

Fraude, deepfakes et confidentialité : l'assistante en première ligne de la sécurité de l'information

Étude de l'Observatoire des Métiers de l'Assistanat Moderne · 12 octobre 2026

Synthèse

En 2025, la fraude par manipulation a atteint 516 millions d'euros en France, soit plus de 40 % de la fraude aux moyens de paiement, et les deepfakes permettent d'imiter la voix et le visage d'un dirigeant. L'assistante, qui connaît l'agenda du dirigeant et se trouve proche des paiements, est une cible naturelle de ces attaques. Une procédure écrite et répétée réduit ce risque.

- **Le chiffre clé.** 516 M€ de fraude par manipulation en 2025, part doublée en quatre ans (Banque de France).
- **Le cas de référence.** Arup, 25,6 M\$ versés en 15 virements après une visioconférence deepfake (CNN, 2024).
- **Le réflexe prioritaire.** Rappeler le dirigeant sur un numéro connu avant toute action financière, et valider à deux sans exception.
- **Le cadre.** Violation de données : notification à la CNIL sous 72 heures si le risque est avéré ; programme CNIL 2026 sur les échanges par messagerie, la transcription et l'IA au travail.
- **L'assistanat privé.** Aucune statistique publique ne mesure la fraude dans ce segment ; l'étude propose une analyse des facteurs de risque propres à ces postes.
- **La formation.** Six compétences à développer, avec des livrables concrets : procédure de validation, charte d'usage de l'IA, fiche réflexe d'incident.

1. Introduction et méthode

L'assistante concentre sur son poste trois ressources que les fraudeurs convoitent : l'accès au dirigeant, la connaissance de son agenda et de ses habitudes, et la proximité avec les circuits de paiement. Cette étude examine comment la fraude par manipulation, dopée par les deepfakes, a fait de ce poste une cible, et quelles pratiques permettent d'y répondre.

Le sujet a pris de l'ampleur dans les statistiques officielles. Selon l'Observatoire de la sécurité des moyens de paiement, la fraude par manipulation (faux conseillers bancaires, fraude au président, substitution d'IBAN) a atteint 516 millions d'euros en 2025, soit un

peu plus de 40 % de la fraude totale aux moyens de paiement. Sa part a doublé en quatre ans.

La démarche repose sur des sources publiques consultées le 12 octobre 2026 : le rapport 2025 de l'Observatoire de la Banque de France, les fiches de Cybermalveillance.gouv.fr et de la CNIL, le programme de travail 2026 de la CNIL, l'enquête Deloitte de 2024 sur les deepfakes financiers, le cas Arup documenté par CNN, et le baromètre AFFO x EY 2026 pour le contexte des family offices.

Trois limites encadrent la lecture.

1. Les statistiques officielles décrivent la fraude aux moyens de paiement en général, sans isoler les entreprises, les particuliers fortunés ou les assistantes.
2. Les chiffres Deloitte datent de 2024 et portent sur des dirigeants d'entreprise uniquement.
3. Enfin, aucune enquête publique consultée ne mesure la fraude visant spécifiquement l'assistanat privé : les passages consacrés à ce segment relèvent de l'analyse de l'Observatoire et sont signalés comme tels.

2. État de la menace

La fraude par manipulation pèse 516 millions d'euros en 2025, soit plus de 40 % d'un total de 1,2 milliard d'euros de fraude aux moyens de paiement. Le montant global progresse de 3,8 %, tandis que le nombre de transactions frauduleuses recule de 8 % (7,2 millions). La fraude par carte baisse, la fraude qui repose sur la victime elle-même gagne du terrain. Ce constat figure dans le [rapport 2025 de l'Observatoire de la sécurité des moyens de paiement](#).

