

 Livre Blanc

Recruter en **confiance** grâce à la vérification pré-embauche

Le guide pratique du background
check en France.



01 Édito

- “Background check” : un terme qui fait peur, un cadre français peu connu
- Qu'est-ce qu'un background check ?



02 Le risque humain, un enjeu sous-estimé

- L'angle mort des entreprises
- Ce que disent les chiffres



03 Un cadre légal clair, encore méconnu

- France ≠ États-Unis : déconstruire le malentendu
- Le cadre légal régi par le RGPD, en 4 principes
- Les secteurs réglementés : un modèle dont tout le monde peut s'inspirer
- Les origines du background check : de la contrainte à la démarche volontaire



04 Vérifier, un levier de confiance et de marque employeur

- L'autorisation, la base de toute vérification
- Accompagner le candidat : la clé d'une vérification fluide
- Vrai ou faux background check ?



05 Le coût de l'inaction

- Les quatre dimensions du coût de l'inaction
- Découvrir un mensonge après l'embauche : le parcours du combattant



06 Passer à l'action, simplement

- Proportionner : tous les postes ne se valent pas
- Vérifier à l'embauche seulement, ou en continu ?
- Auto-diagnostic : où en est votre organisation ?



07 Pour aller plus loin

- Sécurisez vos recrutements, sans alourdir vos process



“Background check” : un terme qui fait peur, un cadre français peu connu

Quand j'ai commencé à parler de background check en France il y a dix ans, deux réactions revenaient sans cesse :

01

Ah, comme aux États-Unis, le criminal record, les enquêtes...

02

Mais est-ce que c'est légal chez nous ?

Ces deux phrases résument à elles seules le malentendu français.

Le terme « background check » nous vient du monde anglo-saxon, et avec lui tout un imaginaire : fouille du passé, contrôle intrusif, suspicion permanente. Résultat, beaucoup d'entreprises rangent le sujet dans la case « pas pour nous », soit parce qu'elles le croient réservé aux secteurs réglementés, soit parce qu'elles le pensent contraire à notre culture ou à notre droit.

C'est doublement dommage. D'une part, car le risque, lui, est bien réel : un CV sur huit* contient un écart notable ou majeur avec la réalité. Et d'autre part, car la France dispose d'un cadre clair, protecteur, qui permet de vérifier les faits sans jamais transformer un recrutement en enquête de police.

Ce document n'est pas une plaquette commerciale, c'est un guide. Il explique ce que le droit français autorise et interdit, comment mener une vérification respectueuse du candidat et de votre marque employeur, comment décider du niveau de contrôle adapté à chaque poste. Vous en ressortirez, je l'espère, avec une vision plus juste et quelques questions concrètes à vous poser sur votre propre organisation.



Yohan Zibi,
Fondateur d'EveryCheck

*source : EveryCheck, 2025.

Qu'est-ce qu'un background check ?

Le mot est anglais, l'imaginaire qu'il traîne est américain, et sa définition reste floue pour beaucoup ou limitée à la vérification de CV. Avant d'entrer dans le cadre légal et les bonnes pratiques, posons une base claire : de quoi parle-t-on exactement quand on parle de background check ?



Background check : Définition

Un background check est la vérification factuelle des informations données par un candidat ou un collaborateur concernant son parcours professionnel, complétée si besoin par des éléments objectifs recherchés avec son accord, notamment dans le cadre d'une vérification d'intégrité. L'objectif est de sécuriser une décision de recrutement ou l'exercice d'une fonction, en s'appuyant sur des faits fiables et vérifiés.

Un background check couvre :

- ✓ La vérification d'identité
- ✓ La vérification des diplômes
- ✓ La vérification du parcours professionnel
- ✓ La vérification des références

C'est le socle, souvent appelé "vérification de CV" ou "vérification des antécédents professionnels"

Un background check complet ajoute la dimension d'intégrité quand le poste le justifie : vérification du casier judiciaire, de sanctions incompatibles avec l'exercice du métier, de potentiels conflits d'intérêts, d'une exposition médiatique sensible ou d'une présence en ligne pouvant exposer l'entreprise à un risque réputationnel.

Un background check n'est pas :

- ✗ Une enquête de moralité
- ✗ Une fouille de la vie privée
- ✗ Une surveillance des réseaux sociaux injustifiée
- ✗ Une consultation du casier judiciaire à l'insu de la personne

Ces pratiques sont encadrées voire interdites en France.

Note : Dans le cadre d'un recrutement, le background check arrive en fin de process. Par conséquent, il n'est pas fait pour piéger ou écarter un candidat, bien au contraire. La vérification sert avant tout à valider l'intuition positive du recruteur et de sécuriser une décision par des faits pour démarrer une collaboration en toute confiance.

