Partielle	Accessible	Naturalisation	Isolement géographique

ℹ Note

Uruguay Tax Holiday 2.0 (depuis janvier 2026) : exonération 10 ans sur revenus étrangers, sous condition d'investissement de 2 M$ en immobilier uruguayen ou 100 000 $/an dans un fonds d'innovation gouvernemental.

⚠ Attention

Avant tout changement de résidence fiscale, consulter un fiscaliste international. Les erreurs administratives peuvent entraîner des conséquences financières significatives.

Précision critique : crypto-actifs et exit tax

Les crypto-actifs détenus en direct (en self-custody ou sur une plateforme) sont **hors du champ de l'exit tax** (article 167 bis CGI), car ils ne sont pas assimilés aux valeurs mobilières de l'article 150-0 A. En revanche, si les crypto-actifs sont détenus via une **holding soumise à l'impôt sur les sociétés**, les parts de cette holding entrent en plein dans le champ de l'exit tax. **L'interposition d'une société peut donc paradoxalement augmenter la surface fiscale lors d'un départ.**

✓ **Recommandation**

Avant tout transfert de résidence fiscale, faire évaluer par un fiscaliste l'impact précis de l'exit tax selon la structure de détention (directe vs holding). Le projet de loi de finances 2026 n'a pas durci le régime, mais des propositions sont régulièrement débattues.

Chapitre 18 — La théorie des 5 drapeaux

La théorie des drapeaux, conceptualisée par Harry D. Schultz dans les années 1960-70 et étendue par W.G. Hill, propose de répartir les différents aspects de sa vie entre plusieurs juridictions pour maximiser la résilience et éviter d'être entièrement soumis à un seul acteur institutionnel.

Drapeau	Définition	Objectif	Exemples
1 — Nationalité	Passeports	2 ou 3 passeports complémentaires	France + Uruguay + Turquie
2 — Résidence fiscale	Où vous payez vos impôts	Fiscalité basse sur revenus étrangers	Panama, Paraguay, Dubaï
3 — Structure d'entreprise	Où est immatriculée votre société	Zéro taxe sur profits, crédibilité	LLC Wyoming / Delaware
4 — Actifs	Où sont vos biens	Propriété inviolable, stabilité	Bitcoin, Suisse, Singapour
5 — Lieu de vie	Où vous vivez (< 183 j/an)	Qualité de vie, sans résidence fiscale	Thaïlande, Bali, Portugal, Espagne

Profils types

Profil 1 : Le freelance nomade

Nationalité française conservée. Activité freelance en remote (3 000-5 000 €/mois). Résidence fiscale au Panama (revenus étrangers exonérés). Vie itinérante : moins de 183 jours dans chaque pays. Structure : auto-entrepreneur sous le plafond, LLC américaine au-delà.

Profil 2 : L'entrepreneur qui scale

Business en ligne à 10 000 €/mois. Résidence en Uruguay (Tax Holiday 2.0). LLC américaine pour facturer les clients internationaux. Démarches passeport uruguayen après 3 ans. Épargne en Bitcoin complétée par des actions américaines.

Profil 3 : La famille en transition

Priorité à la qualité de vie et à la continuité scolaire. Résidence au Portugal ou en Espagne. Travail en remote pour un employeur européen ou activité freelance. Actifs diversifiés. Application partielle de la théorie des drapeaux avec optimisation progressive.

Cette architecture n’est pas universellement applicable. Pour les salariés en présentiel ou les personnes ayant des contraintes familiales locales, son application est nécessairement partielle. Mais même **deux ou trois drapeaux** représentent un gain de liberté substantiel par rapport à une situation entièrement concentrée dans une seule juridiction.

7. Passer à l'action

La compréhension des mécanismes de vulnérabilité et des leviers de résilience ne produit d'effet que **traduite en actions concrètes**. Cette dernière partie propose une feuille de route structurée en quatre horizons temporels.

Vous n'êtes pas obligé de tout faire immédiatement. **L'efficacité de cette stratégie repose sur la progression, pas sur la perfection.** Chaque action accomplie réduit la surface d'attaque. Commencez par le bloc « Aujourd'hui » : il prend moins de deux heures et produit des effets immédiats.

Aujourd'hui — Actions immédiates

Ces quatre actions peuvent être réalisées en quelques heures.

4. Installer un **gestionnaire de mots de passe** (Bitwarden ou KeePass). Générer des mots de passe uniques et aléatoires pour tous les comptes existants. Cela seul neutralise la grande majorité des risques de compromission en cascade.
5. Vérifier si vos adresses e-mail ont été compromises sur **haveibeenpwned.com**. Changer immédiatement les mots de passe des comptes concernés. Activer les alertes automatiques pour les fuites futures.

