Godot & Fils : la fuite dont le client paie le coût

En juin 2026, le négociant en métaux précieux Godot & Fils informe ses clients d'un accès non autorisé à son système d'information, aussitôt interrompu selon lui. Cinq mois plus tard, des clients âgés remettent leurs lingots à de faux policiers qui connaissaient leurs commandes. L'incident avait été qualifié par ce qui n'avait pas été pris. Sa gravité tenait à ce que l'attaquant pouvait faire de ce qui l'avait été. Entre les deux, le coût a quitté le bilan de l'entreprise pour celui de ses clients : c'est ce qu'Arthur Cecil Pigou décrivait en 1920 comme un écart entre produit net privé et produit net social, une externalité négative (un coût imposé à d'autres que celui qui le cause, sans compensation).

Par Alexandre Berge · 25 novembre 2026 · 13 min de lecture · Chronique

Ce que tout le monde a vu : de l'or remis sur le pas de la porte

L'appel vient d'un homme qui se présente comme un agent antifraude de la société où la victime a acheté son or. Il détaille ses achats, cite des informations personnelles, puis annonce que l'entreprise a été piratée. Il conseille de porter plainte et de mettre l'or en sécurité en le remettant à un policier, contre un code secret. Quelques heures plus tard, le faux policier repart avec lingots, louis d'or ou bijoux. C'est le scénario révélé par RTL le 16 novembre 2026. Le lendemain, France 2 nomme l'enseigne : Godot & Fils.

À la date du 23 novembre 2026, les faits publics sont les suivants. En juin, l'enseigne écrit à ses clients qu'un accès non autorisé « à une partie de notre système d'information a été détecté et immédiatement interrompu », selon le courriel cité par France 2. Les équipes de France Télévisions indiquent s'être procuré les données dérobées : nom, téléphone, adresses électronique et postale, détail et montant des commandes. Elles avancent, au conditionnel, le chiffre de 50 000 personnes touchées. France 2 fait état de six victimes identifiées, âgées de 65 à 72 ans. Le préjudice de 765 000 euros est, selon RTL, un minimum estimé à ce stade par l'enquête : la valeur des biens remis par les seules victimes connues, alors que leur recensement se poursuit. Des plaintes ont été déposées dans une douzaine de départements. Les deux médias divergent sur le calendrier. France 2 décrit une vague d'escroqueries en août, puis une autre dans la semaine précédant son reportage. RTL fait commencer les escroqueries en septembre et situe en août la découverte de l'attaque par la société.

Le 20 novembre, la procureure de la République de Paris, Laure Beccuau, et la gendarmerie

annoncent la mise en examen, la veille, de dix personnes soupçonnées d'avoir piraté trois sociétés de courtage en métaux précieux et une société d'aide à la déclaration de cryptoactifs, puis exploité leurs fichiers de clients. Selon la procureure, citée par l'AFP, les auteurs, « munis des informations les concernant », appelaient les victimes en se présentant comme employés des courtiers ou membres des forces de l'ordre, et les mettaient en garde contre des risques de cambriolage. Le parquet ne nomme aucune société et ne chiffre pas le préjudice. À cette date, aucune autorité n'a établi publiquement que Godot & Fils figure parmi les trois courtiers. Le lien entre l'intrusion et les escroqueries est rapporté par RTL, d'après une source policière, et par France Télévisions, qui identifie l'enseigne, et c'est à ce titre qu'il est repris ici.

La couverture a raconté l'affaire par ses auteurs et par l'ampleur du coup de filet, 176 gendarmes mobilisés selon la procureure. Le bandeau d'alerte du site de l'enseigne suit le même fil : il met en garde contre les escrocs qui se réclament d'elle, sans évoquer l'incident de juin. Le général Hervé Pétry, qui commande l'Unité nationale cyber de la gendarmerie, parle pourtant de données volées transformées en « fichiers de renseignement permettant de cibler des victimes ». La formule pose la question que le récit des escrocs laisse de côté : comment un fichier commercial devient un fichier de renseignement, et qui en porte le coût.

L'incident a été qualifié par ce que l'attaquant n'avait pas pris

Le 24 juin, sur la plateforme d'avis Trustpilot, l'équipe de l'enseigne répond à un client inquiet que les données ont été « consultées et non pas fuitées ». Elle ajoute que les données sensibles au sens du RGPD (règlement général sur la protection des données) désignent les données bancaires et les mots de passe, et que noms, prénoms et adresses ne peuvent être qualifiés ainsi. Le 3 juillet, une autre réponse récuse toute minimisation et précise que sont concernés l'identité, les coordonnées et l'historique de transactions des clients, à l'exclusion des données bancaires, mots de passe et documents d'identification.