L'angle mort des entreprises

Définition

Le risque humain, c'est la possibilité qu'une personne, par ce qu'elle a caché, falsifié ou par un profil incompatible avec sa fonction, cause un dommage à l'organisation qui l'emploie. Un faux diplôme, une expérience inventée, un passé de fraude, un conflit d'intérêts non déclaré : autant de réalités qu'un entretien ne révèle pas, et qui ne se manifestent souvent qu'une fois la personne en poste.

Le risque humain : un sujet qui n'appartient à personne et à tout le monde à la fois

Ce risque a une particularité. Personne n'en est propriétaire, alors que tout le monde en subit les conséquences.



La direction RH gère le recrutement, l'administratif, et le time to hire

Pourtant elle engage sa responsabilité si elle fait entrer la mauvaise personne sans avoir pris de précaution.



La direction Conformité et/ou Juridique gère la réglementation et la conformité.

Elle doit aussi prouver la diligence de l'entreprise en cas d'audit.



La Direction Générale gère la stratégie et le business.

Mais c'est elle qui encaisse la perte de chiffre d'affaires, l'atteinte à la réputation, parfois la mise en cause personnelle du dirigeant en cas d'incident.

La responsabilité de la vérification est discutable mais la facture, elle, tombe chez tout le monde.

S'y ajoutent trois réflexes qui minimisent le sujet :

- ❗ **La confiance par défaut** : un entretien convaincant suffit souvent à emporter la décision, au détriment de la vérification.
- ❗ **Le coût perçu comme accessoire** : la vérification est vue comme une dépense superflue, jusqu'à ce qu'un recrutement raté en révèle le coût réel.
- ❗ **L'illusion de l'exception** : la conviction que ce risque ne touche que les autres, tant qu'aucun incident n'est venu la contredire.

Le risque le plus sous-estimé vient de l'intérieur

On pense volontiers aux menaces externes, mais le risque interne (ce qu'on appelle en anglais l'*insider threat*) est souvent le plus lourd de conséquences : c'est une personne déjà dans la place, avec des accès et la confiance de l'organisation. C'est précisément ce risque qu'une **cartographie des risques**, l'exercice par lequel une direction identifie et hiérarchise ses zones d'exposition, doit intégrer, au même titre que les risques financiers ou cyber.

Ce que disent les chiffres

Les chiffres sur la fraude ou les écarts dans le recrutement doivent être lus avec prudence : ils varient selon les méthodes, les pays et les déclarations. Mais leur convergence dessine une tendance nette.

1 CV/8

présentait un écart notable ou majeur avec la réalité en 2025, contre 1 sur 12 en 2024.

(EveryCheck, 2025)

+103 %

de hausse du volume de CV présentant un écart avec la réalité entre 2024 et 2025, et +45 % pour les seuls écarts majeurs.

(EveryCheck, 2025)

+23 %

d'augmentation des fraudes liées à la fraude interne sur cinq ans.

(Allianz Trust, 2024)

67 %

des cadres dirigeants se disent prêts à un comportement non éthique pour leur intérêt personnel.

(EY Global Integrity, 2023)



Le coût d'un mauvais recrutement

Selon les estimations couramment citées, un recrutement raté sur un poste cadre coûte **entre 30 000 et 150 000 euros*** ou plus simplement, **environ un an de salaire**. Le chiffre surprend, jusqu'à ce qu'on additionne tout ce qu'un mauvais recrutement englutit, bien au-delà du seul salaire versé.

Les coûts directs :

- Le salaire et les charges de la personne recrutée sur la période
- Le salaire des personnes sollicitées pour le recrutement : les heures des équipes RH, Paie, des managers et des dirigeants mobilisés en entretien
- Le coût éventuel d'un cabinet ou d'une annonce
- La formation initiale, pendant laquelle la personne ne produit pas encore de valeur mais mobilise celles et ceux qui l'accompagnent
- Le coût de la séparation lorsqu'elle devient nécessaire : procédure, indemnités, temps de gestion.
- Le coût de tout recommencer : un poste de nouveau vacant, un recrutement complet à relancer, puis un nouveau collaborateur à former et à faire monter en compétence.

Les effets indirects, plus difficiles à chiffrer mais bien réels :

- La désorganisation de l'équipe qui a absorbé les manques et la charge reportée sur les collègues
- La perte de confiance interne
- L'atteinte à la réputation vis-à-vis des clients ou des partenaires.

Mis bout à bout, ces montants sont sans commune mesure avec le coût d'un background check en amont.

