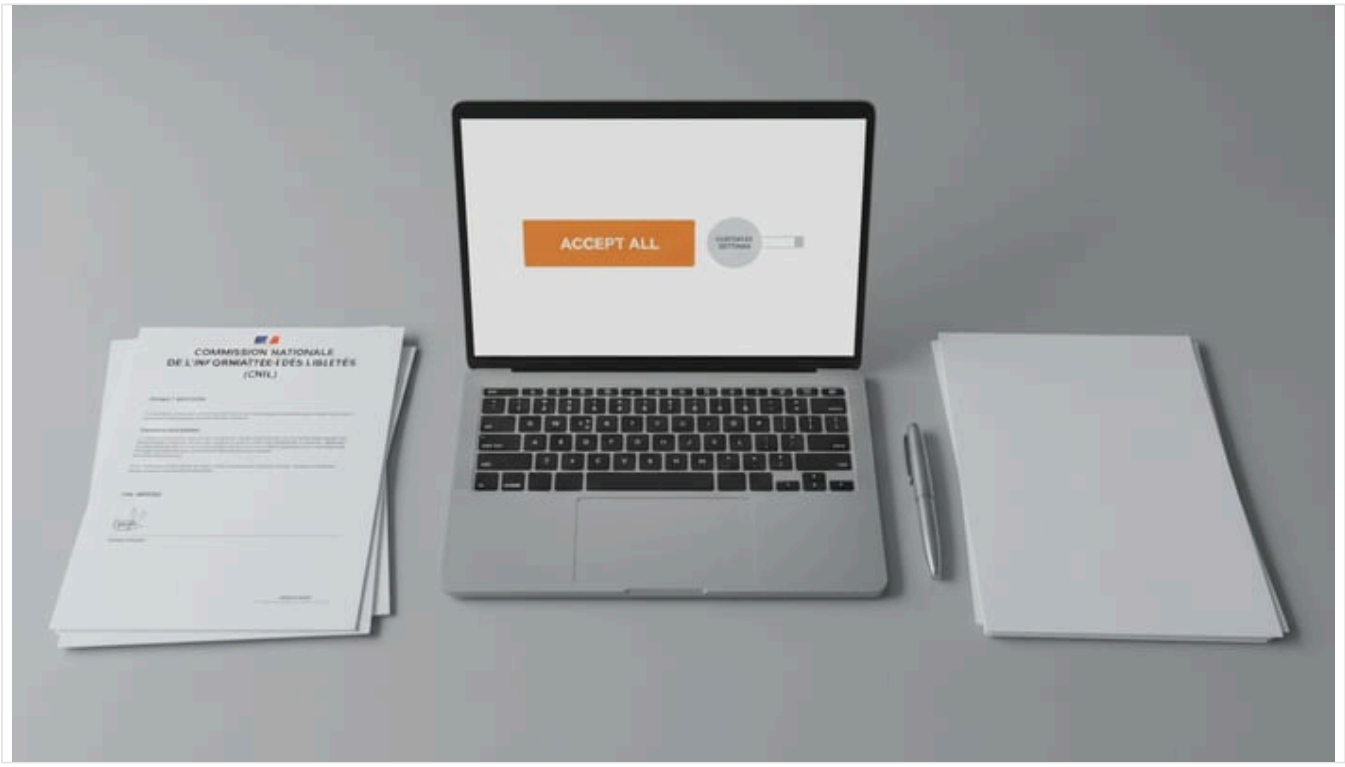
Pénalités pour le consentement aux cookies : Amendes RGPD et risques juridiques expliqués

By rankstudio.net Publié le 24 octobre 2025 40 min de lecture



Synthèse

Les bannières de consentement aux cookies sont devenues omniprésentes sur les sites web ces dernières années, sous l'impulsion de lois sur la vie privée qui exigent l'autorisation de l'utilisateur avant que les technologies de suivi (comme les cookies) puissent être déployées. Ne pas afficher une bannière de consentement aux cookies appropriée – et donc ne pas obtenir un consentement utilisateur valide – est une violation directe de ces lois. Dans toutes les juridictions, les sanctions pour de telles violations peuvent inclure des **amendes substantielles et des ordonnances d'exécution**. Par exemple, en 2025, l'Autorité française de protection des données (CNIL) a infligé des *amendes record* pour des infractions liées aux cookies : Google et Shein ont été frappés de pénalités de 325 millions d'euros et 150 millions d'euros, respectivement, pour avoir placé des cookies de suivi sans consentement librement donné (Source: www.lemonde.fr) (Source: www.cnil.fr). Les tribunaux ont également sanctionné les « murs de cookies » – des bannières qui forcent de manière coercitive les utilisateurs à accepter les cookies comme condition de service – et ont exigé des entreprises qu'elles ajoutent des options claires de « refus » sous peine d'amendes journalières (Source: www.lemonde.fr) (Source: noyb.eu). En Belgique, par exemple, l'APD a ordonné à quatre grands sites d'information d'ajouter un bouton visible « tout refuser » sous peine de pénalités de 50 000 € par jour (Source: noyb.eu). En bref, **omettre une bannière de consentement aux cookies conforme (ou en utiliser une défectueuse)** peut déclencher les sanctions maximales en vertu de la loi sur la protection des données – souvent plafonnées à 2-4 % du chiffre d'affaires mondial d'une entreprise ou à des dizaines de millions d'euros – et peut inclure des amendes journalières ou des ordonnances injonctives jusqu'à ce que la conformité soit atteinte.

