

Suis-je espionné ?

Micros, caméras cachées, balises GPS, logiciels espions : comprendre, détecter, prouver. Le guide de référence pour reprendre le contrôle de votre vie privée — sans commettre d'infraction.

Cadre juridique 2026

Téléphone & stalkerware

Micros & caméras

Balises GPS & AirTag

Méthode d'inspection

Constituer une preuve

Ce que ce guide est — et ce qu'il n'est pas

Vous avez acheté ce guide parce qu'un doute s'est installé. Peut-être qu'une information que vous pensiez confidentielle est remontée à quelqu'un qui n'aurait pas dû la connaître. Peut-être que votre téléphone chauffe sans raison, que votre conjoint semble toujours savoir où vous êtes, ou qu'un objet a changé de place dans votre bureau. Ce doute est légitime, et il mérite mieux qu'une nuit blanche : il mérite une méthode.

Ce guide vous donne cette méthode. Il a été rédigé par les équipes du Groupe Prometheus, cabinet d'investigations privées agréé par le CNAPS, à partir de la pratique de terrain de nos interventions de contre-mesures techniques (TSCM). Il condense ce que nous vérifions, dans quel ordre, et pourquoi.

CE GUIDE N'ENSEIGNE PAS À ESPIONNER

Vous ne trouverez ici aucune indication permettant de placer, dissimuler, configurer ou exploiter un dispositif de surveillance. Les descriptions techniques de matériels servent exclusivement à les **reconnaître** et à les **détecter**. Poser un micro, une caméra ou une balise sur une personne sans son consentement est un délit puni d'emprisonnement et d'amende (chapitre 2). Nous ne prêtons assistance à aucune démarche de ce type, et le simple fait d'être « la victime dans l'autre sens » ne crée aucun droit à la riposte.

À qui ce guide s'adresse

Il a été pensé pour trois profils, qui se recoupent souvent :

- **Le particulier** confronté à un doute personnel : séparation conflictuelle, harcèlement d'un ex-partenaire, voisinage intrusif, location de vacances suspecte, sentiment d'être suivi.
- **Le dirigeant, le cadre ou l'élu** dont les décisions ont une valeur économique ou politique : fuite d'information, négociation en cours, contentieux, litige d'associés.
- **Le professionnel du droit** — avocat, mandataire, commissaire de justice — qui doit apprécier la recevabilité et la solidité d'un élément de preuve.

Comment l'utiliser

Le guide suit l'ordre logique d'une intervention réelle. Nous vous recommandons de le lire une première fois intégralement, sans rien faire, puis de revenir aux chapitres opérationnels une fois que vous aurez compris deux choses essentielles : **ce que vous avez le droit de faire**, et **ce qui détruirait une preuve**. C'est la raison pour laquelle la partie juridique précède la partie technique. Dans notre expérience, la majorité des dossiers perdus le sont non pas faute de preuve, mais parce que la preuve a été détruite, contaminée ou obtenue de façon irrecevable dans les premières heures.

PORTÉE JURIDIQUE DU DOCUMENT

Ce guide constitue une information générale à jour de l'état du droit français à la date de son édition. Il ne constitue ni une consultation juridique, ni un avis d'avocat, et ne saurait se substituer à l'analyse d'un professionnel du droit sur votre situation particulière. Les textes cités (code pénal, code civil, code du travail, code de la sécurité intérieure) sont susceptibles d'évoluer ; vérifiez la version en vigueur ou faites-la vérifier avant toute démarche contentieuse.

UNE NOTE SUR LA PEUR

La surveillance illicite existe, elle est documentée, et elle est devenue techniquement accessible. Mais l'angoisse d'être surveillé produit aussi, à elle seule, des symptômes qui ressemblent à des indices : une batterie qui se vide, un bruit sur la ligne, une voiture garée deux fois de suite dans la même rue. Ce guide vous apprend précisément à faire la différence entre un signal et un bruit. Si le doute vous empêche de dormir, de travailler ou de vivre normalement, parlez-en — à un proche, à votre médecin, ou à nous. Un diagnostic, même négatif, vaut mieux qu'une incertitude qui dure.

