



FEBEA

FÉDÉRATION DES
ENTREPRISES DE LA BEAUTÉ

RISQUES NUMÉRIQUES :

Enjeux et perspectives
pour l'industrie française
de la beauté

FEBEA
137 rue de l'Université - 75007 PARIS
Tél. 01 56 69 67 89
www.febea.fr
@leLabdeClaire

Risques numériques :

Enjeux et perspectives
pour l'industrie française
de la beauté



Executive summary

Le secteur français de la cosmétique constitue un fleuron économique de premier plan constituant l'incarnation d'un savoir-faire historique, d'une exigence rigoureuse et d'une relation de confiance indispensable entre nos marques et les consommateurs. Deuxième contributeur à la balance commerciale nationale, notre secteur d'activité s'appuie sur un écosystème territorial puissant qui génère un chiffre d'affaires global de 35,6 milliards d'euros, capte 15 % du marché mondial et exporte près de deux tiers de sa production à l'international, représentant 22,4 milliards d'euros injectés dans l'économie nationale. C'est précisément cette immense valeur immatérielle et financière, caractérisée par une visibilité mondiale et une forte désirabilité, qui fait aujourd'hui de notre secteur une cible hautement stratégique et prioritaire pour les réseaux malveillants.

Face à ce prestige, la fraude numérique s'est muée en une menace systémique et hautement industrialisée, dont les méthodes s'alignent sur les standards de la criminalité transnationale organisée. Les acteurs de la cosmétique font désormais face à un état de siège permanent caractérisé par l'augmentation de sites miroirs, de campagnes de phishing par intelligence artificielle, de détournements réputationnels et de fraudes au président. Cette criminalité organisée opère sous le modèle du Crime-as-a-Service, créant une asymétrie structurelle et capacitaire déloyale : **alors que les réseaux criminels automatisent des attaques de masse à un coût marginal proche de zéro, les entreprises opèrent sous une exigence de défaillance zéro** pour protéger l'intégrité de leur chaîne de valeur, exposant collaborateurs et consommateurs à des préjudices financiers et des risques sanitaires majeurs.

Afin d'objectiver l'ampleur de ce phénomène, la

Fédération des Entreprises de la Beauté (FEBEA) a mené au premier semestre 2026 une étude hybride. Ce travail s'est structuré autour de trois piliers complémentaires : une revue approfondie de la littérature criminologique internationale, un volet quantitatif administré auprès de nos adhérents durant le premier trimestre 2026, et une campagne d'entretiens avec ces derniers. L'enquête révèle le constat que **100 % des répondants ont subi au moins un incident de fraude numérique majeur au cours de l'année écoulée**, confirmant que l'exposition au risque

cybercriminel est totale, continue et indépendante de la taille de l'entreprise ou de son chiffre d'affaires.

Le principal enseignement opérationnel de cette étude réside dans la mise en évidence de **l'inertie des plateformes numériques, qui complique toute résolution de crise**. Alors qu'un

incident cyber interne sur le propre périmètre d'une entreprise est généralement circonscrit en moins de 24 heures, le délai de résolution explose et atteint 4 à plus de 8 semaines dès que l'action requiert l'intervention d'une plateforme tierce (réseaux sociaux, hébergeurs, places de marché). Ce délai de carence offre aux fraudeurs une fenêtre d'impunité pour maximiser leurs profits aux dépens de la réputation de nos marques. De plus, les recours juridiques traditionnels, comme la procédure UDRP (Uniform Domain Name Dispute Resolution Policy) pour récupérer un nom de domaine usurpé, sont obsolètes, trop lents et prohibitifs, tandis que les dispositifs étatiques de signalement existants restent inadaptés aux besoins professionnels.

Face à cette carence publique, les entreprises en sont réduites à une privatisation contrainte de leur défense.

Forte de ce constat, la FEBEA demande aux pouvoirs publics d'articuler leur action autour de sept leviers majeurs :

1. **Moderniser la gouvernance des noms de domaine** en imposant un blocage automatisé des usurpations de marques à la source par les registrars et en dotant l'ARCOM (Autorité de régulation de la communication audiovisuelle et numérique) ou l'ANSSI (Agence nationale de la sécurité des systèmes d'information) de leviers administratifs de blocage d'urgence sans recours judiciaire préalable ;
2. **Élever la lutte contre la contrefaçon cosmétique au rang d'enjeu de santé publique** afin d'aligner les moyens de la police judiciaire sur ceux des autorités sanitaires face aux risques toxicologiques majeurs ;
3. **Responsabiliser et contraindre réellement les plateformes numériques** (y compris le marché de la seconde main) en généralisant les mesures d'injonctions dynamiques et en exigeant des barrières techniques proactives (traçabilité, scan de codes unitaires) ;
4. **Créer un fonds de soutien ou crédit d'impôt cyber dédié aux TPE, PME et ETI** pour briser le « plafond de verre » sécuritaire en finançant des audits, de l'équipement proactif et des formations face à l'ingénierie sociale ;

5. **Instaurer un guichet unique de signalement professionnel B2B (Business to Business)** sur le modèle éprouvé du NASC australien pour centraliser et industrialiser la riposte ;
6. **Accélérer la réponse pénale et la rendre réellement dissuasive** en augmentant les moyens d'instruction judiciaire et en raccourcissant drastiquement les délais de traitement des plaintes au pénal ;
7. **Défendre la compétitivité et la souveraineté économique des entreprises françaises au niveau européen**, en influençant activement le futur Digital Fairness Act afin d'y intégrer la co-responsabilité juridique des plateformes et une obligation stricte de retrait des contenus illicites sous 24 heures.

La protection de l'excellence ne peut plus reposer sur les seules épaules des entreprises. Elle appelle une mobilisation partagée, entre les acteurs économiques, les pouvoirs publics et les intermédiaires numériques. Tel est l'objet de ce rapport, qui invite l'ensemble des parties prenantes, et notamment les autorités publiques, à se mobiliser pour valoriser et défendre l'industrie française des cosmétiques. Il s'agit de préserver un patrimoine et un savoir-faire historique face aux défis actuels. ■

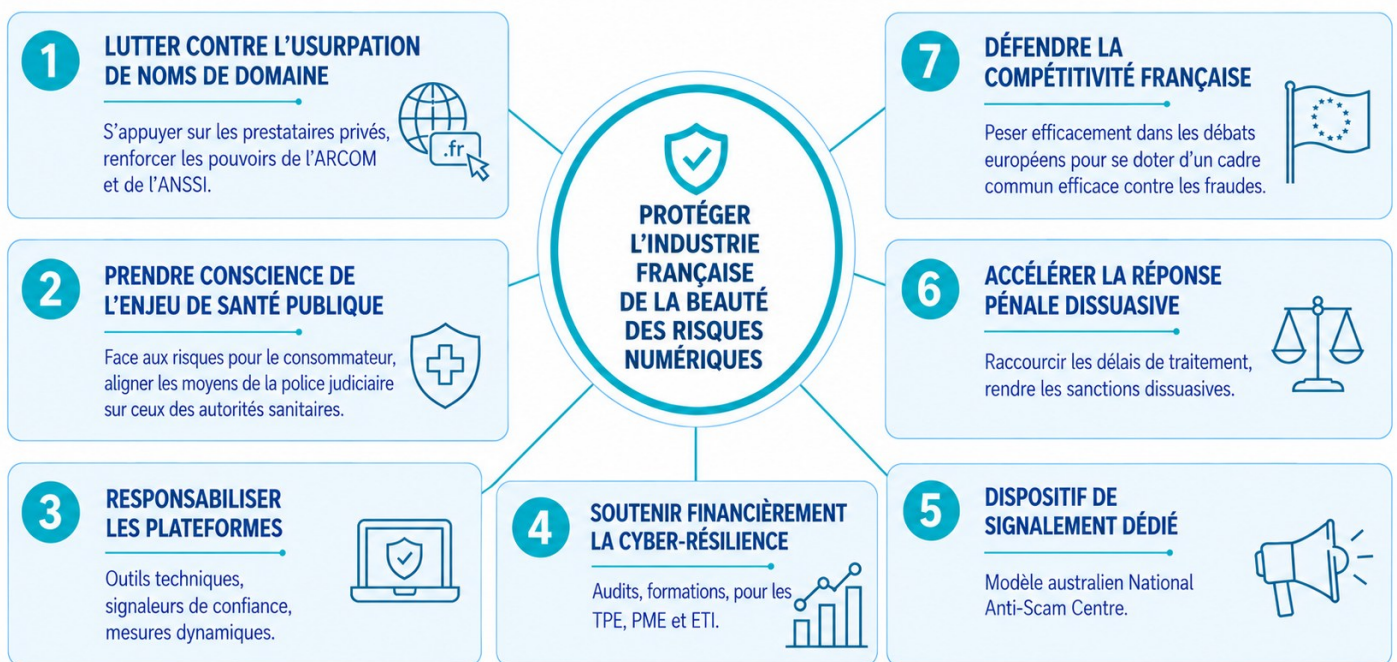


Table des matières

Executive summary	4
Table des matières	6
Partie 1 :	
Menaces numériques sur le secteur de la cosmétique, de quoi parle-t-on ?	8
La fraude numérique, nouveau visage de la criminalité organisée	8
La beauté, chaîne de valeur propice à la génération de revenus frauduleux	9
Les différents visages de la fraude numérique	10
Les collaborateurs, victimes du détournement des messageries chiffrées	10
Un cyberspace sans gardien qui dupe à grande échelle, aux risques et périls du consommateur	11
La réputation attaquée des acteurs français, au détriment de toute une économie	14
La fraude organisationnelle touche directement la trésorerie des entreprises	14
La fraude numérique touche tous les acteurs de la cosmétique	15
Une menace aux moyens augmentés, qui cible toutes tailles d'entreprises	16
La moindre maturité numérique de certains acteurs les transforme en cibles immédiates	16
Partie 2 :	
Anatomie des forces en présence	18
Le coût infini de la protection	18
Une réponse interne mobilisant des ressources considérables	18
Des stratégies externes aux résultats incertains	18
Un coût de réaction permanent et imprévisible	19
Un « plafond de verre » sécuritaire pour les PME	19
Le coût déloyal de l'inaction des plateformes	20
Une inertie qui transforme les entreprises en « otages »	20
L'absence de « gardien capable », une faille systémique	20
Le coût subi du renoncement des autorités	21

Table des matières

Partie 3 :

Quelles solutions pour protéger l'excellence française ? 25

Lutter efficacement contre l'usurpation de noms de domaine 25

Élever la lutte contre la contrefaçon des produits cosmétiques au rang d'enjeu de santé publique 25

Responsabiliser et contraindre réellement les plateformes 26

Soutenir financièrement la cyber-résilience des entreprises les plus vulnérables 27

Créer un dispositif de signalement dédié aux entreprises 27

Accélérer la réponse pénale et la rendre réellement dissuasive 28

Défendre la compétitivité des entreprises françaises 28

Annexes : pour aller plus loin 29

La FEBEA et la cosmétique française : poids stratégique d'un leader mondial 29

Cadre méthodologique 30

Bibliographie 30

Crédits photos 31

Menaces numériques sur le secteur de la cosmétique, de quoi parle-t-on ?

La fraude numérique, nouveau visage de la criminalité organisée

La fraude numérique à laquelle sont confrontées les entreprises de la cosmétique a cessé d'être un sujet marginal pour se transformer en une menace systémique.

Son architecture et son niveau de sophistication s'alignent sur les standards de la criminalité organisée internationale (ONUDC, Office des Nations Unies contre la drogue et le crime, 2024). Cette réalité microéconomique s'inscrit dans le prolongement direct des constats macro-criminels de référence tels que dressés par Europol et l'ONUDC. La pression cyber sur les entreprises est devenue systémique : entre violations de données quotidiennes et cyberattaques constantes (usurpation, contrefaçon, fraude au virement bancaire).