Ce rapport fournit une analyse approfondie des règles légales et des tendances d'application régissant les bannières de consentement aux cookies, des types de sanctions imposées en cas de non-conformité et des implications pratiques pour les organisations. Il couvre l'évolution historique des lois sur le consentement aux cookies, les cadres réglementaires actuels dans différentes régions (en particulier l'UE et le Royaume-Uni, où les lois sont strictes) et les sanctions qui ont été imposées dans des cas réels. Nous examinons la recherche universitaire sur la conformité des bannières de cookies, les commentaires d'experts et les

études de cas (y compris les amendes majeures de la CNIL et d'autres). Nous explorons également les contre-perspectives (par exemple, les préoccupations de l'industrie concernant la « fatigue du consentement » et les réformes potentielles futures des règles relatives aux cookies). Tout au long du rapport, les affirmations sont étayées par de nombreuses citations de sources juridiques, d'annonces réglementaires, de reportages et d'études universitaires.

Introduction

L'augmentation spectaculaire des technologies de suivi en ligne au cours des deux dernières décennies a incité les régulateurs à exiger des sites web qu'ils obtiennent le **consentement** de l'utilisateur avant de déployer des cookies ou des outils analogues. Cette exigence remonte au début des années 2000 avec la « loi sur les cookies » de l'UE (la directive sur la vie privée et les communications électroniques) et a depuis été renforcée par des lois plus larges sur la protection des données (notamment le Règlement général sur la protection des données de l'UE, ou RGPD). En pratique, la manifestation la plus visible de ces règles est la **bannière de consentement aux cookies** ou la fenêtre contextuelle qui accueille les visiteurs sur de nombreux sites web aujourd'hui. Ces bannières informent généralement les utilisateurs de l'utilisation des cookies et leur demandent d'accepter ou de refuser les cookies non essentiels.

Cependant, de nombreux sites web ont eu du mal à mettre en œuvre ces bannières de manière entièrement légale. Les défaillances courantes incluent le fait de ne pas afficher de bannière du tout, de masquer l'option de refus/désinscription, de pré-cocher les cases de consentement, ou d'orienter autrement les utilisateurs vers le consentement. En conséquence, les régulateurs de la vie privée ont de plus en plus sévi, enquêtant sur les sites et imposant des sanctions. En effet, les bannières de cookies non conformes sont devenues un axe majeur de l'application de la loi. Les défenseurs de la vie privée (tels que le groupe européen NOYB) ont déposé des centaines de plaintes concernant des bannières trompeuses, incitant les autorités de protection des données (« APD ») à agir.

Ce rapport aborde la question : **Quelle est la sanction pour ne pas afficher de bannière de consentement aux cookies ?** En d'autres termes, quelles actions d'exécution et sanctions un opérateur de site web peut-il attendre s'il ne parvient pas à obtenir un consentement valide aux cookies. Nous commençons par exposer le cadre juridique (pourquoi le consentement est requis), puis nous résumons les diverses sanctions (amendes, injonctions, etc.) imposées en cas de défaillance. Nous analysons les données et les études de cas, et examinons plusieurs perspectives (régulateurs, entreprises, experts en confidentialité). Nous discutons également du contexte plus large et de l'avenir probable de la loi sur le consentement aux cookies. La réponse est complète : elle explore les subtilités du droit ePrivacy et de la protection des données, examine les tendances d'application dans différentes juridictions et fournit des exemples détaillés de sanctions, étayés par des sources expertes et universitaires.

Contexte Légal et Réglementaire

Évolution des Règles de Consentement aux Cookies

L'obligation d'afficher des bannières de cookies découle principalement des **lois sur la protection des données** adoptées dans l'UE et les juridictions associées. Les racines principales sont :

- **Directive ePrivacy de l'UE (2002/58/CE)** : Souvent appelée la « loi sur les cookies », cette directive de l'UE (modifiée en 2009 par la Directive 2009/136/CE) exige explicitement que les sites web ne puissent pas stocker ou accéder à des informations sur l'appareil d'un utilisateur (par exemple via des cookies) *à moins* que l'utilisateur n'ait **donné un consentement clair** après avoir été informé des finalités. Dans la plupart des États membres, cela a été transposé dans le droit national (par exemple, le Règlement sur la vie privée et les communications électroniques du Royaume-Uni, « PECR »). La règle fondamentale peut être résumée ainsi : **Les sites web doivent informer les utilisateurs sur les cookies et obtenir leur consentement univoque avant de placer des cookies non essentiels**.