*source : étude Manpower / OpenSourcing / HR Voice, 2020.

France ≠ États-Unis : déconstruire le malentendu



Yohan Zibi,
Fondateur d'EveryCheck

“L'image qu'on se fait du background check est américaine. Le cadre qui s'applique, lui, est bien français.”

Aux États-Unis, vérifier un candidat peut signifier rechercher directement son casier judiciaire dans les registres publics, interroger son historique de crédit, passer au crible ses réseaux sociaux voire même imposer un test de dépistage aux drogues. Cette culture du contrôle étendu s'est exportée avec le terme « background check » et beaucoup de dirigeants français imaginent que c'est de cela qu'on parle.

C'est faux. En France, la vérification obéit à une logique inverse : on ne cherche pas à tout savoir, seulement ce qui a un lien direct avec le poste.

Une différence culturelle, pas seulement juridique

Le malentendu tient aussi à une différence de culture. Le monde anglo-saxon vit depuis longtemps dans une logique de vérification, résumée par la formule de Ronald Reagan dans les années 1980 : « *Trust but verify* », faire confiance mais vérifier. C'est là que les background checks se sont généralisés. La culture latine, elle, a longtemps préféré le ressenti, l'intuition, le feeling d'un entretien, percevant la vérification comme une défiance importée. Cette culture évolue : à mesure que les enjeux se matérialisent (fraude, réglementation, responsabilité des dirigeants), vérifier devient une marque de sérieux plutôt qu'un manque de confiance. **Le feeling ne disparaît pas, il s'appuie désormais sur des faits.**



Quelques différences de fond

	 Modèle américain	 Cadre français
Casier judiciaire :	Consultation fréquente et large, parfois libre d'accès.	Sur demande au candidat, dans un cadre légal strict.
Historique de crédit :	Couramment utilisé.	Interdit dans le cadre d'un recrutement.
Réseaux sociaux :	Passés au crible.	Données publiques, pertinentes au regard du poste, avec l'accord du candidat.
Principe directeur :	Tout savoir sur le candidat.	Vérifier ce qui a un lien direct et nécessaire avec le poste.



Le cadre français n'est donc ni le fantasme américain, ni une zone de non-droit. **C'est un régime précis,** protecteur pour le candidat comme pour l'entreprise, que détaillent les pages suivantes.

Le cadre légal régi par le RGPD, en 4 principes

En France, toute vérification repose sur le Code du travail et le RGPD. Loin d'empêcher le background check, ces textes lui donnent une méthode, un cadre clair, et rendent la pratique saine et sûre pour les candidats et les entreprises.

Les 4 grands principes qui cadrent le background check :

01

La finalité légitime

Toute vérification doit poursuivre un but précis et légitime : s'assurer qu'un candidat peut occuper le poste en confiance. L'article L.1221-6 du Code du travail le pose clairement, les informations demandées à un candidat ne peuvent servir qu'à apprécier sa capacité à occuper l'emploi. On ne vérifie pas pour savoir, on vérifie pour décider.

02

La proportionnalité

C'est le principe de minimisation : on ne collecte que ce qui est nécessaire à cette finalité. On ne vérifie pas tout, on vérifie ce qui compte pour ce poste précis. Une fonction en contact avec des fonds n'appelle pas les mêmes contrôles qu'un poste sans accès sensible.

03

La transparence

Le candidat doit être informé avant toute vérification, de ce qui sera contrôlé et pourquoi, et doit l'accepter explicitement. Aucune vérification ne se fait à son insu ni sans son autorisation. C'est une obligation légale et, on le verra plus loin, un atout.

04

Le droit et la loyauté

La vérification s'appuie sur une base légale et se mène loyalement. Le candidat autorise la vérification, participe, et conserve ses droits sur les données le concernant : accès, rectification, et une conservation limitée dans le temps, les données étant supprimées une fois le délai nécessaire écoulé.



La différence entre "Conforme RGPD" et "certifié CNIL"

Un abus de langage courant mérite d'être corrigé. On dit d'un dispositif qu'il est conforme au RGPD, le règlement européen qui fixe les règles. La CNIL, elle, est l'autorité de contrôle : elle veille au respect du RGPD, mais elle ne « certifie » pas les entreprises. Parler de « certification CNIL » n'a pas de sens. La bonne formule est « conforme RGPD », idéalement « RGPD by design », c'est-à-dire pensé dès la conception pour respecter ces règles, comme c'est le cas d'EveryCheck, lancé la même année que le RGPD.