Ce constat se traduit par **une évolution des méthodes frauduleuses, désormais portées par des outils numériques.**

Les incidents observés par les entreprises (prolifération de sites miroirs, campagnes d'hameçonnage de pointe et usurpations massives d'identités numériques) illustrent le modèle de

Le Crime-as-a-Service (CaaS) désigne un modèle économique souterrain dans lequel des cybercriminels développent et monétisent des outils, des ressources et des prestations techniques "clés en main" au profit d'autres fraudeurs (campagnes d'hameçonnage automatisées, lots de données personnelles volées, réseaux de blanchiment ou encore des logiciels complexes d'usurpation d'identité). Ce modèle d'externalisation abaisse radicalement les barrières à l'entrée de la cybercriminalité : il permet à des délinquants disposant de faibles compétences informatiques de déployer des attaques hautement sophistiquées et à très grande échelle.

Crime-as-a-Service, documenté par les instances telles Europol.

Le développement du cyberspace a fourni aux réseaux criminels les leviers pour industrialiser leurs processus délictueux, engendrant une asymétrie structurelle et capacitaire entre les fraudeurs et les cibles :

- D'un côté, grâce notamment à l'IA, les réseaux malveillants automatisent des **attaques de masse à un coût marginal proche de zéro**. Cette industrialisation leur permet une stratégie d'essais-erreurs illimitée, où l'échec n'a aucune conséquence financière, tandis qu'un seul succès suffit à rentabiliser l'opération ;
- De l'autre, les entreprises opèrent sous une **pression de défaillance zéro**, la sécurisation de l'ensemble de leur chaîne de valeur devenant un enjeu stratégique, là où le réseau criminel n'a besoin d'exploiter qu'une seule et unique faille (qu'elle soit logicielle ou humaine) pour infiltrer l'écosystème.

Cette vulnérabilité garantit aux attaquants un retour sur investissement élevé, faisant de la fraude un moteur économique.

Dès lors, et conformément aux analyses de l'ONUDC, **les utilisations des outils numériques à des fins malveillantes (fraude, cyberattaque, vente de produits contrefaisants, etc.) ont cessé d'être des épiphénomènes isolés pour s'imposer comme des piliers de financement de la criminalité transnationale organisée**. Face à cette puissance capacitaire, les entreprises sont contraintes de s'engager dans une « course à l'armement » coûteuse, imposant une mobilisation massive de ressources telles que l'investissement dans des outils technologiques de protection et de riposte, le recours à des services externes de notice & takedown ou encore la souscription d'assurances cyber.

A ces opportunités exponentielles créées par le numérique s'ajoute la fragmentation géogra-

phique des réseaux criminels.

Les savoir-faire de ces entreprises s'articulent autour de différents axes de développement :

- Une production et une ingénierie technologique délocalisées dans des zones à faible régulation, exploitant les failles de gouvernance de certains États ;
- Un appui sur des chaînes où des usines en principe licites (notamment en Asie) ayant des activités illicites en parallèle ;
- Une distribution mondialisée s'appuyant sur la puissance des plateformes de commerce électronique légales, diluant la traçabilité des flux. Certains contrefacteurs vont jusqu'à créer de fausses histoires de marque et à gonfler les prix pour tromper la vigilance des consommateurs par un positionnement haut de gamme.

Les organisations cybercriminelles opèrent selon des modèles structuraux agiles, calqués point par point sur l'architecture des entreprises légitimes. Ce mimétisme permet aux fraudeurs de se constituer un redoutable « vernis de légalité », conçu avec la double ambition de tromper la vigilance des consommateurs, employés, fournisseurs ou autres partenaires commerciaux des entreprises, voire d'abuser les fournisseurs de services de paiement.

Les mesures d'authentification des entreprises et des banques sont de plus en plus souvent contournées par l'interception des codes de sécurité. Europol documente que les fraudeurs ciblent désormais les méthodes de paiement modernes (cartes « tokenisées » et portefeuilles électroniques) en interceptant les mots de passe à usage unique envoyés par les établissements bancaires pour autoriser les transferts. La mondialisation des échanges et les progrès technologiques de la FinTech ont créé de nouveaux canaux permettant de déplacer l'argent volé à

une vitesse vertigineuse d'un pays à l'autre.

La beauté, chaîne de valeur propice à la génération de revenus frauduleux

L'univers de la beauté, fondé sur la relation de confiance entre une marque et ses clients, constitue un terrain de prédilection pour la cybercriminalité. Le croisement des préjudices recensés par la FEBEA avec les données d'Europol confirme que la cosmétique française n'est plus une cible fortuite, mais une priorité stratégique pour les réseaux criminels, soumise à une menace désormais constante.

La criminologie environnementale utilise l'acronyme

VIVA (Valeur, Inertie, Visibilité, Accès) pour définir ce qui fait d'un objet ou d'une marque une cible idéale dans le cyberspace : sa Valeur, son Inertie (facilité avec laquelle on peut la déplacer ou la cloner en ligne), sa Visibilité et l'Accès. Les marques cosmé-



tiques, très prisées et visibles mondialement, cochent toutes ces cases.

La cosmétique cumule plusieurs facteurs qui en font une cible privilégiée :

- **La valeur et la nature des marques.** Les marques de cosmétique ont développé le plus souvent une valeur émotionnelle et aspirationnelle. Cette notoriété attire les fraudeurs : un nom de domaine proche de celui d'une marque connue (cybersquatting, typosquatting) capte immédiatement du trafic et de la confiance. Les marges sont immédiatement élevées, que ce soit sur des prises de commandes malhonnêtes qui ne donneront lieu à aucune livraison ou sur la vente de produits contrefaisants dont le coût de fabrication réel est faible pour un

investissement initial limité, le tout aux risques et périls du consommateur.

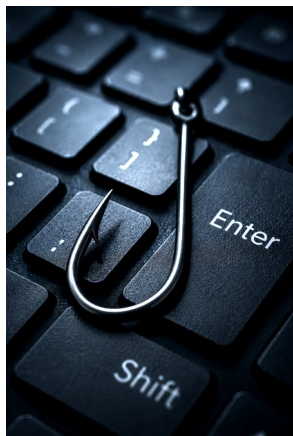
- **Le comportement d'achat.** La recherche de « bonnes affaires » sur des produits habituellement haut de gamme rend les consommateurs plus enclins à cliquer sur une offre suspecte et moins méfiants face à un prix anormalement bas.
- **La valeur des données clients.** Au-delà de la contrefaçon, les entreprises du secteur détiennent des bases de données importantes : informations de paiement, mais aussi données sensibles liées à la peau, à la santé ou aux préférences personnelles, utiles pour le marketing comme pour les cybercriminels. Cela en fait des cibles intéressantes pour le vol de données, le rançongiciel ou la fraude.
- **Les caractéristiques des produits eux-mêmes.** Les cosmétiques sont relativement faciles à imiter visuellement (packaging, flacon, étiquette), le consommateur ne pouvant vérifier la composition du produit au moment de l'achat, qui plus est online. Le rythme soutenu de lancements, d'éditions limitées et de collaborations crée en permanence de nouvelles références à copier que les vendeurs frauduleux exploitent.
- **La numérisation massive de la distribution et du marketing.** Le secteur s'appuie fortement sur le e-commerce, les marketplaces, le social commerce et les influenceurs. Cette présence en ligne diffuse multiplie les surfaces d'attaque : faux sites marchands, faux comptes sur les réseaux sociaux, publicités frauduleuses, places de marché difficiles à contrôler. Il est facile d'usurper l'identité visuelle d'une marque et de toucher directement des millions de consommateurs.
- **Un environnement international et fragmenté.** Chaînes d'approvisionnement mondialisées, multiplicité des extensions de noms de domaine par pays, déclinaisons de marques sur de nombreux marchés : tout cela complique la surveillance et l'action juridique, et offre aux fraudeurs des zones grises où opérer.

Pour les fraudeurs, le secteur de la cosmétique est devenu un levier de rentabilité industrielle : ils ne se contentent plus de copier des produits, ils parasitent le prestige du savoir-faire français et détournent la confiance des consommateurs pour financer leurs activités à l'échelle internationale.

Loin de l'image d'Epinal du contrefacteur isolé, les entreprises de la filière cosmétique font face à des fraudeurs expérimentés. Cette mutation exige un changement de paradigme : la protection périmétrique des organisations est devenue insuffisante. Elle doit s'intégrer dans une stratégie de défense collective, soutenue par une coopération avec les instances de régulation nationales et internationales.

Les différents visages de la fraude numérique

La fraude organisationnelle a franchi un cap de professionnalisation, dont l'agilité et l'efficacité opérationnelle s'alignent sur les standards des entreprises légitimes. Les nouveaux visages de la fraude numérique s'appuient sur une ingénierie, technique et psychologique, d'une grande finesse.



Elle incarne le pilier de la « Capacité », concept cardinal du Diamant de la Fraude (WOLFE, HERMANSON) théorisé par la littérature criminologique.

Dans la pratique, les assaillants délaissent la confrontation directe avec les infrastructures de cybersécurité pour privilégier un contournement stratégique : ils déplacent le vecteur d'attaque vers les failles humaines, en investissant des canaux de communication hybrides qui échappent, par nature, à la vigilance des entreprises.

Les collaborateurs, victimes du détournement des messageries chiffrées

Le détournement des messageries chiffrées privées pour perpétrer des fraudes au président, via l'usurpation d'identité des dirigeants, s'est érigé en standard opératoire et constitue une tendance alarmante.

Une ETI témoigne ainsi que ces tentatives sont devenues « récurrentes » et surviennent désormais « plusieurs fois par mois ». **La mise en scène est d'une précision chirurgicale** : grâce aux bases de données que constituent les réseaux sociaux professionnels, les criminels créent de faux comptes reprenant le nom et la photographie exacte d'un membre du top management (Président, Directeur général, Directeur financier, etc.). Ils contactent ensuite les collaborateurs dans leur sphère privée, créant un effet d'urgence (voire de proximité) redoutable, leur demandant le plus souvent de réaliser une transaction en urgence, parfois avec leurs moyens de paiement personnels. En s'introduisant sur le smartphone du collaborateur, le fraudeur contourne l'intégralité de la chaîne de sécurité de l'organisation.

Les entreprises expriment une véritable exaspération face à cet angle mort sur lequel elles n'ont « aucun contrôle, aucune maîtrise de ces comptes et pas de levier d'action », contrairement aux outils internes classiques (e-mails, messageries d'entreprise) qu'ils peuvent tenter de monitorer et filtrer. Cette vulnérabilité est accentuée par des pratiques de gouvernance interne, un répondant alerte sur le danger (silencieux) des groupes informels entre collègues créés sur ces messageries privées, sur lesquels « des informations sont partagées sur des espaces où restent parfois des collaborateurs ayant quitté la société », transformant ces discussions en failles de sécurité béantes.

Face à ce risque, plusieurs acteurs du panel affirment avec fermeté que l'utilisation des messageries chiffrées privées pour des flux professionnels « devrait être bannie » ou, à minima, « proscrire » pour toute communication sensible.

Ce type de fraude est désormais considéré comme un enjeu de gouvernance, imposant une implication parfois au plus haut niveau de l'entreprise. Comme souligné par un membre de la fédération : « Malheureusement sans sponsoring fort de la Direction Générale, cet usage perdure... Pour l'instant ces fraudes n'ont pas abouti, mais jusqu'à quand ? ». Cette interrogation traduit la difficulté ressentie face à l'asymétrie de moyens : la parade technologique habituelle (filtres, antivirus, blocage d'Internet Protocol) est inopérante sur les messageries chiffrées, laissant les entreprises désarmées face aux fraudes opérées via ces flux privés.