Sommaire

PARTIE I — COMPRENDRE LA MENACE

01 Êtes-vous concerné ? Signaux, contextes et réalité du risque	6
---	---

PARTIE II — LE CADRE JURIDIQUE

02 Ce que la loi interdit : les six infractions à connaître	11
03 Ce que vous avez le droit de faire — et les pièges de la preuve	15
04 Le cas de l'entreprise : surveillance des salariés et locaux professionnels	18

PARTIE III — PANORAMA DES DISPOSITIFS

05 Ce qui existe réellement : la taxonomie des dispositifs	21
06 Comment ça fonctionne : alimentation, transmission, dormance	25

PARTIE IV — DÉTECTER

07 Votre téléphone : diagnostic complet iOS et Android	29
08 Vos locaux : la méthode d'inspection visuelle en 7 étapes	33
09 Votre véhicule : balises GPS et traceurs	36
10 AirTag et traceurs Bluetooth : le cas particulier	38
11 Les appareils de détection : ce qu'ils voient, ce qu'ils ne voient pas	40
12 Les cinq angles morts du « faites-le vous-même »	43

PARTIE V — AGIR

13 Vous avez trouvé quelque chose : les sept réflexes	46
14 Constituer un dossier opposable	48
15 Faire appel à un professionnel : ce qu'est une intervention TSCM	50

ANNEXES

A Checklist d'inspection — 62 points de contrôle	53
B Fiche d'urgence « je pense être suivi » — 30 minutes	56
C Tableau menace → méthode de détection	57
D Trame de plainte et articles à viser	58
E Glossaire	60
F Contacts et ressources utiles	61

PARTIE I

Comprendre la menace

Avant de chercher un dispositif, il faut savoir ce que l'on cherche, qui aurait un intérêt à le poser, et à quoi ressemble un vrai indice. C'est le travail de tri qui précède toute intervention technique.

01 — Êtes-vous concerné ? Signaux, contextes et réalité du risque

Êtes-vous concerné ?

La question n'est pas « est-ce que cela existe » — cela existe, c'est en vente libre et cela coûte moins qu'un dîner en ville. La question est de savoir si votre situation présente les trois conditions qui font passer un risque théorique à un risque réel : un mobile, un accès, et un bénéfice.

1.1 La démocratisation du matériel

Il y a quinze ans, poser un micro exigeait un matériel spécialisé, un budget de plusieurs milliers d'euros et un minimum de compétences techniques. Ce n'est plus le cas. La convergence de trois évolutions industrielles — la miniaturisation des capteurs issue de la téléphonie mobile, les batteries lithium-polymère à haute densité, et la couverture 4G/5G généralisée — a mis entre les mains de n'importe qui des dispositifs qui relevaient auparavant des services de renseignement.

Aujourd'hui, un micro GSM autonome opérationnel se trouve pour une vingtaine d'euros, une caméra à objectif sténopé de moins d'un millimètre intégrée dans un objet du quotidien pour une cinquantaine, une balise GPS magnétique avec plusieurs semaines d'autonomie pour une soixantaine. Ces prix ne sont pas des ordres de grandeur théoriques : ce sont ceux des places de marché grand public.

< 50 € Prix d'un micro espion opérationnel disponible en ligne	1 mm Diamètre d'un objectif sténopé contemporain, résolution Full HD	90 j Autonomie en veille d'un traceur GPS moderne à batterie
--	---	---

Cette accessibilité change la nature du problème. Le profil de l'auteur n'est plus celui d'un professionnel du renseignement, mais celui d'un ex-conjoint, d'un associé en conflit, d'un concurrent local, d'un bailleur curieux ou d'un collègue. C'est ce qui explique que la détection soit devenue un sujet de vie quotidienne, et non plus un sujet de sécurité industrielle.

UN MOT SUR LES CHIFFRES QUE VOUS LIREZ AILLEURS

Le marché de la contre-surveillance produit beaucoup de statistiques spectaculaires et peu de statistiques vérifiables. Il n'existe pas, en France, de recensement officiel des dispositifs de surveillance illicites découverts chaque année : par nature, ceux qui ne sont pas trouvés ne sont pas comptés, et une grande partie de ceux qui sont trouvés ne fait l'objet d'aucune plainte. Méfiez-vous des prestataires qui vous annoncent des pourcentages précis. Ce qui est certain et documenté, ce sont les décisions de justice, les prix du matériel et les capacités techniques — c'est sur ces trois piliers que ce guide est construit.