Indicateur (France, 2025)	Valeur
Fraude totale aux moyens de paiement	environ 1,2 Md€ (+ 3,8 %)
Transactions frauduleuses	7,2 millions (- 8 %)
Fraude par manipulation	516 M€, plus de 40 % du total
Part de la manipulation dans la fraude	doublée en quatre ans
Taux de fraude par carte	47 € pour 100 000 € de paiements
Virements instantanés	17 % des virements émis, valeur annuelle doublée entre 2024 et 2025

Ce dernier point est particulièrement intéressant. Le virement instantané est irréversible et se fait en quelques secondes. Plus il se généralise, moins il reste de temps pour rappeler les fonds après une erreur de jugement. Le rapport ne ventile pas la fraude au virement par type de client : on ne peut donc pas isoler la part qui touche les entreprises ou les patrimoines privés.

L'arrivée des deepfakes

La fraude au président classique repose sur un email urgent et confidentiel. Les deepfakes vont plus loin et peuvent être redoutablement efficaces en ajoutant la voix et l'image. L'enquête Deloitte menée en mai 2024 auprès de plus de 1 100 dirigeants, relayée par [Le Monde Informatique](#), donne l'ordre de grandeur : environ 15 % d'entre eux ont vu leurs données financières ou comptables visées par un deepfake au moins une fois dans l'année, 11 % ont été victimes de plusieurs arnaques de ce type, et plus de la moitié s'attendaient à une hausse. Environ 10 % indiquaient que leur entreprise ne faisait rien pour s'en protéger. Deloitte précise que le nombre réel est probablement plus élevé, car les entreprises communiquent peu sur ces incidents.

Le cas Arup, repère de ce que permet la technique

Le groupe d'ingénierie britannique Arup a signalé en janvier 2024 à la police de Hong Kong une fraude de 200 millions de dollars de Hong Kong, soit environ 25,6 millions de dollars américains, selon [CNN](#). Un employé de la finance avait d'abord reçu un message ressemblant à du phishing, émanant du bureau britannique, qui demandait une transaction secrète. Ses doutes ont cédé après une visioconférence où le directeur financier et d'autres collègues apparaissaient, tous recréés par deepfake. Quinze virements ont suivi. Arup a précisé qu'aucun de ses systèmes internes n'avait été compromis : l'attaque a porté sur la confiance accordée à des visages et des voix familiers.

Ce cas illustre un point central pour la suite : une visioconférence ne constitue plus une preuve d'identité.

3. Anatomie d'une attaque

Une attaque par faux ordre de virement suit une séquence reconnaissable. La [CNIL](#) décrit trois temps : reconnaissance, usurpation, hameçonnage ciblé. La [fiche réflexe de Cybermalveillance.gouv.fr](#) précise que l'attaque est menée par téléphone, par email, ou par les deux, parfois après le piratage de la messagerie de la personne imitée.

1. **Reconnaissance.** L'attaquant collecte des informations publiques : organigramme, clients, fournisseurs, déplacements, réseaux sociaux, communiqués de presse. Pour un dirigeant exposé, ces informations abondent.

2. **Usurpation.** Il enregistre un nom de domaine proche de celui de l'organisation (typosquatting) ou prend la main sur une vraie boîte mail. Avec quelques minutes d'enregistrement audio public, une voix peut être clonée.
3. **Prise de contact.** Le message vise la personne qui peut agir : assistante, comptable, responsable administratif. Il se présente comme urgent et confidentiel.
4. **Isolement.** La demande interdit d'en parler : le dirigeant est "en réunion", "en déplacement", "injoignable". La consigne de discrétion coupe les vérifications.
5. **Pression et validation.** Un appel, un second email ou une visioconférence deepfake donne un aspect de réalité à la demande.
6. **Exécution.** Le virement part, souvent vers un compte à l'étranger, puis les fonds sont dispersés rapidement.

Trois variantes à connaître

La fiche de [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) distingue trois scénarios.

Variante	Mécanisme	Personne visée
Fraude au président	Faux ordre attribué à un dirigeant, présenté comme urgent et confidentiel	Assistante, comptabilité
Changement de RIB fournisseur	Un faux fournisseur communique de nouvelles coordonnées bancaires	Comptabilité, assistante en charge des règlements
Faux salarié	Un faux collaborateur demande de verser son salaire sur un autre compte	RH, paie

L'assistante privée est exposée aux deux premières, parfois aux trois lorsqu'elle gère la paie du personnel de maison. Elle traite des factures d'artisans, de prestataires, de gestionnaires de patrimoine, et un changement de coordonnées bancaires y paraît banal.

