MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

FLASH INGÉRENCE ÉCONOMIQUE DGSI #122

Août 2026

LES DIFFÉRENTS MODES OPÉRATOIRES DE L'INGÉRENCE ÉCONOMIQUE ÉTRANGÈRE : ILLUSTRATIONS ET PRÉCONISATIONS

Ce « flash » évoque des actions d'ingérence économique dont des sociétés françaises sont régulièrement victimes.

Ayant vocation à illustrer la diversité des situations auxquelles les entreprises sont susceptibles d'être confrontées, il est mis à votre disposition pour vous accompagner dans la diffusion d'une culture de sécurité interne.

Il est également disponible sur le site internet : **www.dgsi.interieur.gouv.fr**

Par mesure de discrétion, le récit ne comporte aucune mention permettant d'identifier les entreprises visées.

Pour toute question relative à ce « flash » ou si vous souhaitez nous contacter, merci de vous adresser à :

▷ securite-economique@interieur.gouv.fr

LES DIFFÉRENTS MODES OPÉRATOIRES DE L'INGÉRENCE ÉCONOMIQUE ÉTRANGÈRE : ILLUSTRATIONS ET PRÉCONISATIONS

Ce flash spécial met en avant plusieurs modes opératoires de l'ingérence économique privilégiés par des acteurs étrangers, illustrés d'exemples démarqués détectés par la DGSI.

1 ATTEINTES CAPITALISTIQUES

Les atteintes capitalistiques portent principalement sur les propositions de rachat ou de prises de participation au capital d'entreprises par des établissements ou fonds d'investissement étrangers. Ces pratiques sont susceptibles de faire passer sous contrôle étranger des activités innovantes ou souveraines. De nombreuses entreprises ont ainsi connu des délocalisations vers l'étranger ou des pertes d'activités, après le rachat de leurs activités par des entités étrangères. Ces situations permettent également à ces investisseurs de récupérer à leur profit les savoir-faire d'entreprises innovantes connaissant des difficultés financières.

EXEMPLE

Une entreprise étrangère a racheté un groupe d'entreprises comprenant une entité française, développant une technologie innovante et détenant plusieurs brevets. Peu après le rachat, le groupe étranger a décidé de se réorganiser, au détriment de l'entreprise française. En effet, l'entreprise étrangère a souhaité réorienter les savoir-faire qu'elle détenait autour de différents pôles. Dans ce cadre, elle a décidé de liquider l'entreprise française mais de conserver la propriété intellectuelle de cette dernière en la transférant à une autre entité du groupe, située à l'étranger.

RECOMMANDATIONS

En amont du rachat :

- Évaluer l'honorabilité des candidats à la reprise de l'entreprise. Dans ce cadre, il s'agit de recueillir le maximum d'informations sur les candidats, afin d'évaluer leurs intentions. Cette vérification peut être effectuée par un cabinet spécialisé ou des consultants externes ;

- Veiller à garantir une protection juridique suffisante aux technologies les plus sensibles. Il peut être utile d'envisager des clauses strictes relatives à la protection de la propriété intellectuelle, afin qu'elle ne soit pas délocalisée ensuite.

À la signature du rachat et ensuite :

- S'interroger sur la question de savoir si le projet de rachat de l'investisseur étranger répond aux conditions d'une opération soumise à autorisation préalable, dans le cadre du dispositif de contrôle des investissements étrangers en France (IEF). En effet, conformément au code monétaire et financier (CMF), certains investissements ou acquisitions, notamment dans un secteur d'activité considéré comme stratégique, doivent être soumis à autorisation de l'administration. Ce dispositif peut conduire l'investisseur à s'engager à respecter certaines conditions. Chargée de la mise en œuvre de ce dispositif, la direction générale du Trésor (DG Trésor), rattachée au ministère de l'Économie, des Finances et de la Souveraineté industrielle, énergétique et numérique, propose des informations complémentaires sur son site internet : www.tresor.economie.gouv.fr ;

- Prendre attache avec le délégué à l'information stratégique et à la sécurité économiques (DISSE), présent dans toutes les régions. Cet interlocuteur est le correspondant local du SISSE et permettra d'obtenir des informations et des conseils, en cas d'association avec un acteur étranger. Les adresses électroniques des DISSE figurent sur la page Internet du SISSE : www.sisse.entreprises.gouv.fr ;

- Contacter la DGSI en cas de suspicion de captation d'informations stratégiques ou d'atteinte à la propriété intellectuelle.