Les secteurs réglementés : un modèle dont tout le monde peut s'inspirer

Dans plusieurs secteurs, la vérification n'est pas une option, c'est une obligation légale. La banque et l'assurance appliquent le standard « **Fit & Proper** », imposé par les régulateurs (ACPR, AMF) pour les dirigeants et les fonctions clés. Derrière ce terme, deux exigences :

- ✓ **La compétence (Fit) :** s'assurer que la personne a les qualifications et l'expérience nécessaires à l'exercice du poste
- ✓ **L'honorabilité (Proper) :** vérifier l'absence d'antécédents ou de condamnations incompatibles avec des responsabilités qui engagent l'argent des clients et la stabilité du système financier.

La santé, la sécurité privée, la petite enfance ou le transport imposent de leur côté des vérifications d'intégrité pour protéger des publics vulnérables ou des activités sensibles.

Ce que ces réglementations disent du background check

Ces obligations ont un point commun instructif : elles ne se contentent pas de demander de vérifier, elles demandent de pouvoir le prouver. Un régulateur qui contrôle une banque n'attend pas une bonne intention, il attend un dossier : qui a été vérifié, sur quels critères, quand, et avec quelle traçabilité. Le background check y est donc pensé non comme un geste ponctuel à l'embauche, mais comme un dispositif documenté, opposable, tenu dans le temps. C'est une conception plus mature de la vérification, dont tous les secteurs peuvent s'inspirer.

Pourquoi ces obligations sont justifiées

Ces règles ne sont pas des tracasseries administratives. Elles existent parce que l'expérience a montré ce qu'un profil non vérifié pouvait coûter : fraude dans la finance, mise en danger dans la santé, atteinte à la sûreté dans les infrastructures. La réglementation a simplement tiré les leçons des incidents passés.

Demain, un périmètre plus large

Le mouvement ne s'arrête pas là. La réglementation s'étend, et le risque humain entre progressivement dans des textes qui ne le nommaient pas hier : **NIS2** (Network and Information Security) et **DORA** (Digital Operational Resilience Act) pour la résilience numérique et la cybersécurité, **CER** (Critical Entities Resilience) pour les entités critiques. À mesure que ces cadres montent en puissance, de nouveaux secteurs seront concernés comme l'énergie, les télécoms, la logistique, la tech au service d'infrastructures sensibles, la santé numérique. La question n'est plus vraiment de savoir si la vérification deviendra un standard partout, mais quand.



À retenir : attendre d'y être contraint, c'est subir la contrainte dans l'urgence, souvent au pire moment. S'en inspirer dès maintenant, c'est prendre de l'avance sur une pratique qui, partout, devient la norme.

Les origines du background check : de la contrainte à la démarche volontaire

La vérification n'est pas née dans les RH. Elle vient du monde de la finance et de la lutte contre la criminalité, avant de devenir, pour les entreprises les plus matures, un choix assumé.



D'où vient la pratique : KYC, AML, LCB-FT

Le premier grand moteur du background check n'a rien à voir avec le recrutement.

Ce sont les obligations dites KYC (*Know Your Customer*, « connaître son client ») imposées aux banques pour vérifier l'identité et l'intégrité de leurs clients. Elles découlent des standards internationaux de lutte contre le blanchiment d'argent (AML, *Anti-Money Laundering*) et le financement du terrorisme, transposés en droit français sous l'appellation LCB-FT (lutte contre le blanchiment de capitaux et le financement du terrorisme) via les directives européennes.

Ces cadres ont installé, secteur par secteur, un principe simple : avant d'entrer en relation avec quelqu'un, on vérifie qui il est. Le passage du client à l'employé (le *Know Your Employee*) était une suite logique.

La vérification comme choix, pas seulement comme obligation

Toutes les vérifications ne sont pas imposées par un régulateur. Certaines relèvent d'une démarche volontaire de transparence. La certification ISO 27001, référence internationale en sécurité de l'information, en est un bon exemple : une entreprise qui la vise s'impose elle-même des exigences de contrôle, dont la vérification des personnes qui accèdent aux données sensibles. Personne ne l'y oblige : elle le décide, pour prouver son niveau de rigueur à ses clients et partenaires.



À retenir : le background check n'est pas qu'une case à cocher pour rester dans les clous. C'est aussi, pour un nombre croissant d'organisations, un standard qu'elles s'imposent volontairement, parce qu'il inspire confiance.

L'autorisation, la base de toute vérification

C'est sans doute le point le moins connu, et le plus important pour comprendre l'esprit du cadre français. La vérification repose sur l'autorisation du candidat, qui peut la refuser.

Ce refus ne peut pas être utilisé comme motif de rejet de sa candidature. Ce garde-fou est précisément ce qui distingue une vérification légitime d'une surveillance imposée.