Pourquoi la proximité avec le dirigeant aggrave le risque

Les attaquants préparent leurs approches avec des détails que seul un véritable proche connaît, ce que confirme l'enquête Deloitte relayée plus haut. Une assistante connaît la plupart de ces détails, et elle est donc aussi la personne la plus difficile à tromper si elle dispose d'une procédure de contrôle claire. Le risque se concentre là où la relation de confiance remplace la procédure.

4. Cadre réglementaire et obligations

Un faux ordre de virement réussi est d'abord un préjudice financier. Il peut aussi devenir un incident de données personnelles, dès lors que des informations sur des personnes ont été divulguées, modifiées ou rendues accessibles à un tiers, par exemple après le piratage d'une messagerie.

Les violations de données

Selon la [CNIL](#), une violation de données est un incident de sécurité qui compromet la confidentialité, l'intégrité ou la disponibilité de données personnelles, qu'il soit malveillant ou accidentel. Trois obligations en découlent pour le responsable de traitement :

- notifier la CNIL dans un délai maximal de 72 heures lorsque la violation présente un risque pour les droits et libertés des personnes ;
- informer les personnes concernées lorsque le risque est élevé ;
- consigner toute violation dans un registre interne, même lorsqu'aucune notification n'est requise.

La CNIL précise sur sa page consacrée à la fraude au président qu'elle ne peut pas accorder de dommages et intérêts à l'entreprise victime, et que la plainte pénale relève de la police ou de la gendarmerie.

Pour l'assistante, la conséquence pratique est le réflexe de signalement : plus l'incident est remonté tôt à la personne qui décide, plus le délai de 72 heures reste tenable. Dans un foyer ou un family office, la notion de responsable de traitement mérite d'être clarifiée par un conseil juridique : l'étude ne tranche pas ce point.

Le programme de travail 2026 de la CNIL

Le [programme 2026 d'accompagnement des professionnels](#) est indicatif et peut évoluer.

Quatre chantiers concernent directement le poste :

1. Un projet de recommandation, soumis à consultation, sur la sécurisation des échanges de données personnelles par email et messagerie.
2. Des clarifications sur les outils de transcription et d'analyse automatique de la voix, à partir de cas d'usage comme la visioconférence.
3. Des recommandations sur l'IA au travail, avec les droits des salariés et les risques de biais.
4. Un travail sur les difficultés pratiques liées aux demandes d'accès des salariés à leurs données.

La CNIL cite aussi la hausse des fuites de données à grande échelle et la transposition prochaine de la directive européenne NIS 2, qui renforce les obligations de cybersécurité de certaines entités. Le champ exact de NIS 2 n'est pas détaillé dans la source consultée : les structures privées de petite taille ne doivent pas en conclure qu'elles sont concernées ou exclues sans vérification.

Ce que la réglementation change pour l'usage de l'IA par l'assistante

Les assistantes utilisent de plus en plus des outils de résumé de réunions et de rédaction. Quand un outil enregistre une réunion ou transcrit une voix, des données personnelles sont traitées, et celles d'un dirigeant ou d'une famille comptent parmi les plus sensibles. Le programme CNIL annonce des précisions pour ces outils. En attendant, la prudence consiste à obtenir l'accord explicite du dirigeant et des participants avant tout enregistrement, et à connaître l'hébergeur et les conditions de réutilisation des données de l'outil utilisé.

5. Spécificités de l'assistanat privé

Cette partie relie les sources aux conditions d'exercice de l'assistanat privé haut de gamme. Il s'agit d'une analyse de l'Observatoire. Aucune des sources consultées ne mesure la fraude dans les foyers fortunés ou les family offices.