Rien dans ces textes ne permet de prêter une intention à l'entreprise. Ils montrent une grille de lecture : l'incident y est mesuré par la catégorie des données touchées, celles qui exposent le compte du client ou la conformité de l'entreprise. Selon cette grille, un nom et une ligne de commande sont des données ordinaires.

Ce n'est pas la grille du règlement. Les catégories particulières de son article 9 visent notamment l'origine ethnique, les opinions politiques ou la santé, non les coordonnées bancaires. Surtout, le texte mesure la gravité d'une violation par le risque qu'elle fait courir aux personnes. Son considérant 85 cite, parmi les dommages possibles, la perte financière, et la CNIL gradue les obligations selon que ce risque est nul, simple ou élevé. **Le droit posait la question de l'usage. La grille employée répondait à celle de la catégorie.**

Pour l'attaquant, la lecture est inverse. Un nom, une adresse et une commande de pièces d'or désignent une personne qui a probablement de l'or chez elle. Répétée sur des milliers de

lignes, cette association forme ce que le général Pétry appelle un fichier de renseignement. **Le fichier client d'un négociant en or est, pour qui sait le lire, une carte des coffres domestiques.**

Le préjudice se forme hors du bilan, chez ceux que les comptes ne voient pas

Pigou ouvre le chapitre IX de la deuxième partie de *The Economics of Welfare* par un constat : l'industriel s'intéresse au produit net privé de son activité, non à son produit net social. Appliquée à l'incident, la distinction devient comptable. Le coût privé d'une fuite comprend l'investigation, la remédiation, les notifications, la prévention, une éventuelle sanction et l'atteinte à la réputation. Le coût social ajoute un poste que les comptes de l'organisation n'enregistrent pas : l'or remis par des clients de 65 à 72 ans. Ce préjudice ne pèse sur aucun de ses indicateurs et reste à la charge des victimes tant qu'aucune décision n'en attribue la responsabilité.

Le dommage est différé, puisque l'escroquerie commence des mois après l'intrusion, quand la gestion de crise est d'ordinaire close. Il est dispersé entre des particuliers de douze départements qui ignorent partager la même cause. Il se concentre enfin, à s'en tenir au profil des victimes identifiées, sur des clients âgés qui conservent leur or à domicile. **Plus le coût s'éloigne du système compromis, dans le temps et dans l'espace, moins il pèse dans la qualification de l'incident.**

> **L'externalité négative (Pigou, 1920)**
>
> Dans *The Economics of Welfare* (Londres, Macmillan, 1920, quatrième édition 1932, partie II, chapitre IX, § 10), Arthur Cecil Pigou décrit la situation où une personne A, en rendant contre paiement un service à une personne B, rend aussi « services or disservices to other persons » (des services ou des préjudices à d'autres personnes), sans que le bénéficiaire puisse être facturé ni le lésé indemnisé. L'intérêt privé cesse alors de conduire au meilleur résultat collectif. Le concept sépare ici ce qu'un incident de données coûte à l'organisation et ce qu'il coûte aux personnes dont elle détient les informations. Les clients sont certes parties à une relation commerciale, mais le risque que leur fait courir la conservation de leur historique ne fait partie ni de ce qu'ils achètent ni de ce qu'ils peuvent observer.

Ledger, 2020 : la fuite réelle devient l'argument de l'escroc

Le précédent le plus proche est celui de Ledger, fabricant français de portefeuilles matériels de cryptoactifs. En juillet 2020, l'entreprise annonce un accès à sa base commerciale et marketing, qu'elle évalue à plus d'un million d'adresses électroniques et environ 9 500 fiches clients détaillées. À l'automne, de faux avis de violation de données à son nom invitent ses clients à installer une application piégée, rapporte BleepingComputer. Le 20 décembre 2020, la base complète est publiée sur un forum : 272 853 acheteurs avec nom, adresse postale et

téléphone. Deux jours plus tard, l'entreprise écrit que certains de ses clients ont été la cible de « menaces personnelles ».

La parenté est structurelle. Le premier périmètre annoncé mesurait ce que l'entreprise savait, non ce que l'attaquant détenait. Le fichier reliait une identité, une adresse et la détention probable d'un actif de valeur. Et la fuite réelle est devenue l'argument de l'escroc, crédible parce qu'il évoque un incident vrai. Chez Ledger comme dans l'affaire Godot & Fils telle que la rapporte la presse, la victime n'est pas trompée malgré la fuite, mais grâce à elle.

La suite du cas montre où se range le coût. Selon La Lettre et TheBigWhale, repris par Next le 24 octobre 2024, la CNIL a infligé à Ledger, qui l'a confirmé, une amende de 750 000 euros plus de quatre ans après les faits, pour des manquements à la sécurité et à la durée de conservation des données. Cette amende va au Trésor public et ne répare rien chez les clients. Certains ont engagé une action civile dès juin 2021, et ce n'est qu'en décembre 2025, selon Next, qu'un juge a ordonné à Ledger de lui transmettre la décision de la CNIL. **La sanction administrative mesure un manquement de conformité. Le dommage des clients relève d'une autre procédure, plus lente et à leur initiative.**

Partout où un fichier révèle un patrimoine, le même écart attend son exploitant

Le mécanisme ne tient pas à l'or. Il se reproduit dès que trois conditions se rencontrent.