Ce que vous ne pouvez pas faire d'un refus

- ✗ Écarter automatiquement un candidat au seul motif qu'il a refusé une vérification.
- ✗ Le mentionner comme un élément défavorable dans l'évaluation de sa candidature.
- ✗ Procéder malgré tout à la vérification sans son accord.

Alors, à quoi sert la vérification si l'on peut refuser ?

À beaucoup, justement. Dans la grande majorité des cas, un candidat de bonne foi accepte sans difficulté une vérification bien amenée dans la conversation avec le futur employeur. Vérifier ses diplômes ou son parcours ne le dérange pas, cela peut même le rassurer sur le sérieux de l'entreprise, son niveau d'éthique et de sécurité. Le droit de refus n'affaiblit pas la démarche, il la rend légitime. Il garantit qu'elle repose sur la transparence et non sur la contrainte, ce qui protège aussi l'entreprise sur le plan juridique.

Un refus n'est pas non plus dénué de sens : il ouvre une conversation. Pourquoi ce refus ? S'agit-il d'une inquiétude sur la protection des données, à laquelle on peut répondre ? D'un malentendu sur ce qui sera vérifié ? D'un signal d'alerte indiquant que le candidat a quelque chose à cacher ? Une discussion bienveillante pour comprendre et rassurer suffit bien souvent à désamorcer la situation.



Yohan Zibi,
Fondateur d'EveryCheck

« La confiance ne se décrète pas, elle se fonde. Vérifier n'est pas douter de quelqu'un : c'est se donner les moyens de lui faire confiance en connaissance de cause. Les candidats sérieux le comprennent et les meilleurs employeurs en font un signe de respect, pas de suspicion. »

Accompagner le candidat : la clé d'une **vérification** fluide

La différence entre un background check subi et un background check accepté tient presque entièrement à sa présentation. Annoncé sans explication en fin de processus, un « contrôle » met le candidat sur la défensive. Informé dès le départ qu'elle fait partie du processus standard, il la vit comme une étape normale.

Les bons réflexes



Normaliser

Présenter la vérification comme un standard appliqué à tous, qui sert à entamer sereinement l'onboarding, non comme prétexte pour rejeter une candidature.



Briefer pour aller vite

Indiquer au candidat les documents à préparer (adresses des établissements et entreprises fréquentées, dates de contrats, coordonnées de référents) pour une vérification rapide et fluide.



Annoncer tôt

Mentionner la vérification dès le début, pas au dernier moment, désamorce la méfiance.



Rester disponible

Répondre aux questions sur le processus, le cadre et les droits des candidats assure leur adhésion.



Expliquer le cadre

Préciser ce qui sera vérifié et pourquoi : le lien avec le poste rend la démarche acceptable et cohérente.

EveryCheck facilite cette communication avec vos candidats : un guide candidat les prépare à la vérification à venir et répond aux questions courantes, et notre équipe Support les accompagne dans l'utilisation de la plateforme.

Un atout pour votre marque employeur

Bien menée, la vérification est le premier contact du candidat avec vos valeurs, la première étape de l'onboarding. Claire et sécurisée, elle installe la confiance, valorise votre marque employeur et rassure les équipes déjà en place.

Le background check rallonge-t-il le recrutement ?

Non : bien organisé, il n'allonge pas le process. Un candidat briefé fournit ses justificatifs sans aller-retour, et les contrôles se mènent en parallèle des dernières étapes. Seule l'improvisation ralentit.



Info : chez EveryCheck, nos vérifications sont effectuées entre 2 et 3 jours en moyenne.

Vrai ou faux

background check ?

Face au besoin de « se renseigner », le réflexe est souvent de bricoler : une recherche Google ou LLM, un coup d'œil au profil LinkedIn, une prise de références sauvage, parfois l'achat de données douteuses. Ces pratiques cumulent le pire des deux mondes car elles exposent l'entreprise juridiquement, mais elles ne prouvent rien.

Les pratiques à proscrire

- ❌ Fouiller les réseaux sociaux personnels et collecter des données sans lien avec le poste → contraire au principe de minimisation et potentiellement discriminatoire.
- ❌ Appeler un référent sans l'autorisation du candidat et non-désigné explicitement par celui-ci → contraire au code du travail et au RGPD.
- ❌ Acheter des « fichiers » ou données d'origine incertaine → fiabilité nulle, conformité inexistante.
- ❌ Se fier à une simple recherche en ligne → certaines informations ne sont pas publiques, fiabilité de la source souvent faible, risque de trouver des homonymes ou des informations obsolètes.