2 ATTEINTES HUMAINES

Les atteintes humaines peuvent notamment se caractériser par des tentatives de débauchage ou des recrutements à risque et constituent l'une des menaces les plus importantes identifiées. Ce type d'atteinte induit régulièrement des pertes de savoir-faire, comme par exemple des compétences propres à des industries de pointe ou à des technologies innovantes. Les débauchages ciblent également le monde de la recherche, fondamentale ou appliquée. Les acteurs étrangers n'hésitent pas, à cette fin, à proposer des conditions particulièrement avantageuses, notamment salariales, afin d'attirer des talents hors de France.

EXEMPLE

Plusieurs salariés d'une entreprise française développant une technologie stratégique ont été ciblés par un concurrent étranger évoluant dans le même secteur, qui a créé une filiale en France quelques mois auparavant. Après plusieurs approches, le concurrent étranger a réussi à débaucher plusieurs cadres de l'entreprise française, dont certains y travaillaient depuis plus d'une dizaine d'années. Il s'est avéré que cette démarche s'inscrivait dans une dynamique plus large visant, pour l'État d'origine de l'entreprise, à rattraper son retard technologique dans le secteur. L'entreprise française a renforcé ses clauses de non-concurrence dans les contrats de ses salariés et a entamé une action en justice envers l'un des salariés débauchés pour concurrence déloyale.

RECOMMANDATIONS

Anticiper les risques de débauchage :

- Effectuer une veille régulière des sociétés concurrentes ;
- Anticiper les situations à risques, comme les tensions internes, qui pourraient créer du ressentiment chez ses salariés ;
- S'assurer d'une protection juridique suffisante dans la rédaction des contrats de travail, particulièrement pour les professions les plus sensibles ;
- Sensibiliser régulièrement tous ses salariés aux risques d'approches étrangères et de captation de données à des fins malveillantes, notamment sur les réseaux sociaux ou les plateformes d'échange de services en ligne.

En cas de débauchage ou d'approche suspecte :

- S'assurer de la restitution effective de tous les supports numériques et documentaires d'un salarié lors de son départ et révoquer l'ensemble de ses accès logiques et physiques ;
- En cas de suspicion d'exfiltration de données d'un ancien salarié, faire analyser le poste de travail par des spécialistes ;
- En cas d'exfiltration de données, déposer plainte auprès des services de police ou de gendarmerie et alerter la DGSI de l'incident ;
- Signaler à la hiérarchie ou à la direction sûreté toute approche suspecte ou intrusive ;
- Mettre un terme aux échanges avec la personne auteur d'approche intrusive.

3 ATTEINTES CYBERNÉTIQUES

Les atteintes cybernétiques sont notamment caractérisées par des intrusions dans les systèmes d'information et des vols de supports informatiques, avec pour objectif la récupération de données stratégiques ou sensibles. Dans ce contexte, l'évolution rapide de certaines technologies, comme l'intelligence artificielle (IA), peut également conduire à des failles de sécurité informatique et constituer des risques pour la souveraineté des entreprises, et plus particulièrement, pour la protection de leurs données.

EXEMPLE 1

Début 2026, un groupe industriel français a été confronté à une divulgation de données sensibles, après qu'une société étrangère spécialisée dans l'IA et plus particulièrement dans la reconnaissance automatique d'objets et d'étiquetages, en contrat avec le groupe, a mis en ligne sur son site Internet plus de 1500 images des locaux du groupe industriel français, en particulier des plans détaillés de sites sensibles. Si le but de la société d'IA était seulement de montrer à d'autres clients potentiels la haute technicité de leurs solutions à travers des exemples réels, les responsables n'ont pas pris la mesure de la sensibilité des informations de leur client et malgré une première mise en demeure, le groupe français a été contraint de déposer plainte constatant que ces données étaient toujours disponibles en ligne.