1.2 Les six contextes à risque

Dans notre pratique, la quasi-totalité des cas confirmés se rattache à l'une de ces six situations. Si vous ne vous reconnaissez dans aucune, la probabilité que vous soyez la cible d'une surveillance active est faible — ce qui ne dispense pas de la vérification, mais permet de la calibrer.

1. La séparation conflictuelle

C'est le premier contexte, de très loin. La rupture d'un couple crée simultanément un mobile (jalousie, contrôle, préparation d'un divorce pour faute, enjeu de garde), un accès historique (l'auteur a vécu dans les lieux, connaît les codes, a manipulé le téléphone, a une clé du véhicule) et un bénéfice perçu. Les dispositifs rencontrés sont généralement le logiciel espion installé sur le téléphone avant le départ, la balise sous le véhicule, et le partage de localisation resté actif.

2. Le contentieux économique

Litige entre associés, cession d'entreprise, procédure prud'homale à fort enjeu, contentieux commercial. La cible est le contenu des échanges avec l'avocat, la stratégie de négociation, le prix plancher. Les lieux visés sont la salle de réunion, le bureau du dirigeant et le véhicule de fonction.

3. L'opération stratégique en cours

Fusion-acquisition, levée de fonds, réponse à un appel d'offres, lancement produit. Le coût d'une fuite se compte en points de valorisation. C'est le seul contexte où l'on rencontre encore des dispositifs de qualité professionnelle, posés par des acteurs qui savent ce qu'ils font.

4. L'accès physique récent et non supervisé

C'est le facteur déclenchant le plus sous-estimé. Emménagement dans des locaux ou un logement occupés auparavant par quelqu'un d'autre, travaux, intervention d'un prestataire (électricien, plombier, société de nettoyage, installateur de box ou d'alarme), location saisonnière, sous-location, colocation qui se termine mal. Toute période pendant laquelle une personne non supervisée a passé du temps seule dans vos murs est une fenêtre d'opportunité.

5. L'exposition publique ou politique

Élu, candidat, dirigeant d'association, journaliste, lanceur d'alerte, syndicaliste. Le mobile n'est pas économique mais réputationnel : il s'agit d'obtenir un enregistrement compromettant ou d'anticiper une prise de position.

6. Le harcèlement et le contrôle coercitif

Un ancien partenaire, un voisin, parfois un inconnu, dont l'objectif n'est ni l'argent ni l'information mais le contrôle lui-même. C'est le contexte le plus dangereux pour la personne concernée, parce que la découverte du dispositif peut déclencher une escalade. Le chapitre 13 y consacre une procédure spécifique.

LE TEST DES TROIS CONDITIONS

Posez-vous les trois questions dans cet ordre. **Mobile** : quelqu'un a-t-il un intérêt concret, chiffrable ou émotionnel, à connaître ce que je dis ou fais ? **Accès** : cette personne a-t-elle pu, physiquement, se trouver seule dans mes locaux, dans mon véhicule ou avec mon téléphone déverrouillé ? **Bénéfice** : observe-t-on des faits qui s'expliquent mieux par une surveillance que par le hasard ? Si les trois réponses sont oui, la vérification n'est plus une précaution : c'est une priorité.

1.3 Les signaux qui comptent — et ceux qui ne comptent pas

La difficulté centrale du diagnostic est que les symptômes réputés révélateurs d'une surveillance sont, dans l'immense majorité des cas, l'expression normale du fonctionnement d'un appareil moderne. Un téléphone qui chauffe, une batterie qui tient moins qu'à l'achat, un grésillement dans un appel : ce sont des banalités techniques. Elles ne

Les six contextes qui doivent alerter

La surveillance illicite n'arrive pas au hasard : elle suppose un intérêt, un mobile et souvent un accès. Si votre situation ressemble à l'une de celles-ci, une vérification se justifie.



1 • La séparation conflictuelle

Divorce, rupture, garde d'enfants : le contexte n°1. Téléphone, véhicule et domicile sont visés.



2 • Le contentieux économique

Litige d'affaires, concurrence, associé en conflit : la fuite d'information a une valeur.



3 • L'opération stratégique

Négociation, levée, rachat, dépôt : une échéance connue attire la captation.



4 • L'accès physique récent

Réparation, prêt du véhicule, invité, ex ayant un double : un accès non supervisé suffit.



5 • L'exposition publique

Personnalité, mandat, médiatisation : la cible a une valeur pour un tiers ou un curieux.