La première est un fichier dont la valeur pour un tiers malveillant excède sa valeur pour son détenteur : historique d'achats de biens de valeur, liste de détenteurs d'un actif, données qui laissent deviner l'âge ou l'isolement. Un bijoutier, un assureur habitation, un gestionnaire de patrimoine ou un service d'aide à domicile en détiennent. Le dossier parisien vise d'ailleurs aussi une société d'aide à la déclaration de cryptoactifs.

La deuxième est une qualification de l'incident par catégories plutôt que par scénarios d'usage. Elle commande la suite : le contenu de la notification, la durée de la vigilance, le moment où le dossier est clos.

La troisième est un délai d'exploitation qui dépasse l'horizon de la gestion de crise. Selon RTL comme selon France 2, les premières escroqueries surviennent deux à trois mois après l'accès signalé en juin, et elles se poursuivent encore en novembre.

Dans une organisation quelconque, plusieurs signes rendent ce mécanisme visible. Le rapport de clôture d'un incident s'arrête à la remédiation technique. La notification aux personnes dit ce qui n'a pas été touché plutôt que ce qui pourrait leur arriver. Les historiques de transactions sont conservés au-delà de leur usage commercial, parce que leur stockage ne coûte presque rien dans les comptes et que leur coût de fuite n'y figure pas.

> **Grille de lecture**
>
> 1. Le dernier rapport d'incident de données de l'organisation décrit-il des scénarios

d'exploitation par un tiers, ou seulement les catégories de données touchées ?

2. Après la clôture d'un incident, combien de temps une personne reste-t-elle nommément chargée d'en suivre les effets chez les clients ?
3. Les fichiers de l'organisation permettent-ils de déduire qu'une personne détient un bien de valeur à son domicile, et cette déduction figure-t-elle dans l'analyse de risques ?
4. La durée de conservation des historiques de transactions a-t-elle été fixée au regard de leur usage, et quand a-t-elle été revue pour la dernière fois ?
5. Le registre des risques comporte-t-il une ligne pour un coût supporté par les clients ?

Ce que montreront l'instruction et les plaintes

L'affaire Godot & Fils s'est d'abord dite dans le vocabulaire de l'entreprise : un accès « détecté et immédiatement interrompu », des données « consultées et non pas fuitées ». Elle se dit désormais dans celui des plaintes : six personnes de 65 à 72 ans, des lingots, au moins 765 000 euros. Entre ces deux vocabulaires, le coût a changé de bilan. C'est l'écart que Pigou décrivait entre produit net privé et produit net social, et qu'une qualification fondée sur les données bancaires ne pouvait pas faire apparaître.

Si la gravité d'une fuite se mesure à son usage, ce sont les procédures, plus que l'entreprise, qui la révéleront. D'ici la fin de 2027, trois éléments seront observables de l'extérieur : l'identification publique, ou non, des trois courtiers visés par les informations judiciaires ouvertes à Paris, l'évolution du nombre de victimes et du préjudice recensés, et d'éventuelles actions civiles de clients contre l'enseigne. Le précédent Ledger laisse attendre qu'une décision de la CNIL, si elle vient, arrive plus tard et sanctionne un manquement sans réparer le préjudice. Si, fin 2027, le préjudice déclaré par les clients a continué de croître sans qu'aucune prise en charge ne soit annoncée, l'externalité aura été confirmée par les faits.

Note méthodologique

Faits arrêtés au 23 novembre 2026, établis par RTL, France Télévisions, Le Figaro avec l'AFP (communiqué du parquet de Paris) et par les réponses publiques de l'entreprise. Le lien entre l'intrusion et les vols reste attribué : RTL ne nomme pas la société, aucune autorité ne l'a confirmé, et l'enquête du parquet a débuté en 2025 selon franceinfo. Pour la date de l'incident, le courriel de juin de l'entreprise a été préféré à la découverte en août rapportée par RTL. La divergence sur la date des premières escroqueries (août pour France 2, septembre pour RTL) est signalée dans le texte. Les victimes étant des clients et non des tiers stricts, le choix de l'externalité comme cadre relève de l'auteur, le risque n'étant ni valorisé ni observable dans la relation commerciale. Recherche de sources, croisement des données et structuration du raisonnement s'appuient sur une assistance par intelligence artificielle. Le choix de l'angle et du cadre théorique, la vérification des sources, les arbitrages et l'établissement du texte final relèvent de l'auteur.

Sources

Documents de l'organisation et textes officiels

Achat Or et Argent (Godot & Fils), réponse de « L'équipe AOEA » à l'avis « accès non autorisé au site achat-or-et-argent », Trustpilot, 3 juillet 2026 (consulté le 23 novembre 2026), https://fr.trustpilot.com/review/achat-or-et-argent.fr

Achat Or et Argent (Godot & Fils), réponse de « L'équipe AOEA » à l'avis « FUITE DE DONNÉES », Trustpilot, 24 juin 2026 (consulté le 23 novembre 2026), https://fr.trustpilot.com/review/achat-or-et-argent.fr?page=2

Godot & Fils, bandeau « Alerte fraude : soyez vigilants face aux tentatives d'escroquerie », achat-or-et-argent.fr (consulté le 23 novembre 2026), https://www.achat-or-et-argent.fr/

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD), considérant 85 et articles 9 et 34, EUR-Lex, https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679

CNIL, « Violations de données personnelles : les règles à suivre », 19 juin 2018 (consulté le 23 novembre 2026), https://cnil.fr/fr/les-violations-de-donnees-personnelles

Presse de référence

Maxime Levy, « Au moins 765.000 euros de préjudice : comment une cyberattaque a alimenté une vaste escroquerie à l'or », RTL, 16 novembre 2026, https://www.rtl.fr/actu/justice-faits-divers/info-rtl-au-moins-765-000-euros-de-prejudice-comment-des-acheteurs-d-or-ont-ete-pieges-apres-la-cyberattaque-d-une-societe-specialisee-7900696992

France 2, journal de 13 heures, « Après un piratage de données, au moins 765 000 euros d'or ont été dérobés par des faux policiers », franceinfo, 17 novembre 2026, https://www.franceinfo.fr/faits-divers/apres-un-piratage-de-donnees-au-moins-765-000-euros-d-or-ont-ete-derobes-par-des-faux-policiers_8286569.html

France 2, journal de 20 heures, « Lingots d'or : une vaste arnaque aux faux policiers pour un préjudice d'au moins 765 000 euros », franceinfo, 17 novembre 2026, https://www.franceinfo.fr/replay-jt/france-2/20-heures/lingots-d-or-une-vaste-arnaque-aux-faux-policiers-pour-un-prejudice-d-au-moins-765-000-euros_8287172.html

Yannick Falt, « Dix personnes mises en examen pour avoir escroqué des propriétaires de cryptomonnaies et d'or », franceinfo, 20 novembre 2026, https://www.franceinfo.fr/faits-divers/dix-personnes-mises-en-examen-pour-avoir-escroque-des-cryptomonnaies-et-des-metaux-precieux-apres-des-piratages-informatiques-de-societes-specialisees_8292965.html

Le Figaro avec AFP, « Dix personnes mises en examen dans le cadre d'une enquête sur une escroquerie aux métaux précieux et aux cryptomonnaies en France », 20 novembre 2026,

https://www.lefigaro.fr/actualite-france/dix-personnes-mises-en-examen-dans-le-cadre-d-une-enquete-sur-une-escroquerie-aux-metaux-precieux-et-aux-cryptomonnaies-en-france-20261120

Cadre théorique

Arthur Cecil Pigou, The Economics of Welfare, Londres, Macmillan, 1920 (quatrième édition 1932), partie II, chapitre IX, « Divergences between marginal social net product and marginal private net product », Library of Economics and Liberty (consulté le 23 novembre 2026), https://www.econlib.org/library/NPDBooks/Pigou/pgEW.html?chapter_num=22

Parallèle historique

Ledger, « Six façons de se protéger contre la violation de données », 22 décembre 2020, https://www.ledger.com/fr/6-ways-to-face-the-data-breach

Ledger, « Mise à jour : efforts visant à protéger vos données et à poursuivre les escrocs », 13 janvier 2021, https://www.ledger.com/fr/mise-a-jour-efforts-visant-a-proteger-vos-donnees-et-a-poursuivre-les-escrocs

Lawrence Abrams, « Physical addresses of 270K Ledger owners leaked on hacker forum », BleepingComputer, 21 décembre 2020, https://www.bleepingcomputer.com/news/security/physical-addresses-of-270k-ledger-owners-leaked-on-hacker-forum/

Sébastien Gavois, « Conservation et protection des données : la CNIL sanctionne Ledger d'une amende de 750 000 € », Next, 24 octobre 2024, https://next.ink/brief_article/conservation-et-protection-des-donnees-la-cnil-sanctionne-ledger-dune-amende-de-750-000-e

Sébastien Gavois, « La CNIL condamne Ledger sans publier la décision : un juge ordonne de la recevoir », Next, 12 décembre 2025, https://next.ink/brief_article/la-cnil-condamne-ledger-sans-publier-la-decision-un-juge-ordonne-de-la-recevoir/