Faute de pouvoir neutraliser la menace en amont, la seule riposte actuelle des organisations repose sur l'« information pédagogique » (ex. par des sessions e-learning) et des campagnes régulières de « sensibilisation ». L'ultime rempart des entreprises repose sur la seule vigilance individuelle du collaborateur (sollicitée régulièrement selon son poste) pour ne pas céder à la pression d'un faux dirigeant agissant derrière son écran.



Un cyberspace sans gardien qui dupe à grande échelle, aux risques et périls du consommateur

La dématérialisation du commerce a transformé l'écosystème de la vente de produits contrefaisants. Les échanges commerciaux, démultipliés par le numérique et les réseaux sociaux (en raison de la fonctionnalité publicitaire et des ventes associées) s'imposent comme un vecteur de vulnérabilité. 100% des entreprises ayant participé à notre étude se disent concernées par la

vente de produits contrefaisants et pointent les canaux numériques (marketplaces, réseaux sociaux, sites pirates de e-commerce, messageries chiffrées privées) comme tout premier vecteur de menace.

Le cyberspace, marqué par l'absence de « gardiens » capables de réguler et de filtrer efficacement les flux, s'est mué en un accélérateur et multiplicateur des formes de fraudes. Les entreprises subissent une exposition continue à une multitude d'attaques parasitaires : usurpation de marque, typosquatting et cybersquatting, vente de produits contrefaisants prolifèrent sur les réseaux sociaux, les moteurs de recherche et les places de marché (marketplaces).

Cette menace subit une évolution constante : le pillage ne se limite plus à la seule reproduction du produit physique, il englobe désormais la captation de la propriété intellectuelle numérique. **Les fraudeurs s'approprient les actifs immatériels des marques (visuels officiels, logos, et photographies protégées par le droit d'auteur) dans une démarche de crédibilité.** Cette agilité est démultipliée par l'émergence de réseaux experts dans le clonage intégral d'identités visuelles. En reproduisant sites et applications sans faire figurer le nom de la marque dans l'URL, ces fraudeurs parviennent à neutraliser les outils de veille traditionnels, rendant la détection de ces officines quasi impossible par les moyens classiques.

Les témoignages recueillis révèlent une sophistication croissante des structures productives. Les membres de la FEBEA soulignent la professionnalisation des réseaux asiatiques (particulièrement en Chine qui s'appuient désormais sur un écosystème d'usurpation multidimensionnel) :

- **Le recours croissant au marché gris s'accompagne de l'édition de factures d'achat factices.** D'un réalisme saisissant, ces documents sont conçus pour tromper la vigilance des grossistes et valider l'authenticité des stocks auprès des plateformes de vente ;
- **Pour neutraliser les réflexes de méfiance, les**

contrefacteurs abandonnent les "prix cassés" au profit de prix alignés sur les standards du marché légitime. Ce positionnement est soutenu par un storytelling de marque sophistiqué, visant à asseoir une illusion de prestige et de crédibilité ;

- **Cette chaîne d'abus de confiance aboutit sur les marketplaces où les volumes s'écoulent.** Une stratégie de contournement plus fine émerge via le drop shipping : des acteurs utilisent des interfaces de vente basées dans l'UE tout en stockant les produits dans des hubs logistiques stratégiques, comme au Luxembourg. En utilisant les systèmes postaux nationaux pour une expédition rapide, ils masquent l'origine réelle des flux, rendant la fraude difficile à détecter et à avérer pour les autorités. Le manque de proactivité des plateformes est largement dénoncé par les entreprises de la filière, les plus grandes d'entre elles (comme par exemple Meta côté réseaux sociaux, ou Shein côté marketplaces) s'abritant derrière l'absence d'obligations de diligence. Ces acteurs maintiennent une perméabilité de leurs systèmes qui permet l'écoulement massif de produits frauduleux, malgré des signalements répétés et documentés par les entreprises.
- **La problématique s'étend désormais aux plateformes de seconde main.** Profitant de l'essor de l'économie circulaire, des particuliers (ou des réseaux se faisant passer pour tels) vendent des produits frauduleux en bénéficiant de la complaisance involontaire de ces acteurs. De nombreuses plateformes se limitent à une modération réactive basée sur les signalements. Pourtant, des solutions proactives existent : une proposition visant à exiger des photographies de toutes les faces du produit pour faciliter l'identification des contrefaçons a été soumise par un membre de la FEBEA, mais refusée par la plateforme. Qu'il s'agisse de contrefaçon ou de réseaux d'exportation parallèle, l'identification des fraudes reste complexe, même avec l'appui de prestataires spécialisés. La difficulté réside notamment dans l'usage de visuels

100% des entreprises sondées se disent concernées par la vente de produits contrefaisants et pointent les canaux numériques comme tout premier vecteur de menace

officiels qui masquent la nature réelle des produits effectivement vendus. Dorénavant, le recours aux photographies ne suffit plus à distinguer avec certitude les produits authentiques des contrefaçons.

- **Ce tableau des menaces ne serait pas complet sans mentionner le phénomène massif des « dupes »**, ces produits alternatifs low-cost imitant les références iconiques des marques, dont la prolifération est dopée par la viralité des réseaux sociaux (comme TikTok ou Instagram) et l'essor du social commerce. Si le dupe joue sur les frontières de la légalité en copiant l'esthétique, le flaconnage ou l'univers olfactif d'une signature de marque sans en reproduire le logo, sa banalisation modifie profondément le comportement d'achat en érigeant la recherche de la « bonne affaire » en vertu de consommation.

Pour la FEBEA, cette tendance représente un danger double. D'une part, elle fragilise le respect de la propriété intellectuelle en habituant le consommateur à tolérer l'imitation et le parasitisme du savoir-faire. D'autre part, et de manière plus pernicieuse, elle sert de couverture idéale aux réseaux criminels : **sous couvert de promouvoir un « dupe » inoffensif sur les plateformes, les fraudeurs orientent en réalité les consommateurs vers des canaux d'achat non contrôlés** (places de marché opaques, plateformes de seconde main, messageries chiffrées privées). Le consommateur pense acheter une alternative maligne alors qu'il acquiert une contrefaçon chimique formulée sans aucun contrôle dermatologique ou toxicologique, transformant un phénomène de mode numérique en un risque sanitaire majeur.

Certaines grandes plateformes mettent en avant la dichotomie territoriale qui rend le retrait des contenus illégaux complexe, le traitement étant différencié selon les droits de Propriété Intellectuelle locaux (ex. entre les filiales européennes et américaines d'une même place de marché). Une des entreprises interrogées témoigne : après avoir signalé à une grande plateforme les comptes de vendeurs non européens proposant des produits contrefaisants, certains produits sont restés visibles sur la version américaine de la plateforme sans être directement commandables depuis l'Europe. Une mention avait cependant été ajoutée, suggérant à l'utilisateur d'utiliser un VPN (Virtual Private Network) pour

finaliser son achat. Cette situation met en évidence un problème de "contournement géographique assisté" : alors que le droit de la propriété intellectuelle est strictement territorial, l'infrastructure technique de la plateforme, reste globale. En facilitant l'accès à des stocks illicites via des outils de masquage d'IP, les interfaces numériques vident de leur substance les actions de retrait (notice & takedown).



À cette impuissance technologique s'ajoute une **barrière financière majeure** dès lors que le litige se déporte en Asie. En Chine, par exemple, la défense d'un dessin ou modèle exige l'obtention d'un « evaluation report » au coût unitaire avoisinant les 3 000 euros. Face à des plateformes comme Temu, Shein, Alibaba, Shopee ou encore Pinduoduo capables d'héberger simultanément plus de 100 modèles contrefaisants, l'investissement requis pour protéger une seule gamme de produits devient rapidement prohibitif, et n'est, dans tous les cas, pas accessible aux acteurs de taille modeste.

La réputation attaquée des acteurs français, au détriment de toute une économie

Au-delà de la vente de produits illicites, les entreprises s'inquiètent d'un détournement des plateformes à des fins de déstabilisation réputationnelle.

Plusieurs membres du panel rapportent des campagnes de désinformation orchestrées visant à éroder la confiance des consommateurs. L'un des cas documentés illustre une stratégie sophistiquée : l'utilisation d'influenceurs et de contenus générés par IA pour diffuser des narratifs fallacieux. Ces messages cherchent à discréditer le savoir-faire français en affirmant, preuves visuelles générées par IA à l'appui, que les produits haut-de-gamme seraient en réalité issus de chaînes de production à bas coûts situées en Asie. Des signalements récents confirment l'usage de deepfakes ou de visuels ultraréalistes simulant des ateliers de fabrication clandestins. **L'objectif des fraudeurs est double : détourner la clientèle des circuits officiels et fragiliser l'image d'authenticité qui constitue le socle de la valeur des maisons françaises.** En instillant le doute sur l'origine réelle des produits, ces réseaux criminels s'attaquent à l'intangible que constitue le capital de marque. Ce type de fraude pose de grandes difficultés dans la mesure où elle impacte la perception des consommateurs. Une fraude, même localisée dans un secteur spécifique, peut entacher l'image de marque dans son intégralité. Bien que les entreprises s'efforcent de se préparer à ces risques, toutes ne sont pas familières avec ce type d'attaque, ni avec la vélocité des algorithmes. Ces derniers peuvent en effet transformer un incident isolé en un phénomène de désinformation massif en un temps record.

De ce fait, cela est susceptible de provoquer une désorganisation et un stress non négligeable des équipes responsables en interne ou des prestataires, avec une « surexposition » via des sollicitations multiples et un besoin urgent de résolution. Une réaction est nécessaire pour réduire la visibilité des publications, tout en gérant, pour la majorité des cas, parallèlement les remontées internes (communication, dirigeants, décisionnaires, autres...). **Les entreprises victimes se heurtent à l'inertie de certains réseaux sociaux refusant de supprimer les contenus frauduleux ou refusant de mettre en place des mesures**

proactives visant à empêcher la réapparition de contenus frauduleux après une suppression.

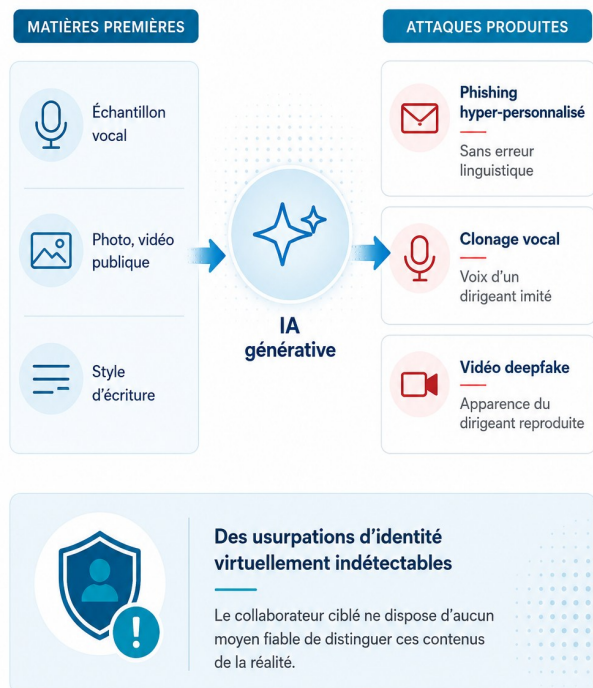
Elles doivent naviguer dans un environnement complexe où toute action de retrait est entravée par les plateformes, ces dernières invoquant systématiquement la "liberté d'expression" pour justifier leur refus de collaborer. Le manque de proactivité des plateformes, et de TikTok, Instagram, YouTube, Snapchat en particulier, favorise l'exploitation de mots-clés stratégiques (keywords) par les fraudeurs. Ces termes de recherche, qui devraient déclencher des mécanismes de modération, sont utilisés de manière récurrente car les systèmes de contrôle des plateformes se limitent à une réaction a posteriori plutôt qu'à une anticipation des tendances. Aussi, **face à la désinformation, les entreprises font face à un choix difficile de l'angle de la communication : choisir de communiquer sur la désinformation au risque de contribuer à la diffusion massive d'informations falsifiées ou à contrario faire le choix de ne pas alimenter la rumeur.** Dans cette situation encore, l'entreprise se retrouve isolée.