6. Définir votre **alter ego opérationnel** : nom d'emprunt, date de naissance légèrement modifiée, adresse de domiciliation distincte, numéro secondaire, adresse e-mail dédiée. Cet alter ego sera utilisé pour toutes les interactions commerciales non officielles.
7. Installer et activer en permanence un **VPN** audité et sans journalisation (LNVPN, Mullvad ou IVPN). Le VPN doit devenir le mode de connexion par défaut, pas une option ponctuelle.

Cette semaine — Les fondations

Ces actions constituent les fondations de la stratégie. Quelques heures à quelques jours.

8. Souscrire à un **service de domiciliation postale** (Paperboy, SeDomicilier ou équivalent). Mettre à jour l'adresse de correspondance auprès des impôts. Utiliser l'avis d'imposition comme justificatif officiel. Pour les entrepreneurs : déclarer cette adresse comme siège social.
9. Engager le **nettoyage des traces numériques** : demandes d'effacement RGPD (Article 17) auprès des sites détenant des données, formulaire droit à l'oubli Google, opt-out PimEyes, suppression ou privatisation des comptes réseaux sociaux inutilisés.
10. Configurer un **navigateur respectueux de la vie privée** (Firefox + uBlock Origin, ou Brave) et adopter un moteur de recherche non traçant (DuckDuckGo, Startpage ou Brave Search).
11. Réaliser un **premier achat de Bitcoin sans KYC** : via meetup Bitcoin local avec paiement en espèces, ou via une plateforme P2P (RoboSats, Peach Bitcoin, Bisq).

Ce mois-ci — Sécuriser et construire

Consolider la stratégie financière et amorcer une activité mobile.

12. Acquérir un **hardware wallet** anonymement. Transférer tous les bitcoins hors des plateformes d'échange. Ne plus conserver que le SBI sur les comptes bancaires.
13. Mettre en place les **solutions de dépense en Bitcoin** : carte Visa virtuelle (Freedomia / Bitsa) pour l'e-commerce, cartes cadeaux Bitrefill pour les commerces du quotidien, Bull Bitcoin pour les virements SEPA.
14. Identifier la **compétence monétisable** la plus accessible et créer un profil sur une plateforme freelance. L'objectif n'est pas la perfection mais la mise en mouvement.
15. Ouvrir un **compte Wise** pour les paiements internationaux. Activer un **DCA mensuel** en Bitcoin pour construire progressivement une épargne hors système bancaire.

Annexe — OPSEC familial

OPSEC est l'abréviation de Operational Security (sécurité opérationnelle).

Les attaques physiques de 2025 en France ciblent en priorité les **proches** (conjoints, enfants, parents) des détenteurs de crypto-actifs. La protection personnelle est inutile si la famille constitue le maillon faible. L'OPSEC familial doit être traité comme une priorité équivalente à la sécurisation technique des fonds.

Règles fondamentales

Ne jamais évoquer les montants détenus en crypto-actifs, y compris devant la famille élargie, les amis, le personnel domestique. Convenir d'un **code de duresse familial** (un mot ou une phrase anodin(e) signifiant « j'agis sous contrainte »). Configurer l'architecture multisig de façon à ce qu'aucune personne au domicile ne dispose d'un nombre suffisant de clés pour autoriser une transaction. Vérifier régulièrement les publications des proches sur les réseaux sociaux (photos de lieu de vie, de véhicule, de voyages). Instruire ses proches via une formation à la sécurité numérique de base (mots de passe, 2FA, phishing).

Protocole en cas de menace directe

Si vous ou un proche êtes menacé(e) physiquement, **l'objectif est de ne pas être en mesure de satisfaire la demande de l'agresseur**. C'est précisément l'avantage du multisig avec clés distribuées géographiquement : même sous contrainte, il est techniquement impossible de débloquer les fonds avec les seuls éléments présents au domicile. Cette impossibilité technique est votre meilleure protection physique. Certains portefeuilles (Coldcard Mk4/Q) intègrent des **PIN de duresse** (duress PIN, trick PIN, brick PIN) qui affichent un portefeuille factice contenant un montant crédible mais faible.

> **✓ Recommandation**
>
> L'OPSEC familial est souvent négligée mais demeure critique. Aucune sécurité technique n'est suffisante si les proches ne sont pas préparés. Elle doit être intégrée dès le début de toute stratégie de sécurisation.

La roadmap long terme — 6 mois à 3 ans

Cette phase ne peut pas être prescrite uniformément. Elle dépend de la situation personnelle, des objectifs et des ressources. Quelques principes directeurs :

- Construire des **revenus en ligne** jusqu'à dépasser le salaire actuel.
- Initier les démarches pour un **second passeport** (par filiation si possible — voie la moins coûteuse).
- Envisager un **changement de résidence fiscale** une fois les revenus stabilisés et les actifs structurés.
- Diversifier les actifs : Bitcoin, actions internationales, immobilier hors de France.
- Consulter un **fiscaliste international** avant toute décision structurelle majeure.