Un environnement à forte valeur d'information

Le [11e baromètre AFFO x EY](#) (juin 2026) représente 928 familles. Près de la moitié des family offices interrogés gèrent plus de 500 millions d'euros d'actifs, et un tiers dépasse le milliard. Leurs priorités : la transmission entre générations (72 %), la fiscalité (58 %), la géopolitique (43 %), la gouvernance familiale (38 %), le numérique et les technologies émergentes (33 %). Ces sujets génèrent des échanges sensibles et des mouvements de fonds importants entre notaires, banques, conseils et fondations.

Un fraudeur y trouve une cible de choix : des montants élevés, des interlocuteurs multiples qui ne se connaissent pas tous entre eux, et des demandes de virement exceptionnelles qui semblent normales dans un contexte de transmission ou d'investissement.

L'absence de filet institutionnel

Dans une grande entreprise, une équipe informatique, un service comptable et un dispositif de double validation encadrent l'assistante. Dans un foyer ou une structure patrimoniale de petite taille, la situation est différente : l'assistante est parfois

l'interlocutrice unique pour les paiements courants, les prestataires et la logistique. Quand elle est seule, la procédure de validation dépend d'elle et du dirigeant ou de la famille.

Facteur	En entreprise structurée	En assistantat privé (analyse)
Validation des paiements	Circuit comptable et double signature	Souvent une personne et le dirigeant
Support informatique	Équipe dédiée	Prestataire externe ou outils personnels
Information exposée	Organigramme, communiqués	Agenda, déplacements, famille, patrimoine
Appareils utilisés	Parc géré	Mélange de matériel professionnel et personnel
Rapport au dirigeant	Hierarchique	Très personnel, forte confiance

La confiance, ressource et vulnérabilité

La relation de confiance est la raison d'être du métier. Elle donne à l'assistante un rôle de filtre précieux : elle détecte souvent qu'un message "ne ressemble pas" au dirigeant. Cette intuition devient un atout de sécurité lorsqu'elle s'appuie sur une règle explicite, par exemple "toute demande de virement inhabituelle fait l'objet d'un rappel sur un numéro connu". Sans règle, la même confiance expose l'assistante à un message qui imite assez bien le ton du dirigeant.

La pression est aussi sociale. Refuser ou retarder une demande "du patron" demande une légitimité. La procédure écrite et validée par le dirigeant fournit cette légitimité : l'assistante applique une règle que le dirigeant a lui-même établie.

6. Bonnes pratiques et procédures

Les recommandations ci-dessous reprennent les préconisations de [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr), de la [CNIL](https://www.cnil.fr) et de l'enquête Deloitte, et les adaptent au contexte de l'assistantat privé (adaptations signalées par la mention "transposition").

Cinq règles de base

- 1. Rappeler sur un canal connu.** Avant toute action financière ou transmission d'information sensible, appeler le dirigeant sur un numéro déjà enregistré, jamais celui indiqué dans le message reçu. La CNIL recommande de confirmer les paiements et

changements de coordonnées par téléphone ou en personne, avec des contacts déjà connus.

2. **Valider à deux, sans exception.** Cybermalveillance.gouv.fr demande une validation hiérarchique pour tout virement inattendu et tout changement de coordonnées bancaires. Transposition : dans une structure sans comptabilité, la seconde validation peut venir d'un conseiller de confiance ou d'un second membre de la famille.
3. **Traiter l'urgence comme un signal.** L'urgence, la confidentialité et l'isolement sont les trois leviers de la manipulation. Une demande qui cumule les trois déclenche la procédure de vérification, quelle que soit la source apparente.
4. **Contrôler les identités en visioconférence.** Après le cas Arup, une image et une voix familières ne suffisent plus. Transposition : convenir avec le dirigeant d'un mot de vérification ou d'une question connue des seuls intéressés, et faire confirmer par un second canal toute demande financière formulée pendant un appel.
5. **Protéger les comptes.** Mots de passe forts et uniques, double authentification sur la messagerie. La fiche réflexe insiste sur ce point, car la prise de contrôle d'une boîte mail permet de produire des demandes parfaitement crédibles.