La fraude organisationnelle touche directement la trésorerie des entreprises

Enfin, les entreprises membres de la FEBEA font face à une prolifération de la fraude organisationnelle.

Comme le souligne le rapport de l'ONUDC, l'escroquerie aux faux ordres de virement (FOVI, ou Business Email Compromise) s'est érigée au rang des menaces transnationales organisées les plus prévalentes à l'échelle mondiale. **Ces cyberattaques capitalisent sur les vulnérabilités humaines et sur la manipulation psychologique.** Les fraudes au président (cf. point sur les messageries chiffrées privées), les compromissions de messageries professionnelles et les falsifications de coordonnées bancaires constituent de véritables entraves au fonctionnement opérationnel des organisations. Le ciblage a atteint un niveau permettant de cartographier les organigrammes, analyser les flux de communication et identifier les partenaires stratégiques pour frapper aux moments de vulnérabilité maximale, tels que les pics d'activité ou les veilles de fermeture de week-end.

L'intelligence artificielle, multiplicateur de menace



L'intelligence artificielle démultiplie cette menace en permettant de générer des campagnes de phishing hyper-personnalisées, totalement exemptes d'erreurs linguistiques. Grâce au clonage vocal et aux deepfakes, les attaquants rendent désormais leurs usurpations d'identité virtuellement indétectables.

La menace dépasse le cadre du simple virement frauduleux pour s'attaquer au patrimoine immatériel de l'entreprise.

La DGSi (Direction générale de la Sécurité intérieure) alerte d'ailleurs sur trois scénarios types d'approches malveillantes envers les entreprises :

- **L'investissement factice** : une structure en difficulté est approchée par un faux cabinet de conseil pour obtenir des données techniques sensibles sous couvert d'un projet d'investissement juridiquement inexistant.
- **L'usurpation de notoriété** : un chercheur ou un expert est contacté par l'entourage fictif d'une célébrité, promettant un financement massif en échange de "taxes" ou de données de recherche.
- **Le faux collègue** : par l'infiltration numérique sur les réseaux sociaux, l'attaquant crée un profil de salarié pour instaurer une fausse relation de confiance et extraire des infor-

mations stratégiques (calendriers de développement, secrets de fabrication).

Cette logique dépasse désormais le strict périmètre de l'entreprise pour irradier l'intégralité de sa chaîne de valeur. À titre d'illustration, une PME de notre panel rapporte le cas critique d'un client dont la messagerie compromise a permis à des tiers de s'immiscer silencieusement dans une transaction. Suivant un mode opératoire identique, une TPE explique qu'un de ses collaborateurs a reçu un virus émanant d'un compte client pourtant authentique, mais préalablement piraté. En interceptant les échanges pour substituer leurs coordonnées bancaires lors de la facturation, les fraudeurs ont transformé une relation commerciale de confiance en une perte financière sèche. Ce constat démontre que la sécurité d'une organisation est désormais indissociable du niveau de vigilance de ses partenaires.

Comme le souligne la DGSi, le caractère dématérialisé de ces échanges tend à réduire la vigilance des collaborateurs. Pourtant, ce qui semble être une approche isolée fait souvent partie d'une campagne de captation de données coordonnée visant l'ensemble de la structure.

Cette porosité des relations tiers impose aux entreprises une vigilance de chaque instant. **Les services financiers sont désormais contraints de systématiser des procédures de double vérification humaine à chaque demande de modification de coordonnées bancaires.**

La fraude numérique touche tous les acteurs de la cosmétique

La multiplicité des risques cyber affectant le secteur de la cosmétique se conjugue à une extension de la menace à l'ensemble des acteurs du secteur. Les données de terrain confirment que l'exposition à la fraude est indépendante de la taille de l'entreprise, de son chiffre d'affaires ou de la notoriété de ses marques.

Une menace aux moyens augmentés, qui cible toutes tailles d'entreprises

Contrairement aux préjugés tenaces, les PME et ETI se retrouvent autant que les grands groupes en première ligne face au risque cybercriminel. Les données du panel révèlent que ces structures subissent une pression opérationnelle tout aussi soutenue que celle de leurs homologues de plus grande taille. 100 % des répondants, qu'il s'agisse de PME ou de grands groupes, déclarent avoir subi au moins un incident de fraude numérique majeur (usurpation de marque, cyberattaque ou fraude au président) au cours de l'année écoulée.

Ces 24 derniers mois, la quasi-totalité des entreprises interrogées rapporte une accélération brutale des attaques, qualifiée de "forte à très forte". Cette récurrence impose aux entreprises un état de « siège permanent » : une large majorité des membres interrogés déclare désormais subir des tentatives d'escroquerie ou des atteintes à leur propriété intellectuelle de manière "continue et récurrente".

Cette pression se traduit par une surcharge opérationnelle critique, avec plusieurs incidents majeurs traités simultanément chaque semaine (plusieurs répondants font état de 5 à plus de 10 incidents majeurs traités simultanément). Un dirigeant témoigne faire face à « plusieurs tenta-

100% des entreprises sondées déclarent avoir subi au moins un incident majeur de fraude numérique au cours de l'année

tives par mois » impliquant des usurpations d'identité au moyen de faux comptes sur des messageries chiffrées privées. Cette menace s'inscrit dans une temporalité longue : selon le rapport de l'Association of Certified Fraud Examiners (ACFE), un schéma de fraude type s'installe au cœur d'une organisation et perdure en moyenne 12 mois avant même d'être détecté par l'entreprise.

Par ailleurs, ne se limitant pas à une simple augmentation des volumes, la fraude s'accompagne d'une généralisation des cibles. Si les grands groupes demeurent des cibles historiques et permanentes en raison de leur surface financière, les données collectées révèlent **une extension des attaques vers les PME et les ETI.**

Les répondants issus de ces structures (de 10 à 249 collaborateurs) rapportent une multiplication d'incidents critiques (fraude au président, compromission de messageries professionnelles et usurpation de marque). Potentiellement perçus par les réseaux criminels comme les "maillons faibles" de la chaîne de valeur (par rapport à une asymétrie de ressources), ces entreprises se heurtent à des obstacles capacitaires. Leurs dirigeants identifient le « coût », la « complexité technique » et le « manque de compétences internes » comme les freins majeurs à l'optimisation de leur cyber-résilience.

Selon l'ACFE la fraude ampute en moyenne 5 % des revenus annuels des organisations. Pour les entreprises cotées, le coût de protection devient prohibitif, cumulant investissements matériels, recours contraint à des prestataires de notice & takedown privés et polices d'assurance cyber aux franchises exorbitantes.

La moindre maturité numérique de certains acteurs les transforme en cibles immédiates

La fréquence soutenue des attaques, combinée à leur sophistication technologique, démontre que les mécanismes de défense périmétriques traditionnels ont atteint leurs limites opérationnelles face à une menace qui s'est enracinée dans l'environnement opérationnel des entreprises.



Cette vulnérabilité systémique s'explique par plusieurs dynamiques majeures :

- **Les réseaux criminels perçoivent souvent les PME comme des entités disposant de protocoles de cybersécurité moins matures et de capacités de riposte juridique restreintes.** Elles constituent des cibles de choix, tant pour des attaques d'opportunité que pour des tentatives d'intrusion latérale destinées à compromettre la chaîne d'approvisionnement globale.

À l'échelle mondiale, le rapport de l'Association of Certified Fraud Examiners (ACFE, 2024) confirme cette vulnérabilité structurelle : les entreprises de moins de 100 salariés subissent une perte médiane de 141 000 dollars par incident (le deuxième niveau de perte le plus élevé, toutes tailles d'organisations confondues). Cette exposition s'explique par le fait que leur taille limite la séparation des tâches et le déploiement de contrôles internes robustes. Les retours d'expériences des PME concernant leur dispositif de riposte corroborent ce diagnostic macroéconomique.

- **Si la menace cyber est désormais indifférenciée, la fragilité initiale des petites structures agit comme un amplificateur de risque.** Cette vulnérabilité structurelle est d'autant plus critique que la dématérialisation transforme chaque faille locale en un point d'entrée systémique, générant ainsi des impacts en cascade.
- **En amont de la chaîne, les grossistes et distributeurs professionnels (B2B) sont les premières cibles d'une ingénierie documentaire sophistiquée.**

Trompés par des facturations factices et des réseaux de distribution gris aux tarifs calqués sur le marché, ils intègrent involontairement des stocks illicites dans leurs circuits officiels. Cette contamination de la chaîne d'approvisionnement se propage jusqu'en aval, atteignant le consommateur final (B2C) exposé à des produits non conformes. En parasitant les réseaux de l'intérieur, la fraude transforme des acteurs économiques légitimes en vecteurs involontaires de contrefaçon, multipliant ainsi les risques de responsabilité des entreprises. Ce détournement de la légalité s'étend jusqu'aux professions réglementées : Europol dénonce le rôle prépondérant joué par des professionnels légitimes (comptables, avocats, courtiers) qui utilisent des structures commerciales légales pour aider les réseaux criminels à blanchir les produits de la fraude.

- **Les attaques cyber touchent également les grands groupes, notamment dans le contexte de fusions et acquisitions.** Lors de ces opérations, l'intégration de systèmes de IT hétérogènes, reposant sur des niveaux de maturité et des politiques de sécurité différents selon les entités, peut créer des failles significatives. L'absence d'harmonisation des dispositifs de protection et des standards de cybersécurité au sein du groupe nouvellement constitué accroît les surfaces d'attaque et facilite l'exploitation de vulnérabilités par des acteurs malveillants. ■

La fraude numérique n'épargne plus aucune typologie d'entreprise. L'idée parfois persistante selon laquelle les acteurs de taille modeste bénéficient d'une quelconque « protection » à la fraude du fait de leur moindre notoriété ne correspond plus à la réalité du terrain.

Face à ce constat, il convient d'opérer un changement de posture : la protection face aux cybermenaces ne peut plus reposer sur la seule responsabilité ou les seuls investissements des entreprises. L'intervention des pouvoirs publics s'impose désormais comme une condition pour protéger l'ensemble du tissu industriel cosmétique.

Anatomie des forces en présence

Le coût infini de la protection

Malgré une prise de conscience réelle et des investissements croissants, les entreprises se heurtent à une asymétrie de moyens face aux réseaux criminels. Une majorité écrasante des entreprises interrogées, quelle que soit leur taille, juge leur niveau de protection actuel comme seulement « partiellement suffisant ».

Une réponse interne mobilisant des ressources considérables

En interne, les entreprises s'appuient le plus souvent sur des compétences internalisées au sein de départements dédiés (Directions des Systèmes d'Information et Directions de la Sécurité). Ces mobilisations sont coûteuses, mais l'enjeu est critique : l'absence de dispositifs préventifs robustes condamne les organisations à une réaction tardive.

S'il est complexe d'évaluer précisément l'impact financier de la fraude, la facture globale en matière de cybersécurité s'avère colossale. Les témoignages recueillis confirment qu'une vigilance constante est indispensable pour ne pas être distancé par l'ingéniosité des fraudeurs : cette exigence impose une actualisation permanente des compétences du personnel, des systèmes techniques et des outils de surveillance.

Bien que certains préjudices soient difficilement chiffrables, les primes d'assurance représentent à elles seules des investissements majeurs, auxquels s'ajoutent des franchises élevées. La pression financière est d'autant plus forte pour les sociétés cotées, dont les investisseurs exigent des garanties de sécurité drastiques, contrairement aux structures plus modestes. Au-delà de ces frais, l'effort financier global est conséquent : il englobe aussi bien l'acquisition de matériel (hardware) et le recours à des prestataires spécialisés que les pertes potentielles liées à l'indisponibilité des systèmes.

Des stratégies externes aux résultats incertains

À ces dispositifs internes s'ajoute la nécessité de stratégies externes lorsque la fraude se produit sur une plateforme numérique.

Les titulaires de droits (en particulier les grandes entreprises) ont généralement recours à des réseaux de prestataires chargés de mettre en œuvre des procédures de notice & takedown de manière systématique, même si d'importantes difficultés subsistent. Les entreprises identifient notamment :

- **L'hétérogénéité des formulaires de signalement** et leur complexité parfois excessive, même si un travail de simplification est engagé à cet égard ;
- **L'absence, à ce jour, d'octroi du statut de « signaleur de confiance »** (trusted flaggers) au bénéfice des titulaires de droits. Un travail conséquent a été mené, et demeure en cours, afin que de tels signaleurs de confiance soient désignés en France ;
- **La multiplication de contre-notifications** répétitives et systémiques, le plus souvent infondées, qui entraînent une perte de temps considérable (notamment sur certaines plateformes chinoises) ;
- **La dichotomie territoriale liée aux zones d'accessibilité des plateformes**, qui entraîne des traitements différenciés selon les droits de propriété intellectuelle applicables localement, et complexifie le retrait des contenus illicites.



Parallèlement à ces actions menées en ligne, les entreprises sont parfois contraintes d'aller plus loin en lançant des enquêtes de terrain pour identifier elles-mêmes l'origine de la fraude. L'un des répondants témoigne de ce type de recherche, conduite en Chine en 2025 afin d'identifier les auteurs d'une campagne de désinformation : coûteuse et complexe, cette enquête a mobilisé les équipes juridiques internes durant trois à quatre mois. Les investigations ont révélé une stratégie sophistiquée : exploitant les failles des législations étrangères, les contrefacteurs s'assuraient que leurs campagnes ne soient pas visibles en Chine afin d'échapper aux contrôles locaux.

Europol détaille d'ailleurs l'usage systématique d'outils de chiffrement (réseaux VPN - Virtual Private Network, bullet-proof hosts) par les fraudeurs pour dissimuler leur identité et sécuriser leurs communications, leur garantissant une impunité quasi totale face aux polices locales. Il est apparu que les auteurs de ces publications agissaient comme des intermédiaires rémunérés, sans lien hiérarchique direct avec les usines incriminées. Malgré cette opacité, le caractère exhaustif des recherches a permis de transmettre des informations stratégiques aux autorités locales. Bénéficiant d'un contexte politique favorable, marqué par la volonté ferme du gouvernement chinois de lutter contre la contrefaçon pour protéger l'image du pays, cette action a débouché sur des raids contre les sites de production et sur des poursuites judiciaires.

Si une décision de justice est encore attendue, la vigilance reste de mise face à des méthodes de fraude en constante évolution. Le coût de telles opérations demeure néanmoins hors de portée d'une grande partie du panel, révélant une « sécurité à deux vitesses » où l'efficacité de la riposte dépend directement de la capacité financière à soutenir des procédures juridiques au long cours et de l'alignement tactique avec les priorités politiques locales.

Un coût de réaction permanent et imprévisible

Cet obstacle financier, couplé à la sophistication croissante des offensives, rend l'identification

des auteurs parfois impossible. Ces impasses techniques génèrent un profond sentiment d'impuissance, exacerbé par la découverte souvent tardive de la fraude. Ce caractère asynchrone est illustré par le témoignage d'un répondant dont l'entreprise n'a découvert l'usurpation d'identité de ses salariés qu'au moment où les criminels tentaient d'immatriculer des sociétés à leur insu. Un tel préjudice outrepassa la sphère de l'entreprise : il expose le personnel à des risques financiers personnels (souscription de crédits frauduleux, endettement, dégradation de la capacité d'emprunt). La compromission peut également s'étendre aux données des

consommateurs, faisant basculer la fraude d'une simple atteinte à l'image de marque vers une crise de gestion bien plus globale.

Le coût des failles se révèle ainsi plus lourd et plus protéiforme qu'il n'y paraît. Au-delà du préjudice financier direct, l'entreprise doit parfois gérer les dégâts à l'échelle mondiale. Lorsqu'elle fait le choix d'indemniser les victimes (ce qui est majoritairement le cas pour préserver son image), son service client doit authentifier chaque dossier avant de procéder aux remboursements. Cet effort de réparation génère un effet d'aubaine pernicieux, favorisant des fraudes collatérales où des tiers opportunistes simulent des préjudices. Entre le temps humain consacré aux vérifications et l'émergence de fraudes « à la carte » sur différents marchés, la gestion de l'après-crise démontre que l'absence de défense préventive condamne l'organisation à un coût de réaction permanent et imprévisible.

Un « plafond de verre » sécuritaire pour les PME

Enfin, les données de terrain révèlent une corrélation nette entre ce sentiment de vulnérabilité persistant et l'identification de deux freins majeurs : le coût financier et la complexité technique de la lutte antifraude.

Ce constat est particulièrement critique pour les PME, bloquées par un véritable « plafond de verre » sécuritaire. Les répondants issus de ces structures identifient un triptyque qui les empêche de se défendre efficacement : « Coût,

Manque de solutions adaptées aux PME,
Manque de compétences internes ».

PME & ETI : Le plafond de verre sécuritaire

Les structures de moins de 250 salariés se heurtent à un triptyque structurel qui les empêche de se défendre efficacement contre la fraude numérique.



NIVEAU DE PROTECTION INACCESSIBLE



Coûts multiples de la protection

Primes de cyber-assurance prohibitives, franchises élevées, prestataires de notice & takedown privés, outils techniques onéreux : la facture dépasse rapidement les capacités des petites structures.



Manque de solutions adaptées

Les outils de cybersécurité sont conçus pour les grands groupes. Les PME n'ont accès ni aux dispositifs publics calibrés pour leurs besoins, ni aux plateformes de signalement adaptées au B2B.



Manque de compétences internes

Absence de DSI ou de Direction Sécurité dédiée, impossibilité d'internaliser des expertises cyber rares et coûteuses. Les équipes manquent de temps et de formation face aux attaques.

Le coût déloyal de l'inaction des plateformes

Comme évoqué précédemment, l'environnement numérique actuel se caractérise par l'absence de « gardiens » capables de réguler les flux illicites. Les résultats de l'étude démontrent que les entreprises de la filière cosmétique sont devenues les « otages » des réseaux sociaux et des places de marché (marketplaces), dont le manque de réactivité paralyse toute tentative de résolution rapide des crises.

Une inertie qui transforme les entreprises en « otages »

Cette inertie est attestée par la corrélation des temps de résolution issus de l'enquête :

- Lorsqu'une entreprise subit une cyberattaque sur son propre périmètre (compromission de messagerie, tentative de fraude au président, attaque sur les serveurs), elle parvient généralement à circonscrire et résoudre l'incident dans un délai

court, de l'ordre de 1 à 24 heures ou de 1 à 7 jours ;

- À l'inverse, dès que la fraude s'externalise et nécessite l'intervention d'une plateforme tierce (pour faire retirer une fausse boutique, un produit contrefait ou un faux compte), le délai de résolution explose, atteignant fréquemment 4 à plus de 8 semaines. Ce délai de carence offre aux fraudeurs une fenêtre d'impunité et démontre que les entreprises ne peuvent s'en sortir seules face à ces intermédiaires numériques.

À cet égard, le rapport mondial 2024 de l'Association of Certified Fraud Examiners documente statistiquement la corrélation entre la durée de détection et de résolution d'une fraude et l'explosion de son coût financier.

L'ACFE démontre que la mise en place de contrôles proactifs permet de réduire la durée d'une fraude de 14 % à 50 %. Or, l'entreprise étant dépendante du bon vouloir de la plateforme pour agir à l'externe, cette inertie imposée annule ses propres capacités de contrôle et multiplie mathématiquement le préjudice financier et réputationnel subi.

L'absence de « gardien capable », une faille systémique

Pour comprendre la nature de cette faille systémique, il convient de s'appuyer sur la Théorie des activités routinières (COHEN & FELSON, 1979). Ce modèle criminologique fondamental postule qu'un délit se produit lorsque convergent, dans le temps et l'espace, trois éléments : un délinquant motivé, une cible appropriée (ici, la valeur des marques cosmétiques et l'argent de leurs clients) et, surtout, l'absence d'un gardien capable (absence of capable guardians).

Dans l'architecture de l'espace numérique, ce rôle de « gardien capable » aurait pu échoir naturellement aux plateformes (hébergeurs, réseaux sociaux, marketplaces). Or, ces acteurs ont institutionnellement failli à cette mission, en grande partie parce que la régulation des flux criminels ne relève pas de leurs prérogatives originelles.

La « complicité passive » de ces acteurs est directement pointée du doigt. Face à des campagnes d'escroquerie manifestes clonant l'identité visuelle des marques pour promouvoir de fausses « braderies », les entreprises

déplorent « l'absence d'action en amont » sur des plateformes comme Facebook. Les remon-
tées de terrain fustigent la posture de géants du
numérique (tels que Meta ou des marketplaces
comme Shein) qui s'abritent derrière l'absence
d'obligation légale de proactivité pour refuser
d'intervenir ou de bloquer préventivement des
comptes, même en présence de signalements
multiples portant sur des fraudes flagrantes et
identiques. **Les entreprises sont ainsi condam-
nées à une lutte chronophage et purement réac-
tive** (a posteriori). De surcroît, les actions de dé-
référencement massives (takedown) sont com-
plexifiées par le risque opérationnel de bloquer
les sites de distribution officiels et autorisés de la
marque (la fameuse « white list »).

Le coût subi du renoncement des autorités

Le constat des entreprises est unanime : face à
des menaces numérisées et mondialisées, l'ar-
senal juridique et institutionnel français et euro-
péen apparaît obsolète, inadapté, inégalement
appliqué ou lacunaire à certains égards. Ce dé-
calage structurel engendre une privatisation
contrainte de la justice et nourrit le calcul des
réseaux criminels, pour qui **le crime est devenu
économiquement rentable puisque pénalement
peu risqué**.

Ce calcul repose sur des fondements très clairs,
modélisés par la Théorie du choix rationnel
(BECKER, 1968) : le fraudeur effectue une ana-
lyse coût-bénéfice stricte avant de passer à
l'acte. L'arsenal judiciaire actuel
étant lent et inadapté, le "coût"
de l'acte (c'est-à-dire le risque
pénal encouru) est perçu
comme quasi nul, face à un
"bénéfice" (le profit financier)
élevé. L'impasse institutionnelle
actuelle rend donc la fraude
rationnelle et systémique.

Cette réalité est d'ailleurs confirmée par l'évolu-
tion de la criminologie : les modèles récents, à
l'image du Pentagone de la fraude (TUGAS,
2012), ont spécifiquement intégré les « in-
fluences réglementaires externes » (External Re-
gulatory Influences) comme une dimension ex-
plicative majeure. Cela prouve académique-
ment qu'un cadre légal inadapté est désormais
une cause directe et reconnue de l'explosion des

fraudes.