Conclusion : la souveraineté retrouvée

L'ensemble de cette stratégie repose sur un principe unique : **réduire le nombre de points de prise** que les acteurs extérieurs institutionnels, criminels ou commerciaux peuvent exercer sur un individu. Chaque surface d'attaque neutralisée est une liberté recouvrée.

Cette démarche ne requiert pas la perfection. Elle requiert la **progression**. L'objectif n'est pas de devenir invisible, ce qui est impossible mais de **ne pas être le maillon le plus faible de la chaîne** : celui qui sera ciblé en premier parce qu'il est le plus facilement accessible.

Les personnes qui n'agiront pas attendront un changement systémique qui ne viendra pas dans les délais espérés. Ceux qui agissent, même partiellement, auront une vie structurellement plus résiliente, plus libre et moins dépendante d'une seule juridiction, d'un seul employeur ou d'un seul système financier.

Devenir un individu souverain signifie bien plus que se protéger soi-même contre d'éventuelles attaques et oppressions, c'est une nécessité si nous voulons tendre vers des **démocraties justes et équitables**. Ce mode de gouvernance est tributaire de la liberté d'agir et de s'exprimer, sans quoi le débat public libre où les idées se confrontent pour évoluer n'a pas de sens (peur de représailles, corruption, propagande). Malheureusement de nos jours, ce schéma est mis à mal par la manipulation des vecteurs de communication, d'information et d'éducation.

Pour mieux l'imager, voici une citation d'**Estelle de Marco** qui souligne que les gouvernements ne rencontrent aucune difficulté à nous imposer certaines choses :

« Si tout le monde avait cette culture de comprendre que la situation actuelle est anormale, qu'il faut râler et que râler peut fonctionner, beaucoup plus de personnes râleraient, et les gouvernements seraient moins enclins à aller aussi facilement. »

Finalement, nous vous invitons à **développer votre esprit critique** car, selon Jules Ferry (discours introduction sommet des libertés a Paris), c'est le facteur déterminant pour s'élever au-dessus des faux débats politiques actuels et proposer des alternatives.

Pour aller plus loin

Cette synthèse de ressources prolonge le présent guide. Elle réunit articles, vidéos, outils et publications de référence permettant d'approfondir les thèmes abordés.

Surveillance biométrique : l'Europe a basculé ? Estelle De Marco

La présidente de la Commission européenne, Ursula von der Leyen, affirme que la liberté d'expression est un VIRUS et que la censure est le vaccin...

Une semaine classique en France par Stachtchenko

Récapitulatif L'IDENTITÉ NUMÉRIQUE LA POSTE + FRANCE IDENTITÉ

Comment les libertariens voient les cycles d'élections.

Un policier parle de l'IGPN. (sur le même sujet…)

Référence à l'épisode de BlackMirror sur les puces neurales

Nouvelle note de recherche de l'Institut National de Bitcoin : Collecter plus, protéger moins ?

Dernière actualité NYM

"La boîte à crypto" : un kit pédagogique gratuit pour enseigner la cryptographie (par l'ARCSI)

Détention, propriété et souveraineté : les nuances de la possession de bitcoins.

"Bitcoin ne sera JAMAIS adopté, la self-custody est trop compliquée…"

"Financial surveillance has been steadily expanding for 55 years. The Digital Asset Market Clarity Act is only the latest expansion"

L'UNION EUROPÉENNE VEUT IMPOSER LE PROJET « CHAT CONTROL ».
DITES NON À : La surveillance de vos messages privés

L'application de vérification d'âge de l'UE piratée en 2 minutes ?

Si vous vous souciez de la confidentialité financière, alors ceci est probablement la recherche la plus importante que vous lirez cette année.

The industry is "too transparent," and it's actually a huge problem.

Why Bitcoin Is Freedom Money

Septembre éternel

Qu'est-ce qu'un IBAN virtuel et pourquoi Tracfin alerte sur la fraude ?

Anatomy of the state

The Way of Bitcoin: Becoming Self-Sovereign

How To Off Ramp Crypto Without Paying Taxes

La cryptographie asymétrique par la peinture

Pangolin , un projet open source qui colle tout ça dans un seul paquet : Proxy inversé, tunnels WireGuard chiffrés, authentification zero-trust, le tout orchestré par Docker. (GUIDE)

Sacrée boîte à outils !

Guard Your Mind': The Techno-Libertarian Manifesto

Si vous avez toujours voulu comprendre comment l'argent chiffré fonctionne réellement → c'est ça.

Plus sur NOSTR : NEWSLETTER septembre 2024

Pour ceux qui veulent découvrir Nostr et faire parti de la communauté #nostrfr vous pouvez commencer par un de ces applications

D'ici quelques mois, les réseaux sociaux exigeront un KYC pour les utiliser. Oubliez Lenster, Farcaster et autres alternatives trop dépendantes des blockchains sur lesquelles elles évoluent. Voici Nostr, l'alternative la plus sérieuse et fiable qui gagne du terrain.

Projet cool de troc digital