Réduire l'information disponible

Cybermalveillance.gouv.fr recommande de limiter les informations publiques qui révèlent quels collaborateurs peuvent autoriser des virements ou modifier des coordonnées bancaires. Transposition : l'agenda, les déplacements, les noms des proches et des prestataires gagnent à rester hors des réseaux sociaux professionnels, y compris ceux de l'assistante. Un profil LinkedIn qui indique précisément pour qui elle travaille et ce qu'elle gère alimente la phase de reconnaissance.

Si l'incident survient

La fiche réflexe décrit la marche à suivre. Elle s'applique à tout poste concerné par les paiements.

1. Identifier tous les virements concernés, réalisés, en attente ou programmés, et prévenir la direction.
2. Si le virement n'est pas parti, le suspendre immédiatement.
3. S'il est parti, contacter la banque au plus vite pour demander le rappel des fonds.
4. Conserver les preuves : numéros de téléphone, messages, ordres de virement, factures.
5. Si la messagerie est compromise, changer le mot de passe sans attendre.
6. Déposer plainte auprès de la police ou de la gendarmerie, en parallèle des démarches bancaires.

Le point clé est la rapidité. Chaque heure compte pour le rappel de fonds, d'autant que les virements instantanés se généralisent.

L'entraînement par simulation

L'enquête Deloitte recommande des simulations internes pour tester les réflexes du personnel, des détecteurs de deepfakes pour ceux qui en ont les moyens, et l'implication de la gestion des risques au-delà du service informatique. Transposition : un exercice annuel de dix minutes avec le dirigeant, au cours duquel un faux message est envoyé puis la procédure rejouée, installe le réflexe sans dramatiser.

7. Implications pour la formation et la profession

La sécurité de l'information relève d'un ensemble de compétences que les recruteurs ne lisent pas toujours sur un CV. France Travail, dans son analyse des [attentes des recruteurs en 2026](#), relaie une étude Cornerstone OnDemand (2025) selon laquelle l'usage pratique de l'IA est devenu la compétence la plus demandée au monde, en hausse de 245 % sur un an.

Le Forum économique mondial (2025) place l'adaptabilité et la résilience parmi les trois compétences les plus recherchées. Une assistante qui maîtrise l'IA et en connaît les risques répond aux deux attentes.

Compétences à développer pour les assistantes modernes

Compétence	Contenu
Reconnaissance des manipulations	Signaux d'urgence, d'isolement, de pression ; variantes de fraude
Application d'une procédure de validation	Rappel sur canal connu, double validation
Hygiène numérique	Mots de passe, double authentification, gestion des appareils
Gestion des données personnelles	Notion de violation, signalement, registre
Usage maîtrisé de l'IA	Outils de transcription, résumé, confidentialité des données soumises
Communication de crise	Alerter vite, préserver les preuves, informer sans panique

Un enjeu de reconnaissance

La fonction de sécurité que remplit l'assistante est rarement formalisée dans la fiche de poste. Documenter ces pratiques (procédure validée, exercice annuel, registre des incidents) transforme une vigilance individuelle en savoir-faire reconnaissable, ce qui sert la négociation du périmètre et de la rémunération. France Travail conseille d'ailleurs de présenter des résultats concrets et mesurables plutôt que des qualités affirmées : une procédure mise en place et testée entre dans cette catégorie.

Sources et références

- Banque de France, [Rapport de l'Observatoire de la sécurité des moyens de paiement 2025](#).
- Cybermalveillance.gouv.fr, [Fiche réflexe : faux ordres de virement](#).
- CNIL, [Le faux ordre de virement international ou "fraude au président"](#).
- CNIL, [Les violations de données personnelles](#).
- CNIL, [Accompagnement des professionnels : le programme de travail de la CNIL pour 2026](#).
- Le Monde Informatique, [Les deepfakes utilisés pour siphonner les entreprises](#), 10 octobre 2024 (enquête Deloitte, mai 2024).
- CNN, [Arup revealed as victim of \\$25 million deepfake scam](#), 16 mai 2024.
- AFFO et EY, [11e baromètre des family offices](#), juin 2026.
- France Travail, [Comprendre les attentes des recruteurs en 2026](#), 24 avril 2026.