Ce constat d'échec, soulevé de manière una-
nime, s'articule autour de trois failles systé-
miques :

- **L'obsolescence et la lourdeur des recours tra-
ditionnels constituent une privation de la ri-
poste.** A titre d'exemple, les procédures lé-
gales classiques pour récupérer un nom de
domaine frauduleux (comme la procédure
UDRP) sont jugées beaucoup trop longues
et trop coûteuses par les entreprises. Spé-
cifiquement sur ce type de fraude, permet-
tant d'agir rapidement, la réactivité des ser-
vices de la DGCCRF (Direction générale de la
concurrence, de la consommation et de la
répression des fraudes) est indispensable. A
défaut, les entreprises sont contraintes
d'abandonner les recours officiels. Comme
le résume l'un des répondants : face à « une
hausse exponentielle des faux sites, nous
avons délaissé les procédures UDRP
(coûteuses et longues) au profit de ta-
akedown (via un prestataire dédié) ». Cette
privatisation contrainte de la justice, où les
entreprises doivent rémunérer des presta-
taires privés pour faire retirer des contenus
et espérer une certaine efficacité, illustre la
faillite du système de régulation public.
- **L'inadaptation des outils de signalement éta-
tiques et l'absence de coordination inter-
Etats** constituent des éléments qui ne per-
mettent pas aux entreprises de pouvoir agir
a posteriori de la détection de la fraude. Les
dispositifs actuels mis en place
par les pouvoirs publics s'avè-
rent inadaptés aux besoins
d'alerte massif et technique des
professionnels (B2B). Les re-
tours de terrain alertent préci-
sément sur ce point, soulignant
« les sites de signalement desti-
nés aux consommateurs ne
sont pas adaptés aux remontées par les en-
treprises » (à l'image des plateformes de la
DGCCRF). Les entreprises se retrouvent sans
interlocuteur étatique réactif face à des
fraudes à grande échelle. Cette impasse est,
comme précédemment mentionné,
exacerbée par la barrière de la territorialité :
dès lors qu'un réseau délictueux présente
des éléments transnationaux (par exemple
un auteur basé en Asie ciblant des consom-

Le crime est devenu
économiquement rentable
puisque pénalement peu
risqué

mateurs en France), aucune autorité ne se déclare compétente, créant un frein absolu au dépôt de plainte et plus largement aux suites susceptibles d'y être données.

- **Le traitement judiciaire de la fraude numérique décourage profondément les victimes.** Les entreprises font face à un enlèvement qui anéantit tout effet dissuasif pour les criminels. Le témoignage d'une PME du secteur est représentatif du sentiment d'abandon généralisé : celle-ci déplore qu'une « plainte de 2024 [ne soit] toujours pas instruite ». Cette paralysie de la chaîne pénale garantit aux fraudeurs une impunité de fait.

aux pouvoirs publics une refonte du traitement de la fraude s'articulant autour d'une « adaptation du cadre juridique », de l'application de « sanctions plus dissuasives », et d'une « meilleure coopération lors des signalements ».

Afin de mieux saisir les leviers et les lacunes du système actuel, le tableau ci-après dresse un **panorama des textes législatifs et réglementaires structurant la lutte contre la fraude numérique**.

Face à ces vulnérabilités persistantes, les entreprises expriment des attentes. **Elles réclament**

Panorama des textes législatifs et réglementaires structurant la lutte contre la fraude numérique

Niveau européen
Digital Services Act (DSA)

Ce règlement de 2022 vise à mettre en pratique le principe selon lequel ce qui est illégal hors ligne l'est aussi en ligne.

Le DSA régule les services numériques en imposant de nouvelles obligations aux plateformes (hébergeurs, réseaux sociaux, marketplaces) pour mieux lutter contre les contenus illicites, la contrefaçon et protéger les utilisateurs.

Les plateformes en ligne doivent :

- Faciliter le signalement et le retrait rapide des contenus illicites ;
- Coopérer avec des signaleurs de confiance et mieux tracer les vendeurs sur les marketplaces pour informer les consommateurs ;
- Assurer la transparence de leurs décisions de modération.

Les entreprises constatent que les effets du DSA sont à ce stade trop limités.

L'obtention de mesures de blocage de contenus nécessite encore bien souvent une action judiciaire préalable, longue et coûteuse.

La persistance factuelle de contenus contre-faisants sur les réseaux sociaux démontre que, malgré ses ambitions, le cadre réglementaire du DSA ne parvient pas encore à briser l'inertie opérationnelle des plateformes.

Niveau européen
Règlement Général sur la Protection des Données (RGPD)

Ce règlement de 2016 a instauré un régime de protection des données plus strict et harmonisé au sein de l'UE, avec des droits renforcés et une responsabilité accrue pour les organisations.

Le paquet omnibus "digital" (en cours de négociations dans les instances européennes) propose des modifications ciblées du RGPD, visant principalement à restreindre la définition des « données à caractère personnel », à clarifier le traitement lié à l'IA et à harmoniser certaines obligations quotidiennes en matière de conformité.

Le RGPD impose un cadre de conformité, son efficacité est circonscrite à la gestion des conséquences. Le règlement sanctionne la faille de sécurité une fois consommée, laissant les entreprises face à la complexité technique de la lutte antifraude en amont.

La Commission européenne et le Comité européen de la protection des données (CEPD) publieront en 2026 des lignes directrices communes sur l'articulation entre le règlement sur les marchés numériques (DMA) et le RGPD.

Tableau illustrant l'état de la législation à date et les enjeux qui y demeurent associés

Panorama des textes législatifs et réglementaires structurant la lutte contre la fraude numérique

Niveau européen

Directive NIS 2
(Network and Information Security 2) et transposition nationale en **Loi sur la cybersécurité**

Adoptée en 2022, la directive vise à renforcer le niveau global de cybersécurité des tissus économiques et administratifs des pays membres de l'UE.

Cette directive ne concerne pas l'ensemble des entreprises (critères d'application).

NIS2 impose un standard nécessaire pour la protection "interne" des entreprises, elle n'a pas vocation à assurer la protection des mail-lons extérieurs de la chaîne.

Considérant les caractéristiques des entreprises du panel et leurs retours, une entreprise peut être parfaitement en règle avec NIS2 tout en restant vulnérable à la fraude, attestant la nécessité d'aller plus loin.

Niveau européen

PSD3 (Payment Services Directive 3) et **PSR** (Payment Services Regulation)

Ce règlement (2023) et cette directive (2023) sur les services de paiement ont vocation à assurer entre autres la sécurité des paiements en ligne et la protection contre la fraude.

Un changement structurel significatif porté par ce règlement et cette directive devrait concerner l'extension de la responsabilité au PSP du bénéficiaire (l'institution recevant le paiement frauduleux) dans les cas de fraude APP (*Authorised Push Payment*). La responsabilité sera désormais partagée. Les révisions sont en attente de la position du Conseil en 1ère lecture.

Conjointement, PSD3 et PSR doivent instaurer une défense harmonisée à l'échelle européenne, capable de neutraliser la fraude par ingénierie sociale (comme la fraude au virement) en automatisant la vérification d'identité des bénéficiaires et en transférant une plus grande part de la responsabilité financière aux prestataires de paiement en cas de faille.

Si la fraude par ingénierie sociale continue de croître, c'est que l'arsenal juridique actuel n'est potentiellement pas en phase avec l'agilité des réseaux criminels.

Niveau européen

EU AI Act

Ce règlement sur l'IA (2024) fixe les règles de gouvernance, de conformité et de sécurité liées au déploiement de l'Intelligence Artificielle au sein de l'Union européenne.

Tous les systèmes d'IA considérés comme une menace manifeste pour la sécurité, les moyens de subsistance et les droits des personnes sont interdits. La législation sur l'IA interdit huit pratiques, dont la manipulation et la tromperie préjudiciables fondées sur l'IA, l'exploitation nocive des vulnérabilités fondée sur l'IA.

Les entreprises dénoncent l'utilisation massive de l'IA dans les fraudes qu'elles subissent (*deepfakes, faux sites générés de bout en bout, phishing automatisé*).

Considérant l'impact de ces pratiques, il semble exister un décalage, voire une inadaptation, entre le cadre actuel et la réalité des menaces.

France

Code de la consommation et **Code de commerce**

Ces codes permettent de caractériser la tromperie et de dénoncer des sites frauduleux ou des contrefaçons auprès de la DGCCRF pour diverses non-conformités (absence de mentions légales, fausses promotions, etc.).

Les entreprises du panel attestent que les plateformes de signalement de la DGCCRF sont structurellement pensées pour les consommateurs (B2C) et inadaptées aux besoins des entreprises (B2B). L'action pénale qui en découle est perçue comme trop faible ou inexistante.

Tableau illustrant l'état de la législation à date et les enjeux qui y demeurent associés

Ce tableau confronte les ambitions théoriques de chaque dispositif (national ou européen) à la réalité opérationnelle rapportée par les entreprises. Il met en lumière le décalage persistant entre l'arsenal juridique ambitieux sur le papier et l'agilité des réseaux criminels à laquelle sont confrontées les entreprises victimes.

Dans les faits, dès qu'une fraude présente des éléments transnationaux, les entreprises se retrouvent en difficulté quant à l'aide qui leur est proposée : aucune autorité ne se déclare compétente, les plaintes n'aboutissent pas et les organismes nationaux comme la DGCCRF sont perçus comme inadaptés pour traiter les plaintes des professionnels. À cette impuissance s'ajoute une exigence procédurale : les signalements auprès d'organismes imposent un investissement en temps difficilement soutenable pour les structures sinistrées. **Les nouveaux outils comme le DSA produisent des effets limités**, ils imposent (presque) systématiquement une action judiciaire préalable, longue et coûteuse, pour obtenir le moindre blocage.

Au-delà des enjeux de propriété intellectuelle (et des conséquences associables), **la contrefaçon de produits cosmétiques soulève un impératif de santé publique**. Contrairement aux produits authentiques soumis à des tests dermatologiques et toxicologiques, les produits contrefaisants et les dupes échappent à tout contrôle, exposant les consommateurs à des substances prohibées ou dangereuses (métaux lourds, agents irritants, impuretés microbiologiques). En théorie, la caractérisation du risque exigerait des analyses de laboratoire systématiques pour chaque saisie ; toutefois, le coût prohibitif de ces expertises constitue un frein majeur. Faute de moyens pour analyser chaque produit saisi, les entreprises ne peuvent évaluer la dangerosité réelle des flux, laissant planer un risque sanitaire majeur sur les consommateurs.

La contrefaçon fragilise les fondements économiques de la cosmétique française. Elle engendre un risque de perte d'activité, alimenté par l'érosion de la confiance des consommateurs et la saturation du marché par des produits illicites. Un client victime d'une arnaque

sans remboursement ne va pas immédiatement racheter un produit (imposant aux entreprises de gérer l'après fraudes parfois par le dédommagement).

En détournant le savoir-faire français, **cette concurrence déloyale dévalue l'investissement en innovation et menace l'employabilité d'un secteur pourtant moteur, fragilisant ainsi toute la chaîne de valeur, de la formulation à la distribution**.

Toutefois, une lueur d'évolution pourrait se dessiner sur le plan juridique. La décision attendue en Cour d'appel dans l'affaire Meta / Groupe Barrière¹ pourrait marquer un tournant décisif. **En remettant potentiellement en cause l'immunité relative du statut d'hébergeur, ce contentieux interroge la responsabilité des plateformes qui tirent un profit direct de flux publicitaires frauduleux**. Un tel basculement forcerait les géants du numérique à passer d'une réaction a posteriori à un devoir de vigilance structurel, imposant une détection proactive des réseaux de désorganisation avant que le préjudice ne devienne systémique.

L'intérêt principal de cet arrêt réside dans la consécration d'une approche particulièrement ambitieuse des injonctions judiciaires à l'encontre des très grandes plateformes en ligne. En confirmant l'obligation faite à Meta de mettre en œuvre, par tout moyen efficace, des mesures destinées à **prévenir la diffusion future de publicités contrefaisantes reproduisant les marques** du Groupe Barrière, la Cour d'appel de Paris dépasse la logique traditionnelle du retrait a posteriori des contenus illicites pour privilégier une logique de prévention.

Elle admet ainsi qu'une plateforme puisse être contrainte de prévenir, avant toute diffusion, la réapparition de contenus contrefaisant des marques, lorsque la mise en place d'un filtrage automatique est possible et que ce filtrage est ciblé et proportionné.

L'arrêt contribue en outre à renforcer l'efficacité des mécanismes de protection des droits de propriété intellectuelle dans l'environnement numérique. ■

¹ Le Groupe Barrière, acteur historique des casinos et de l'hôtellerie en France, s'est retrouvé victime d'une campagne publicitaire frauduleuse sur les plateformes de Meta (Facebook, Instagram, Messenger). Entre novembre 2023 et janvier 2024, des centaines de profils d'annonceurs ont diffusé quelques 2.400 publicités reproduisant sans autorisation les marques « Barrière » pour promouvoir des applications de jeux de casino en ligne, lesquels sont interdits en France. Ces publicités imitaient les codes visuels du groupe et utilisaient parfois des photos de devantures de casinos Barrière pour donner l'illusion d'un partenariat officiel. Face à la persistance de ces contenus malgré une plainte pénale, plusieurs signalements et une mise en demeure, le Groupe Barrière a saisi le juge des référés qui, par ordonnance sur requête du 11 janvier 2024, a ordonné à Meta de mettre en œuvre des mesures de filtrage. Meta a contesté cette ordonnance en référé-rétractation, sans succès. L'ordonnance du 24 avril 2024, confirmée en appel, a maintenu l'obligation de filtrage.

Quelles solutions pour protéger l'excellence française ?

Le cadre légal s'avère très insuffisant face à l'agilité des cybercriminels, augmenté par l'IA. Les délais judiciaires et administratifs découragent les entreprises victimes et nourrissent un sentiment d'impunité totale pour les fraudeurs.

En réponse à ces vulnérabilités systémiques, la FEBEA formule plusieurs recommandations concrètes.

Lutter efficacement contre l'usurpation de tout nom de domaine à des fins frauduleuses

Face à l'explosion des faux sites et des usurpations, les entreprises délaissent les recours légaux traditionnels. **La procédure officielle UDRP pour la récupération de noms de domaine est jugée beaucoup trop lente et coûteuse.** Les entreprises sont contraintes de se tourner vers des prestataires privés. Il existe une faille juridique où l'action n'intervient qu'a posteriori, sans accompagnement proactif d'autorités nationales compétentes telles que l'ARCOM (Autorité de régulation de la communication audiovisuelle et numérique) ou l'ANSSI (Agence nationale de la sécurité des systèmes d'information).

En matière d'usurpation de noms de domaine, **l'absence de solution centralisée et de coopération internationale coordonnée laisse le champ libre aux pratiques frauduleuses.** Ce déséquilibre permet aux cybercriminels de bénéficier d'une avance constante. Aucun mécanisme ne permet d'anticiper ou de bloquer de manière proactive les réservations malveillantes.

Contrairement aux marques, brevets ou dessins et modèles, qui bénéficient de cadres harmonisés et de l'appui d'autorités spécialisées, la lutte contre la fraude aux noms de domaine souffre d'un volet répressif désordonné et d'une véritable faille de gouvernance. Il en résulte une insécurité juridique, alimentée par l'absence de règles internationales contraignantes et de mécanismes d'exécution efficaces.

Le système actuel de gestion des noms de domaine semble avoir atteint ses limites, appelant à une refonte profonde et à une harmonisation globale de ses standards de régulation.

Recommandation n°1 :

Lutter efficacement contre l'usurpation de nom de domaine à des fins frauduleuses

La FEBEA préconise une modernisation des outils de gouvernance des noms de domaine, ainsi que des leviers administratifs de blocage couplée à un renforcement du cadre réglementaire.

L'action isolée au niveau national étant rendue inopérante par des réseaux criminels transnationaux, la FEBEA appelle à une harmonisation du volet répressif au niveau de l'Union européenne. L'instauration d'une autorité centrale de signalement permettrait une coopération immédiate et contraignante entre les États membres, évitant ainsi que les autorités nationales ne se renvoient la compétence.

L'objectif est de neutraliser la fraude à la source en automatisant l'interdiction de réserver des domaines identiques ou cyber squattant des marques protégées.

Élever la lutte contre la contrefaçon des produits cosmétiques au rang d'enjeu de santé publique

Bien que la fraude soit principalement traitée sous l'angle de la propriété intellectuelle ou du préjudice financier, les dirigeants rappellent que **la contrefaçon cosmétique constitue avant tout un risque sanitaire majeur pour les consommateurs.**

Il ne s'agit plus seulement de protéger une marque, mais de garantir que le produit appliqué sur la peau d'un consommateur n'est pas une formule chimique non contrôlée.

La responsabilité des intermédiaires numériques doit être engagée dès lors qu'ils ne déploient pas les outils de vérification - dont l'efficacité est aujourd'hui techniquement démontrée - des exigences réglementaires applicables (obligation d'information, ingrédients, allergènes, allégations, exigences de sécurité et de documentation, enregistrement et notifications, interdiction de tests sur les animaux...).

Recommandation n°2 :

Élever la lutte contre la contrefaçon des produits cosmétiques au rang d'enjeu **de santé publique**

Cette requalification doit permettre l'alignement des moyens de la police judiciaire sur ceux des autorités sanitaires, afin de déployer un arsenal répressif d'exception contre les produits présentant un risque toxicologique pour les consommateurs.

Également, des mécanismes de coopération renforcée apparaissent nécessaires entre ces autorités publiques et les organismes représentatifs du secteur (agissant au nom des entreprises cosmétiques), afin d'identifier les risques et de mettre en œuvre des actions rapides et efficaces.

Responsabiliser et contraindre réellement les plateformes

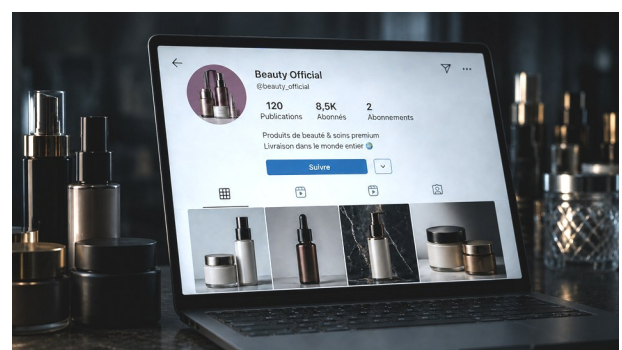
L'espace numérique souffre d'un défaut systémique de régulation proactive. La fraude prospère en l'absence de « gardiens capables » de protéger les entreprises et les consommateurs. Aujourd'hui, les plateformes numériques (réseaux sociaux, hébergeurs, marketplaces, moteurs de recherche) échouent à ce rôle de gardien. Face aux géants du numérique, la France ne peut plus agir de manière isolée ; seul l'échelon européen offre la possibilité de légiférer à cette échelle.

Cette ambition se heurte à des modalités d'exécution complexes. Les entreprises constatent que les outils réglementaires récents, à l'image du DSA européen, produisent des effets trop limités et exigent bien souvent une action judiciaire préalable, longue et coûteuse, pour obtenir de simples blocages de contenus. Bien que les répondants attestent que le manque systémique de reconnaissance des titulaires de droits en tant que « signaleurs de confiance » (trusted flaggers) ait eu jusqu'à présent un impact négatif

significatif sur le terrain, une évolution majeure et positive se dessine. En effet, le récent projet de lignes directrices de la Commission européenne clarifie désormais expressément que les entités privées, y compris les titulaires de droits de propriété intellectuelle, sont pleinement éligibles à ce statut. Pour l'obtenir et bénéficier du traitement prioritaire de leurs signalements, ces entités devront toutefois démontrer aux autorités compétentes qu'elles remplissent l'ensemble des conditions fixées par le DSA, règlement européen sur les services numériques, notamment en matière d'expertise, d'indépendance et de capacité à soumettre des notifications de manière objective.

Face à ce blocage, l'administration tente de transformer ces impasses en leviers d'action. La vision de Sarah LACOCHE, Directrice Générale de la DGCCRF, atteste d'une lecture qui privilégie l'exploitation des failles du droit existant à une réforme législative : "L'enjeu est d'exploiter tout le potentiel du cadre actuel avant d'envisager une réouverture du texte. Pour pallier la difficulté persistante à joindre les responsables des vendeurs hors-UE, nous préconisons de qualifier l'absence de maîtrise de ces interlocuteurs de 'risque systémique' au sens de l'article 35 du DSA. Ce levier permettrait, à droit constant, d'imposer aux plateformes des mesures d'atténuation beaucoup plus strictes".

Sans incriminer les plateformes, dont l'usage premier est lui-même détourné, c'est en les contraignant légalement à assumer leur rôle de régulateur que les pouvoirs publics européens mettront fin à l'impunité numérique dont bénéficient aujourd'hui les réseaux criminels. Cet objectif doit également concerner les plateformes dédiées à la seconde main, leur vocation initiale d'économie circulaire est aujourd'hui dévoyée par des acteurs malveillants.



Ce constat impose aux autorités nationales et européennes d'exiger des intermédiaires un devoir de vigilance accru, notamment pour les acteurs du marché de l'occasion massivement exploités par les contrefacteurs.

Les autorités doivent exiger de ces plateformes la mise en place proactive des barrières techniques de nouvelle génération, comme :

- L'authentification par scan de codes unitaires,
- L'analyse de cohérence par intelligence artificielle,
- L'obligation de traçabilité de l'achat,
- L'obligation de fournir des photographies sous plusieurs angles de chaque produit.

Recommandation n°3 :

Responsabiliser et contraindre *réellement* les plateformes

La FEBEA dénonce la passivité ou la coopération limitée de certaines plateformes, alors même que les outils techniques permettant d'identifier les contenus illicites existent. Les autorités européennes et nationales doivent désormais exiger de ces acteurs la mise en œuvre systémique de ces outils, aujourd'hui financés par les marques pour une efficacité très limitée.

A l'image de la décision Meta Platforms c/ Groupe Lucien Barrière rendue par la Cour d'appel de Paris, la FEBEA prône la généralisation de mesures « dynamiques » permettant de prévenir la diffusion future de contenus contrefaisants ou dénigrants, reproduisant les marques ou portant atteinte à leur réputation, sur les plateformes ou les réseaux sociaux.

Soutenir financièrement la cyber-résilience des entreprises les plus vulnérables

L'étude de l'Association of Certified Fraud Examiners prouve que la mise en place de contrôles internes proactifs (formation des employés, lignes de signalement/hotlines, audits surprises) permet de réduire de 50% la durée d'une fraude et de faire chuter les pertes médianes de 40% à 50%.

Face à la fraude, les entreprises font état d'un « mur du coût », tant pour l'investissement dans des solutions défensives matérielles que pour souscrire à des cyber-assurances dont les franchises constituent un investissement. **L'État ne peut pas seulement exiger des entreprises**

qu'elles se protègent, il doit les y aider.

Ce soutien doit permettre de financer des audits externes, des programmes de formation continue pour les salariés (le maillon le plus ciblé par l'ingénierie sociale) et l'accès à des outils d'Intelligence Artificielle souverains et sécurisés pour contrer le risque.