EXEMPLE 2

Au printemps 2026, le manager du sous-traitant informatique d'une entreprise spécialisée dans la conception de médicaments et titulaire de nombreux secrets industriels, s'est rendu compte que plusieurs employés transmettaient quotidiennement vers une IA gratuite et grand public des dizaines de documents très sensibles dans le seul but d'automatiser des processus bureautiques (transformation en pdf par exemple). Des mesures en interne ont été prises par la suite pour empêcher cette pratique.

RECOMMANDATIONS

Mesures d'hygiène et de sécurité informatique :

- Organiser les accès informatiques au sein de la société par profil et selon les fonctions des employés ;
- Nommer un référent sécurité des systèmes d'information qui aura pour mission d'être l'interlocuteur privilégié sur les questions liées à la sécurité du SI, de sensibiliser les utilisateurs et d'effectuer ponctuellement des contrôles sur l'application des bonnes pratiques SSI ;
- Formaliser dans un document les bonnes pratiques de sécurité des systèmes d'information qui devront être mises en œuvre au sein de la société. Ce document pourra servir de base dans le but d'élaborer une politique de sécurité des systèmes d'information ;
- Définir une politique d'application des mises à jour des composants du système d'information et les procédures associées ;
- Renforcer la perception des risques informatiques auprès de ses collaborateurs, par exemple en conduisant des campagnes de tests de type « tentative d'hameçonnage », « ingénierie sociale » et « tests d'intrusion red team » destinées à évaluer leurs réactions face à divers scénarios d'attaques informatiques ;
- Effectuer un audit de sécurité informatique (ex : « audit de configuration », « test d'intrusion ») en privilégiant un prestataire de service de confiance, afin d'identifier et corriger les vulnérabilités de son système d'information ;
- Définir et mettre en œuvre une politique de sauvegarde des composants et données les plus critiques afin de pouvoir restaurer le service en cas d'attaque informatique ;
- Identifier les évènements les plus critiques pour la sécurité du système d'information et activer la journalisation de ceux-ci sur les équipements et applications sensibles, afin de pouvoir identifier et investiguer les dysfonctionnements ou/et les incidents de cybersécurité.

Sur l'usage de l'IA :

- Définir et encadrer les conditions d'usage de l'outil. Comme pour tout outil informatique, le cadre d'emploi de l'IA doit être défini, dans une charte informatique par exemple ;
- Pour un gage de sécurité et de souveraineté des données, il est préférable d'installer une IA en local sur ses serveurs, hébergés en Europe ou a minima de choisir un partenaire national ;
- Ne pas soumettre de données personnelles (nom, téléphone, adresse, analyses médicales, photos

personnelles, etc.) et proscrire l'utilisation d'outils d'IA commerciale pour un usage professionnel impliquant des données sensibles ;

- Vérifier l'exactitude et la pertinence des résultats obtenus, en s'appuyant par exemple sur des experts qualifiés. Il est fortement déconseillé de fonder des prises de décision uniquement sur les résultats fournis par l'IA et non vérifiés par des personnels qualifiés en interne ;
- Faire preuve de vigilance face à la manipulation de l'information et aux réponses biaisées ;
- Avertir la DGSI de tout évènement suspect lié à l'utilisation de l'IA par le biais de son adresse électronique dédiée aux sujets de protection économique : securite-economique@interieur.gouv.fr

4 ATTEINTES PHYSIQUES

Les atteintes physiques peuvent se matérialiser par des vols consécutifs à des intrusions dans des locaux d'établissements ou des captations d'informations ou de matériels sensibles par des personnes étrangères ou non, aux entités victimes. De nombreuses entreprises déplorent par ailleurs régulièrement la disparition de documents ou de prototypes, à la suite de visites de délégations étrangères, en raison d'un manque d'encadrement ou de préparation de la visite.