Les 6 exigences d'un vrai background check

- ✓ Autorisation préalable et éclairée du candidat.
- ✓ Traçabilité : chaque vérification est documentée et peut être justifiée.
- ✓ Vérification à la source auprès de l'établissement qui a délivré le diplôme, de l'ancien employeur, de sources officielles et fiables.
- ✓ Hébergement des données dans l'Union européenne, conforme au RGPD.
- ✓ Minimisation : uniquement les données pertinentes pour le poste.
- ✓ Sécurité et durée de conservation maîtrisées, avec suppression à l'échéance.

Un risque loin d'être théorique

Le non-respect du cadre légal expose l'entreprise à plusieurs risques. Côté RGPD, la CNIL peut prononcer des mises en demeure ou des amendes jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires mondial annuel. Le candidat dispose aussi de plusieurs recours : plainte directe à la CNIL, action civile devant les prud'hommes en cas de discrimination ou de collecte déloyale, voire plainte au pénal, la discrimination à l'embauche étant un délit passible de 45 000 € d'amende et trois ans d'emprisonnement pour la personne physique responsable, un montant nettement supérieur pour l'entreprise.

C'est pour sécuriser vos recrutements sur ce plan qu'**EveryCheck intervient comme tiers de confiance** : une prestation 100 % conforme au RGPD, fiable, traçable et opposable en cas de contrôle ou d'audit, pour vérifier sereinement et en conformité.

Les quatre dimensions du coût de l'inaction

Ignorer le risque humain ne le fait pas disparaître : cela ne fait que reporter la facture, et l'alourdir. Ce coût prend quatre formes bien distinctes : financière, juridique, réputationnelle et humaine, souvent invisibles jusqu'au jour où elles se manifestent toutes à la fois.

01

Le coût Financier

Coût direct d'un recrutement raté (30 000 à 150 000 € pour un cadre*), auquel s'ajoutent les coûts indirects et de potentielles fraudes internes ou détournements.

02

Le coût Juridique

Responsabilité de l'employeur, contentieux, sanctions dans les secteurs réglementés, difficulté à se séparer d'un collaborateur après la découverte d'un mensonge.

03

Le coût Réputationnel

Un incident qui s'ébruite, en interne, chez les clients ou sur les réseaux, abîme durablement la marque et la marque employeur.

04

Le coût Humain

Une équipe déstabilisée par un profil toxique ou incompetent, une confiance collective entamée, un management qui s'épuise.

*source : étude Manpower / OpenSourcing / HR Voice, 2020.



Un cas parlant : l'affaire Kiabi

En 2024, l'enseigne Kiabi a révélé une fraude interne estimée à environ 100 millions d'euros, qu'aurait orchestrée son ancienne trésorière. L'affaire est aujourd'hui devant la justice et la personne mise en cause reste présumée innocente. Un élément, largement rapporté par la presse, retient l'attention : cette personne aurait déjà été licenciée par de précédents employeurs pour des faits de détournement similaires.

Ce que cela illustre : un simple contrôle de CV n'aurait sans doute rien révélé. C'est un background check complet associant vérification des antécédents professionnels, prise de références et enquête d'intégrité, qui aurait augmenté les chances de détecter ce passé pour une fonction aussi sensible que la trésorerie. Le risque n'était pas invisible : il n'avait simplement pas été cherché au bon endroit.

Découvrir un mensonge après l'embauche : le parcours du combattant

Une fois la personne en poste, se séparer d'elle pour un mensonge est difficile et la négligence de l'employeur peut se retourner contre lui.

Beaucoup d'employeurs pensent qu'un mensonge découvert après l'embauche justifie un licenciement immédiat. La réalité juridique est bien plus nuancée, et elle plaide fortement pour la vérification en amont.

Le mensonge, à lui seul, ne suffit **pas**

Pour la Cour de cassation, un renseignement inexact ne justifie une sanction que s'il a été **déterminant** dans la décision d'embauche et qu'il constitue un dol, une manœuvre destinée à tromper l'employeur. Un licenciement pour faute grave a ainsi été validé pour un salarié s'étant faussement prévalu d'un diplôme et d'une expérience décisifs pour le poste (Cass. soc. 25 nov. 2015, n° 14-21521 ; déjà 17 oct. 1995, n° 94-41239). Mais si le salarié dispose des compétences réelles pour occuper le poste, le mensonge ne suffit pas à fonder le licenciement (Cass. soc. 30 mars 1999, n° 96-42912).

La **négligence** de l'employeur peut se retourner contre lui

La Cour de cassation a jugé qu'un employeur **ne peut pas se prévaloir de sa propre négligence** : celui qui n'a pas vérifié un diplôme ou une certification obligatoire, alors qu'il en avait la responsabilité, ne peut pas ensuite invoquer le mensonge pour annuler le contrat ou licencier (Cass. soc. 9 juin 2017, n° 16-15244 ; confirmé le 26 mars 2025, n° 23-21414).