6 • Le contrôle coercitif

Harcèlement, emprise, violences : la surveillance y sert à contrôler la victime.

À retenir : plusieurs contextes peuvent se cumuler. Plus votre situation en réunit, moins il faut attendre pour vérifier.

deviennent des indices que par leur **soudaineté**, leur **concomitance** avec un événement, et leur **convergence** avec d'autres signaux.

GRILLE DE LECTURE DES SIGNAUX

OBSERVATION	EXPLICATION BANALE	CE QUI EN FERAIT UN INDICE
Batterie du téléphone qui se vide beaucoup plus vite	Vieillessement de la batterie, mise à jour du système, nouvelle application	Dégradation <i>brutale</i> , apparue en quelques jours, sans mise à jour ni nouvel usage, et persistant après redémarrage
Téléphone chaud au repos	Charge, indexation, synchronisation photo, réseau faible	Chaleur écran éteint, sans charge, sans application ouverte, de façon répétée
Consommation de données mobiles anormale	Vidéo en arrière-plan, sauvegarde cloud, mise à jour automatique	Volume important attribué à une application système générique ou inconnue, en pleine nuit
Bruits, échos ou clics pendant les appels	Qualité réseau, VoLTE, casque Bluetooth, opérateur	Quasiment jamais un indice. Les interceptions modernes n'introduisent pas de bruit audible. Ce mythe date de la téléphonie analogique.
Écran qui s'allume seul, redémarrages	Notifications, bug applicatif, mise à jour	Redémarrages répétés à heure fixe, écran actif pendant une conversation sensible
Objet déplacé, vis desserrée, poussière déplacée	Ménage, maintenance, mémoire imparfaite	Objet déplacé dans une pièce fermée à clé, vis dont la fente a changé d'orientation, trace nette dans la poussière
L'autre partie « sait » des choses	Recoupement, indiscrétion d'un tiers, réseaux sociaux, métadonnées de photos	Connaissance d'un propos tenu à huis clos, dans un lieu précis, sans témoin
Véhicule retrouvé exactement là où on l'attendait	Habitudes de trajet prévisibles	Interception sur un trajet inhabituel et non annoncé, plusieurs fois

LE SIGNAL LE PLUS FIABLE

Il n'est pas technique : c'est **la fuite d'un propos tenu à huis clos**. Si une information n'a existé que dans une pièce fermée, entre deux personnes, sans écrit, sans téléphone, et qu'elle ressort à l'extérieur, vous avez un problème dont la surveillance technique est l'explication la plus économique. C'est le seul indice qui justifie, à lui seul, une intervention professionnelle immédiate.

1.4 Ce qui n'est pas une surveillance technique

Avant d'engager du temps et de l'argent dans une détection, éliminez les explications concurrentes. Elles sont statistiquement plus fréquentes que le micro caché.

- **L'accès légitime resté ouvert.** Un compte iCloud ou Google partagé, une sauvegarde commune, un « partage de position familial » activé il y a deux ans, un ancien identifiant sur un ordinateur du foyer, un abonnement de suivi de véhicule souscrit par l'employeur ou le loueur. Ce n'est pas de l'espionnage : c'est une configuration oubliée. Le chapitre 7 vous fait passer en revue toutes ces portes.

- **Le renseignement en source ouverte.** Une part considérable de ce que l'on croit « volé » a été publié. Photos géolocalisées, publications de proches, avis en ligne, annonces, registres publics d'entreprises, cadastre, réseaux professionnels. Un adversaire méthodique reconstitue beaucoup de votre quotidien sans jamais rien poser chez vous.
- **L'indiscrétion humaine.** Un collègue, un proche, un prestataire commun. Elle reste, de loin, le premier canal de fuite.
- **Les objets connectés que vous avez installés vous-même.** Enceinte vocale, caméra de surveillance domestique dont un tiers a conservé l'accès, babyphone, sonnette connectée, montre, télévision. La question n'est pas « y a-t-il un micro chez moi » — il y en a probablement une dizaine — mais « qui a accès à ces micros ».

COMMENCEZ PAR LE MOINS CHER

L'ordre de vérification rentable est toujours le même : d'abord les comptes et les accès numériques (gratuit, une heure), ensuite l'inspection visuelle des lieux et du véhicule (gratuit, une demi-journée), enfin seulement l'instrumentation. Inverser cet ordre est la première erreur des personnes inquiètes, et la plus coûteuse.