EXEMPLE

Une société française qui développe des produits sensibles a rencontré plusieurs représentants d'un pays étranger dans un établissement privé tiers. Les échanges ont permis d'aboutir à la signature de contrats de commercialisation desdits produits au bénéfice de l'État étranger. Un individu, en tenue de serveur de l'établissement, a attendu que les protagonistes quittent la salle pour entrer dans la pièce discrètement et photographier les contrats, avant de quitter les lieux. L'utilisation de la vidéosurveillance a permis de constater ces agissements et d'initier une action en justice.

RECOMMANDATIONS

Prévenir les risques de vol de matériel sensible :

- Sensibiliser les salariés aux risques de vol de matériels sensibles à l'intérieur et à l'extérieur de l'entreprise (salon, établissement tiers, etc.) ;
- Mettre en place des mesures élémentaires d'ordre organisationnel, visant à contrôler les accès aux différents espaces, y compris hors des périodes de visites ;
- Veiller à un encadrement spécifique des stagiaires, apprentis et sous-traitants ;
- Renforcer les contrôles d'accès pour les locaux hébergeant les matériels les plus sensibles de l'entreprise ;
- Renforcer la sécurité numérique des matériels hébergeant des données sensibles afin de limiter les risques en cas de vol ;
- Effectuer un audit de sûreté bâtimentaire pour cartographier les locaux de l'entité, hiérarchiser les différents espaces selon leur niveau de sensibilité et identifier les vulnérabilités.

Lors de l'accueil de représentants d'entités étrangères :

- Faire preuve de vigilance sur les délégations étrangères ;
- Exiger plusieurs jours à l'avance les identités des participants (noms, prénoms, date et lieu de naissance, etc.) ;
- Identifier un parcours de visite ou d'accueil des représentants étrangers, en limitant toute zone sensible ;
- S'assurer de la bonne compréhension des règles mises en place par les personnels étrangers ;
- Sensibiliser les personnels de l'entreprise aux risques de captations ;
- Faire preuve de vigilance lors des échanges informels.

Réagir à la suite d'un vol de matériel / information sensible :

- Évaluer rapidement la nature et la sensibilité des informations de l'entreprise compromises par le vol ;
- Déposer plainte et contacter la DGSI ;
- Mettre en place une veille active afin d'anticiper une possible mise en vente du matériel volé sur Internet ;
- Effectuer systématiquement un retour d'expérience interne sur les circonstances du vol.

5 ATTEINTES JURIDIQUES

Les atteintes juridiques se rapportent à la fois à l'instrumentalisation par des États étrangers de l'extraterritorialité de leurs lois, mais aussi à l'exploitation de failles juridiques susceptibles d'exposer la propriété intellectuelle d'entreprises ou laboratoires français. Une large part des atteintes juridiques concerne également le détournement de procédures d'audits financiers ou réglementaires à des fins de captations d'informations sensibles ou l'instrumentalisation des audits de conformité.

EXEMPLE

Une société française, qui exporte une part importante de sa production, fait régulièrement l'objet d'audits étrangers, destinés à vérifier la conformité des produits avec la législation des pays importateurs. Lors d'un audit, les inspecteurs étrangers ont visité une partie de l'usine de fabrication de l'entreprise française, en posant une série de questions habituelles pour ce genre de procédures. À la suite de l'audit, la délégation étrangère a été conviée au sein des locaux du siège de la société pour un moment de convivialité. Lors de cette période, plusieurs inspecteurs étrangers ont tenté d'obtenir des informations de cadres de la société française, en les interrogeant sur des formules, les matières premières utilisées et la qualité des produits. Sensibilisés en amont de l'audit par la DGSI, aucun membre de la société française n'a divulgué d'information confidentielle.