Recommandation n°4 :

Créer un fonds de soutien étatique ou un crédit d'impôts dédiés à la cyber résilience et aux dispositifs de sécurité numérique des TPE, PME et ETI

La FEBEA préconise la création d'un fonds de soutien étatique ou de crédits d'impôt spécifiquement dédiés à l'équipement des PME et ETI en matière de cybersécurité.

Créer un dispositif de signalement dédié aux entreprises

Les dispositifs étatiques actuels (comme ceux de la DGCCRF) sont pensés pour les litiges de consommation courante et s'avèrent inadaptés aux signalements massifs et techniques émanant des entreprises.

L'État français pourrait s'inspirer de modèles internationaux performants, à l'image du NASC australien, qui repose sur le principe du « no wrong door ».

Cette architecture centralise le recueil des fraudes afin d'éviter que les victimes ne soient renvoyées d'une administration à l'autre, tout en garantissant que chaque signalement alimente une base de renseignement criminelle unique. Les retours d'expérience sur ce dispositif soulignent une solution efficace, marquée par une baisse des pertes financières subies par les victimes de l'ordre de 13 % dès les premiers trimestres d'activation.

Recommandation n°5 :

Instaurer un guichet unique de signalement pour les professionnels

Afin d'optimiser la remontée d'incidents, la FEBEA recommande la mise en place de plateformes spécifiques, distinctes des canaux grand public. Ce dispositif permettrait d'industrialiser le traitement des alertes, facilitant ainsi une réponse coordonnée et une analyse technique immédiate des nouveaux modes opératoires de fraude.

Accélérer la réponse pénale et la rendre réellement dissuasive

Le délai de traitement des plaintes au pénal face à la fraude numérique décourage les acteurs économiques.

À l'image de certaines PME membres de la FEBEA, **des plaintes déposées en 2024 ne sont toujours pas instruites des années plus tard**. Les entreprises constatent que le soutien des autorités est quasi-inexistant et perçoivent que l'issue de leur plainte dépend (trop) souvent du bon vouloir d'un enquêteur.

Évoquée précédemment, la territorialité constitue elle aussi un frein : face à des escroqueries transnationales, les autorités se renvoient la compétence, poussant les entreprises à ne même plus porter plainte tant la démarche s'avère inutile en pratique.

Si le cadre législatif existe, les entreprises constatent de manière unanime que son application reste insuffisante.

Recommandation n°6 : Accélérer la réponse pénale et la rendre réellement dissuasive

La FEBEA plaide pour un durcissement de l'arsenal répressif, avec l'application de sanctions pénales et financières exemplaires dans des délais d'instruction compatibles avec l'échelle de temps économique, afin de restaurer la confiance des acteurs économiques envers l'institution judiciaire.

Défendre la compétitivité des entreprises françaises

Enfin, la FEBEA demande aux pouvoirs publics français de peser de tout leur poids pour que l'Europe impose un cadre légal plus strict, forçant la coopération active des intermédiaires technologiques.

Cette démarche pourrait s'articuler autour des exigences suivantes :

- **Imposer aux hébergeurs, réseaux sociaux et marketplaces des canaux de signalement dédiés** aux entreprises couplés à une obliga-

tion légale de retrait des contenus illicites sous 24 heures.

- **Instaurer un principe de co-responsabilité.** Tout refus ou retard injustifié de la part des plateformes à agir proactivement face aux signalements des entreprises doit automatiquement engager leur responsabilité juridique et financière.

Cette stratégie pourrait s'intégrer dans le DFA (Digital Fairness Act) attendu au 4^{ème} trimestre 2026. Avec l'essor du commerce électronique et des nouvelles technologies, le DSA vise à répondre aux préoccupations d'exposition des consommateurs. Pour autant, des lacunes persistent sur l'essor des plateformes d'e-commerce qui ne relèvent pas du champ d'application du DSA. Pour la combler, la Commission a l'intention de proposer une loi sur l'équité numérique afin de protéger les consommateurs contre certaines pratiques en ligne telles que les « dark patterns ».

Un point important de discussion concerne la manière dont le DFA complètera, plutôt que de faire double emploi avec le DSA, le DMA, le RGPD et l'IA Act. Le DSA interdit déjà certaines interfaces manipulatrices sur les plateformes, mais le DFA est destiné à s'appliquer à « tous les types de commerçants », y compris les sites de commerce électronique, les applications et les services qui ne sont pas couverts en tant qu'intermédiaires par le DSA. ■

Recommandation n°7 : Défendre la compétitivité des entreprises françaises

La FEBEA demande à l'Etat français de faire de la cyber-résilience de ses entreprises, condition *sine qua non* de leur compétitivité et de leur solidité, une priorité absolue. Cela passe par une influence renforcée sur chaque nouveau véhicule législatif européen pour adopter les outils permettant aux entreprises françaises d'être défendues efficacement contre les fraudes numériques, tout en offrant aux consommateurs européens un marché intérieur sécurisé.

Annexes

Pour aller plus loin

La FEBEA et la cosmétique française : poids stratégique d'un leader mondial

La FEBEA rassemble les entreprises du secteur français de la cosmétique, écosystème riche et diversifié, composé de 82 % de TPE-PME (dont 18 % de TPE et 64 % de PME, 13 % de grands groupes et 5 % d'ETI).

L'industrie cosmétique française conjugue un ancrage local et un rayonnement international de premier plan.

Forte d'un chiffre d'affaires global de 35,6 milliards d'euros, la France s'affirme comme le leader incontesté de la beauté en captant 15 % des parts du marché mondial. Ce dynamisme hisse l'industrie cosmétique au rang de second secteur contributeur à la balance commerciale nationale, derrière l'aéronautique et le spatial et devant le vin et les spiritueux.

L'exportation demeure le véritable moteur de cette croissance : avec 22,4 milliards d'euros générés hors des frontières françaises, l'international pèse pour près des deux tiers (60 %) de l'activité totale du secteur. Le maquillage, les soins et les parfums constituent le fer de lance de ce succès, représentant à eux seuls les trois quarts des exportations de produits de beauté et d'hygiène.

Portée par un ancrage territorial fort, l'industrie cosmétique s'appuie sur un écosystème complet qui valorise chaque maillon de sa chaîne de valeur. Au-delà d'une signature de provenance, l'origine "France" atteste de la richesse du savoir-faire industriel français (depuis les filières agricoles et chimiques en amont jusqu'aux laboratoires de R&D) qui permet d'accroître de 30% en moyenne la valeur perçue des produits. Cette synergie consolide l'influence de la France à l'international. Ce rayonnement immatériel se traduit par une domination commerciale sur les

marchés mondiaux où les produits français s'exportent avec l'Union européenne, les États-Unis et la Chine comme trio de tête des destinations.

Véritable levier de décentralisation et de dynamisme territorial, le secteur se distingue par le choix de la proximité, en localisant 67 % de ses entreprises et 80 % de ses emplois en région. Par ailleurs, pour répondre avec agilité aux attentes des consommateurs, les produits cosmétiques s'appuient sur une stratégie omnicanale alliant différents circuits de distribution complémentaires : grandes et moyennes surfaces, distribution sélective, ou encore pharmacies et parapharmacies.

Au-delà de sa puissance économique, l'industrie de la beauté s'affirme comme un employeur stratégique sur le territoire national. Elle se distingue par sa mixité et son engagement inclusif, avec 60 % de femmes au sein de ses effectifs, à qui elle offre des perspectives de carrière attractives et variées.



Cadre méthodologique

Dans un contexte technologique en pleine mutation, ce rapport a été produit par la FEBEA et s'attache à offrir une photographie fidèle de la menace numérique actuelle subie par les entreprises du secteur cosmétique. Il est l'aboutissement d'un travail d'observation et d'analyse de long terme mené par la FEBEA, reposant sur une mobilisation et un investissement important de ses adhérents. Celui-ci résulte d'une étude hybride, menée au 1^{er} semestre 2026 et structurée autour de trois piliers complémentaires :

- **Une revue des travaux déjà menés comme socle théorique** : l'analyse de terrain est complétée et mise en résonance avec la littérature scientifique et les rapports d'instances internationales de premier plan.
- **Un volet quantitatif pour un état des lieux objectif** : l'administration d'un questionnaire auprès des adhérents de la fédération durant le premier trimestre 2026 a permis de collecter les premières données afin d'objectiver les tendances, de mesurer l'ampleur systémique des phénomènes de fraude et de dresser un panorama représentatif de l'exposition actuelle.
- **Un volet qualitatif ancré dans la réalité opérationnelle** : la conduite d'entretiens semi-directifs avec les professionnels du secteur a permis de capter les enjeux stratégiques et les signaux faibles. Cet ancrage terrain s'est avéré indispensable pour comprendre la complexité des attaques, illustrer les statistiques par des expériences métiers vécues et identifier les impasses techniques ou juridiques rencontrées au quotidien par les entreprises.

Cette étude permet de mettre en perspective les données recueillies et d'asseoir les préconisations de la FEBEA sur des fondamentaux solides. Cette dernière dépasse le simple stade du constat : il s'affirme comme un véritable appel à l'action.

Bibliographie

[Social change and crime rate trends: A routine activity approach. American Sociological Review](#), Lawrence E. Cohen and Marcus Felson, University of Illinois, 1979

[Serious and Organised Crime Threat Assessment: Crime in the Age of Technology](#), Europol, 2017

[Organized Crime: Analyzing Illegal Activities, Criminal Structures, and Extra-legal Governance](#), Klaus von Lampe, Berlin School of Economics and Law, Janvier 2016

[Advancing theory of fraud: the S.C.O.R.E. model](#), Georgios Vousinas, National Technical University of Athens, 2019

[Mapping the Risk of Serious and Organised Crime Infiltrating Legitimate Businesses: Final Report](#), Ernesto U. Savona and Michele Riccardi, Transcrime.it, 2021

[Internet Organised Crime Threat Assessment \(IOCTA\)](#), EUROPOL, 2023

[Online Fraud Schemes: A Web of Deceit](#), Europol, 2023

[The Other Side of the Coin: An Analysis of Financial and Economic Crime](#), European Financial and Economic Crime Threat Assessment 2023, Europol, 2023

[Targeting scams. Report of the National Anti-Scam Centre on scams activity 2023](#), April 2024

[Occupational Fraud 2024: A Report to the Nations](#), Association of Certified Fraud Examiners (ACFE), 2024

[Fraude organisée : Étude thématique](#), Office des Nations Unies contre la drogue et le crime (ONUDC), 2024

[Targeting scams. Report of the National Anti-Scam Centre on scams activity 2024](#), Mars 2025

[Revisiting the Fraud Triangle in Corporate Frauds: Towards a Polygon of Elements](#), Paolo Roffia & Michele Poffo, Department of Management, University of Verona, 2025

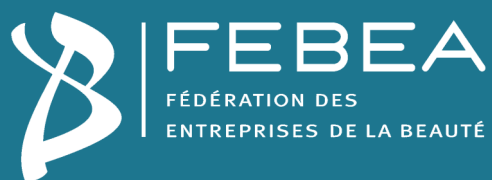
[Approches malveillantes sur les réseaux sociaux professionnels](#), Flash ingérence économique DGSI, novembre 2025

[AI scams in 2026: how they work and how to detect them](#), Vectra.ai, 2026

Crédits photo

Photo de la page de couverture :
iStock.com / [guvendemir](#) / Ref. 1129103253

Les autres illustrations de ce rapport ont été produites avec le concours de l'intelligence artificielle. Elles sont destinées à une fonction illustrative et ne constituent pas des photographies ou documents authentiques.



137 rue de l'Université - 75007 PARIS
Tél. 01 56 69 67 89
www.febea.fr
[@leLabdeClaire](https://www.instagram.com/leLabdeClaire)