En clair : ne pas avoir vérifié avant peut priver l'employeur de son recours après. L'inaction initiale devient un handicap juridique.

Note : produire un faux diplôme constitue un délit de faux (article 441-1 du Code pénal), passible de trois ans d'emprisonnement et 45 000 € d'amende mais encore faut-il que la fraude ait été détectée, ce qui ramène encore une fois, à la vérification.

Proportionner : tous les postes ne se valent pas

Le principe de proportionnalité, au cœur du droit français, est le meilleur guide pratique : l'intensité de la vérification doit être calibrée sur le risque que le poste fait courir à l'organisation. Un poste sans accès sensible n'appelle pas le même niveau qu'une fonction qui manie des fonds, des données critiques ou la sécurité d'autrui.

Deux questions pour situer un poste

Quel est le pouvoir du poste ? Accès aux finances, données personnelles, systèmes critiques, pouvoir de décision, d'engagement ou de management.

Quelle serait la conséquence d'une défaillance ? Un incident coûterait-il quelques centaines d'euros ou bien plus, avec un impact sur la conformité, la réputation, voire la sécurité de personnes ?

De la cartographie des risques au niveau de vérification

Dans les fonctions conformité, juridique ou RH structurées, chaque poste est relié à une cartographie des risques, à laquelle correspond un niveau de vérification, standardisé en France comme à l'international (light, standard, enhanced) :

Vérification basique : identité, diplômes, parcours professionnel, références, pour les postes à faible exposition.

Vérification standard : références approfondies, contrôle d'intégrité adapté, pour les fonctions à responsabilité ou en contact avec des publics sensibles.

Vérification renforcée : dispositif complet, contrôle d'intégrité approfondi, réévaluation périodique, pour les fonctions les plus exposées : finance, direction, sécurité, accès à des données critiques.

Exemple de matrice de cartographie des risques

		GRAVITÉ				
PROBABILITÉ		Mineure	Faible	Moyenne	Forte	Majeure
	Quasi inévitable	5	10	15	20	25
	Probable	4	8	12	16	20
	Possible	3	6	9	12	15
	Faible	2	4	6	8	10
	Rarissime	1	2	3	4	5
		Risque non critique Risque à surveiller Risque à traiter en priorité				

Vérifier à l'embauche seulement, ou en continu ?

Le risque humain n'est pas figé à la signature du contrat : il évolue avec le poste et la personne. Le recrutement reste le moment naturel du background check, mais pas le seul : le risque peut aussi se déplacer après l'embauche, avec une promotion sensible, un changement de périmètre, une évolution réglementaire ou un événement personnel.

Un cadre de lecture : le triangle de la fraude

Ces évolutions ne sont pas anodines : elles peuvent modifier les conditions du triangle de la fraude, modèle du criminologue Donald Cressey, qui identifie trois facteurs d'un passage à l'acte : une pression, une opportunité liée à un accès ou contrôle insuffisant, et une rationalisation permettant de justifier le geste à ses propres yeux. Ces facteurs évoluent à tout moment d'une carrière, c'est pourquoi le risque n'est jamais figé. Le background check n'a pas de prise sur la pression, imprévisible, mais agit sur l'opportunité en écartant en amont les profils déjà identifiés.

Trois moments à considérer

- **À l'embauche.** Vérifier avant de s'engager, quand la marge de manœuvre est maximale et le coût minimal.
- **En poste.** Lors d'une mobilité vers une fonction plus sensible, ou d'une exigence réglementaire nouvelle qui étend le périmètre à vérifier.
- **Sur événement déclencheur.** Un incident, un audit, une prise de fonction critique peuvent justifier une réévaluation ciblée, toujours dans le respect du cadre légal et de la transparence.

Le juste équilibre : la vérification continue ne signifie pas surveiller en permanence. Elle signifie réévaluer aux moments qui comptent, sur les postes qui le justifient et avec la même transparence qu'à l'embauche.

Pression

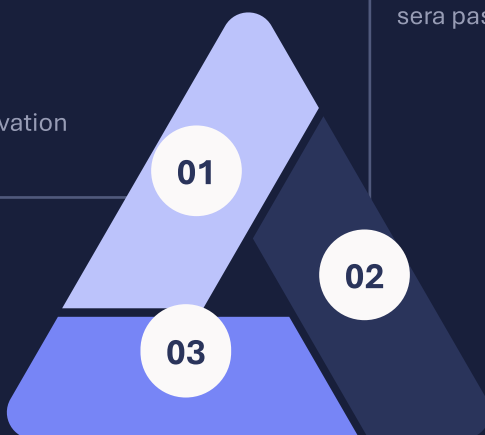
La pression financière ou professionnelle crée la motivation de la fraude

Opportunité

La perception d'un dispositif de contrôle absent ou trop faible donne le sentiment que l'on ne sera pas détecté.

Rationalisation

Le fraudeur se convainc que son acte n'est pas criminel. Il ne fait que pour compenser une situation injuste selon lui.



Auto-diagnostic : où en est votre organisation ?

Onze questions pour évaluer votre dispositif actuel et repérer vos angles morts. Ce diagnostic n'a pas de bonne ou mauvaise note. Chaque « non » ou « je ne sais pas » signale simplement un point à examiner. Parcourez-le pour votre organisation.

Comment lire vos réponses : plus vous cumulez de « oui » assurés, plus votre dispositif est solide. Les « je ne sais pas » sont souvent les plus instructifs, ils désignent les zones où le risque est présent sans que personne ne l'adresse.

Questions	Oui	Non	Je ne sais pas
Savez-vous précisément qui porte la responsabilité de s'assurer que les bonnes personnes entrent dans l'entreprise, et que la sécurité et l'intégrité des équipes sont préservées ?	☐	☐	☐
Vérifiez-vous systématiquement l'identité, les diplômes et le parcours sur vos postes sensibles ?	☐	☐	☐
Vos vérifications reposent-elles sur des sources fiables ?	☐	☐	☐
Informez-vous le candidat, en amont, de ce qui sera vérifié et pourquoi ?	☐	☐	☐
Recueillez-vous son autorisation, et savez-vous quoi faire en cas de refus ?	☐	☐	☐
Vos données de vérification sont-elles hébergées dans l'UE, sécurisées et supprimées à échéance ?	☐	☐	☐
Pourriez-vous, en cas d'audit ou de litige, démontrer ce qui a été contrôlé sur un recrutement donné ?	☐	☐	☐
Adaptez-vous le niveau de vérification à la sensibilité du poste ?	☐	☐	☐
Avez-vous identifié les postes qui, chez vous, justifieraient une vérification renforcée ?	☐	☐	☐
Réévaluez-vous le risque régulièrement pour les fonctions sensibles ?	☐	☐	☐
Votre entreprise peut-elle se permettre une fraude, une perte financière, une atteinte réputationnelle, un défaut de sécurité ?	☐	☐	☐

Sécurisez vos recrutements, sans alourdir vos process

Depuis 2015, EveryCheck aide les entreprises françaises à recruter en toute confiance : nos vérifications sécurisent votre décision et protègent votre organisation, sans ralentir vos process ni transiger sur la conformité légale. En 2025, plus de 75 000 vérifications ont été réalisées pour plus de 150 clients, de la PME au grand groupe.

Ce que couvrent nos background checks

- ✓ Vérification **d'identité**
- ✓ Vérification des **diplômes et certifications**
- ✓ Vérification du **parcours professionnel**
- ✓ **Prise de références** désignées
- ✓ Vérification du **casier judiciaire** (mention néant du bulletin n°3)
- ✓ Exposition médiatique **négative**
- ✓ Personnes **Politiquement Exposées**
- ✓ Listes de **sanctions** et de surveillance internationales
- ✓ **Situation** entrepreneuriale et mandats sociaux
- ✓ Exposition **risquée** sur les réseaux sociaux

Ce qui fait la différence



Une équipe d'experts
basée à **Rennes**

Qui mène chaque vérification et
vous accompagne à chaque
étape.



Une technologie pensée
pour s'intégrer dans vos
process :

Plateforme intuitive,
intégrations ATS, et des
investissements continus en
R&D.



Une plateforme conçue
RGPD by design

Plateforme hébergée en **France**
et traçabilité complète.



Une exécution rapide :

Nos vérifications sont réalisées en **2 à 3 jours** en
moyenne.

"EveryCheck réalise près de 600
vérifications par an pour notre société.
Nous avons pu constater l'excellence de
leurs services, qui se distinguent par
leur fiabilité et leur efficacité."



Laetitia Thirion

Responsable Développement RH
La Poste Branche Grand Public et
Numérique



Envie d'échanger sur votre contexte ?

Prenez rendez-vous avec l'un de nos experts en
conformité RH.

Prendre rendez-vous



everycheck.com



02 23 61 32 59



Livre Blanc

Recruter en confiance grâce à la vérification pré-embauche

Le guide pratique du background check en France.