RECOMMANDATIONS

En cas d'inspection ou audit par une administration étrangère :

- Identifier en interne les données les plus sensibles et les zones de l'entreprise auxquelles un auditeur ne devrait pas avoir accès ;
- Bien identifier, au sein de son entité, les personnels qui seront chargés de répondre aux auditeurs ;
- Répondre aux exigences des autorités étrangères, sans dépasser le cadre des questions posées, et répertorier l'ensemble de leurs demandes ;
- Dans la mesure du possible, privilégier une solution numérique sécurisée et souveraine pour communiquer avec l'entité chargée de l'audit ;
- Faire remonter à la DGSI toute difficulté ou tout incident en lien avec la procédure d'audit ;
- Concernant le contenu des informations à transmettre dans le cadre de cet audit, prendre attache avec le SISSE. L'avis rendu par le SISSE précisera, à l'aune de la loi de blocage, ce qui peut être transmis ou non sans exposer la responsabilité pénale de l'entreprise en France. L'avis rendu par le guichet sécurise la conduite à tenir au regard du droit. Ces services seront en mesure de conseiller les entreprises dans leur stratégie de remédiation à adopter en amont ou en cas de difficultés rencontrées dans le cadre de l'audit : guichet.sisse@finances.gouv.fr

Prévenir les risques juridiques et réglementaires :

- Effectuer une veille juridique de chaque pays dans lequel la société est implantée ou avec lesquels elle entretient des liens économiques, commerciaux ou partenariaux ;
- Recenser les contentieux juridiques s'étant produits au sein des pays dans lequel la société est implantée ou possède des intérêts ;
- Assurer un audit de conformité en interne, si possible par un cabinet spécialisé et certifié, afin de se prémunir des risques liés aux mécanismes juridiques extraterritoriaux ;

Dans le cadre d'un contentieux juridique ou réglementaire :

- Évaluer l'impact de la procédure ou de la sanction éventuelle pour les activités de la société dans le pays concerné ;
- Signaler à la DGSI la procédure ou la demande des autorités locales ;
- Entrer en contact avec les autorités compétentes, en cas de demande d'accès à des informations stratégiques, notamment le SISSE dans le cadre d'un recours éventuel à la Loi de blocage.

6 ATTEINTES À LA RÉPUTATION

Les atteintes à la réputation concernent toutes les actions qui visent à déstabiliser ou dénigrer une entité. Il peut s'agir de rumeurs, de diffamation ou encore de mise en cause sur le fondement de la responsabilité sociale ou environnementale. De nombreux évènements internationaux sont de nature à porter atteinte à la réputation d'une entité, à l'image de l'utilisation de ses produits ou services dans le cadre d'un conflit à l'étranger ou au profit d'une puissance étrangère autoritaire. Les entités œuvrant dans des secteurs ayant un impact environnemental négatif sont particulièrement exposées aux attaques réputationnelles, qui peuvent aller jusqu'à des actions de manipulation de l'information.

EXEMPLE

Une grande entreprise française a été ciblée par une campagne de diffamation par deux de ses concurrents étrangers. Ces derniers ont transféré de fausses informations à plusieurs parlementaires de leur pays d'origine, selon lesquelles l'entreprise française serait impliquée dans des opérations de guerre. Ils ont également contacté une chaîne d'information en continu, qui a relayé les accusations à l'encontre de l'entreprise française. Celle-ci a contacté les autorités du pays en question, qui représente des parts de marché importantes, afin de démentir les faits et apporter des éléments de preuve.

RECOMMANDATIONS

Prévenir les risques d'atteinte à la réputation :

- Identifier les activités et projets les plus propices à des actions visant à nuire à son image ;
- Surveiller son image sur internet et les réseaux sociaux, notamment dans le cadre d'une expansion commerciale sur des marchés étrangers ;
- Prendre connaissance des pratiques commerciales des concurrents, lors de l'implantation sur de nouveaux marchés ;
- Assurer la visibilité des informations de la société concernant les normes et les certifications qu'elle respecte ;
- Anticiper les coûts d'une campagne médiatique et solliciter les services d'un cabinet d'avocats pour envisager des réponses judiciaires.

En cas d'atteinte avérée à la réputation :

- Évaluer la crédibilité et l'ampleur de l'atteinte à la réputation ;
- Déposer plainte pour toute atteinte à la réputation susceptible de constituer une infraction, à l'image de la diffamation ;
- Signaler à la DGSI la démarche malveillante qui cible l'entreprise.

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité