TRIBUNES

L'Europe face aux identités fabriquées : la menace invisible du recrutement à distance. Par Bruno Durand

Publié le 13/03/2026

Avec la généralisation du travail à distance en Europe, les services RH ne gèrent plus seulement les talents : ils doivent désormais naviguer dans un environnement où le recrutement devient une surface d'attaque à part entière. Des candidats soigneusement construits pour paraître crédibles et irréprochables, parfois soutenus par des organisations criminelles ou des acteurs étatiques, utilisent aujourd'hui l'anonymat numérique, l'IA générative et des identités synthétiques pour infiltrer les entreprises. L'objectif varie selon les groupes : soutirer de l'argent, accéder à des environnements sensibles, ou contourner les sanctions internationales via des emplois obtenus illégitimement.

Le recrutement détourné par l'IA

Ce phénomène s'est amplifié à mesure que les **outils d'IA se sont banalisés**. L'élaboration de CV impeccables, de lettres de motivation calibrées ou de photos de profil artificielles est devenue accessible à tous. Certains **fraudeurs** vont jusqu'à bâtir de faux écosystèmes professionnels : adresses e-mail multiples, profils LinkedIn cohérents, entreprises fictives servant de références croisées ou réseaux de candidatures opérés en série. Dans cet environnement, l'entretien vidéo reste souvent la seule confrontation avec la réalité, mais même celui-ci peut être contourné. Certains candidats avancent des excuses techniques pour **éviter la caméra**, jonglent entre arrière-plans artificiels ou affichent une maîtrise approximative du contexte local, malgré leur prétendue présence en Europe.

Des candidats qui accumulent des comportements inhabituels

Les **incohérences** ne se limitent pas à la présentation. Dans plusieurs cas **recensés par des entreprises européennes**, des candidats ont insisté pour accélérer les démarches, **esquiver les vérifications d'identité** ou imposer l'usage d'un ordinateur personnel plutôt que du matériel professionnel doté de solutions de sécurité. D'autres ont multiplié les changements d'adresse de livraison ou de coordonnées bancaires, cherchant à brouiller les traces ou à contourner les processus internes. Aucun de ces comportements n'est, isolément, la preuve d'une **fraude**. Mais leur accumulation révèle souvent une tentative d'infiltration structurée.

Un exemple européen illustre bien cette tendance. En 2023, une société technologique basée à Düsseldorf a découvert qu'un développeur recruté pour un poste totalement à distance utilisait en réalité les identifiants empruntés de plusieurs personnes. L'employé, qui prétendait vivre en Allemagne depuis plusieurs années, évitait systématiquement la caméra, invoquant des **problèmes de confidentialité**. Son CV, remarquable à première vue, contenait un enchaînement d'expériences crédibles, mais difficilement vérifiables. Ce n'est que lorsque l'entreprise a tenté d'envoyer un équipement professionnel à son adresse qu'elle a constaté que celle-ci correspondait à un immeuble de bureaux inoccupé. L'enquête interne a révélé que la personne se connectait depuis un pays tiers sous sanctions et redistribuait même une partie de son travail à un petit groupe de sous-traitants non déclarés. L'affaire aurait pu permettre à un acteur externe d'accéder à des données sensibles sur les systèmes logiciels de l'entreprise si celle-ci n'avait pas détecté les irrégularités à temps.

Les équipes RH, pilier de la cybersécurité en entreprise

Ces situations rappellent à quel point les **équipes RH occupent désormais une position stratégique**. Elles ne sont pas seulement responsables de l'adéquation poste-profil : elles constituent la **première barrière de sécurité d'une entreprise**. Sans devenir experts en cybersécurité, les recruteurs doivent désormais intégrer une vigilance nouvelle, fondée sur l'observation de la cohérence globale d'un candidat : sa manière de se présenter, l'alignement entre ses documents, son discours, son environnement et la capacité à vérifier, par des moyens officiels ou indépendants, l'**authenticité de son parcours**.

La **protection des organisations** passe ainsi par la **rigueur** plutôt que par la méfiance. Des processus standardisés, appliqués de manière uniforme, offrent une défense redoutablement efficace. Ce n'est pas la recherche du moindre faux pas qui permet d'**identifier les menaces**, mais une méthode solide, constante, qui évite les exceptions et garantit que chaque candidature transite par les mêmes filtres. Dans un monde où les identités numériques peuvent être fabriquées en quelques heures, la **cohérence** devient la **meilleure alliée des RH** européennes.

À propos de Bruno Durand