- **RGPD de l'UE (2016/679)** : Bien que le RGPD ne mentionne pas spécifiquement les « cookies », il affirme que les cookies identifiables (en particulier ceux qui suivent le comportement) constituent des données personnelles. Ainsi, le traitement de ces données nécessite une base légale, le plus souvent le *consentement*. En vertu du RGPD, le consentement doit être donné librement, spécifique, éclairé et univoque (Article 4.). Si une bannière de cookies ne respecte pas ces normes – par exemple en acceptant par défaut tous les cookies ou en masquant l'option de désinscription – le consentement n'est pas valide en vertu du RGPD. De nombreuses amendes de l'UE pour des violations de cookies ont en fait été considérées comme des infractions au RGPD (par exemple, le fait de ne pas obtenir le consentement tel que requis par les Articles 6 et 7 du RGPD).

- **Mises en œuvre nationales** : Les États membres de l'UE (et les pays adoptant des lois similaires) ont promulgué ou adapté leurs lois sur la vie privée pour imposer des obligations de consentement aux cookies. Par exemple, la Loi Informatique et Libertés française contient des dispositions (par exemple, l'Article 82) ciblant spécifiquement les « cookies publicitaires », faisant écho à la règle de l'UE (Source: www.cnil.fr). Au Royaume-Uni, le PECR et le Data Protection Act (et maintenant le RGPD britannique) régissent les cookies. D'autres pays (par exemple, la Suisse, le Japon, la Corée du Sud) ont leurs propres lois sur la vie privée, et dans certains cas des règles spéciales pour les technologies de suivi, bien que souvent moins détaillées ou strictement appliquées qu'en UE (Source: ico.org.uk) (Source: cookie-compliance.co).

En termes simples, en vertu de la législation actuelle de l'UE/Royaume-Uni, un site web **doit** (1) informer les visiteurs de la manière dont les cookies sont utilisés, et (2) leur permettre de *consentir activement* aux cookies non essentiels. Les cookies essentiels (par exemple, pour la fonctionnalité du panier d'achat ou la sécurité de base) sont exemptés, mais pratiquement tous les cookies publicitaires, d'analyse et de médias sociaux nécessitent un consentement. La bannière de cookies du site web est le mécanisme pour atteindre (1) et (2). Comme l'indique le guide de l'ICO britannique : « vous devez informer les gens de la présence des cookies ; expliquer ce que les cookies font et pourquoi ; et obtenir le consentement de la personne pour stocker un cookie sur son appareil » (Source: ico.org.uk). Si un site web ne parvient pas à obtenir un consentement valide (par exemple, en n'ayant pas de bannière, ou en la présentant de manière incorrecte), il est en infraction avec les règles ePrivacy/RGPD et s'expose donc à des sanctions.

Exigences de Consentement en Détail

En vertu de l'Article 7 et du Considérant 32 du RGPD, le consentement doit être un **acte positif clair**. Cela signifie pas de cases pré-cochées ou de consentement présumé par le silence. La CJUE (Cour de justice de l'UE) a clarifié que les paramètres de confidentialité ou la simple utilisation du site web ne peuvent pas servir de consentement. Les utilisateurs doivent effectuer une action explicite (cliquer sur « accepter », par exemple). De plus, le consentement doit être aussi facile à retirer qu'à donner ; une option de « refus » doit être disponible sans pénalité (Source: www.cnil.fr) (Source: www.mishcon.com).

Les bannières de cookies échouent souvent à ces tests par conception : des chercheurs ont constaté que de nombreux sites pré-cochent « tout accepter » par défaut ou utilisent des « dark patterns » pour inciter à l'acceptation. Une étude à grande échelle a révélé que **54 %** des sites web testés violaient la loi — par exemple, en ne laissant aucun véritable choix aux utilisateurs. Plus précisément, ils ont découvert des dizaines de sites qui enregistraient un « consentement positif » même lorsque l'utilisateur ne faisait rien, et beaucoup qui n'offraient pas d'option de désinscription directe (Source: arxiv.org). Une autre enquête menée sur 7 500 sites web en Grèce et au Royaume-Uni a révélé que moins de la moitié d'entre eux affichaient même un avis sur les cookies, bien que la plupart plaçaient des cookies de suivi (Source: arxiv.org).

Les régulateurs insistent parfois sur les exigences de forme. Par exemple, le Digital Clearing House de l'autorité irlandaise des données a noté que les bannières sont illégales si elles omettent un bouton « non » clair ou biaisent autrement le consentement (Source: www.mishcon.com). En 2023, le Commissaire de l'ICO britannique a averti les entreprises : ne pas offrir une option simple « tout refuser » sur votre bannière est une violation de la loi, et l'ICO la poursuivrait (bien qu'avec des étapes intermédiaires avant d'infliger des amendes) (Source: www.mishcon.com). De même, le Groupe de travail Article 29 de l'UE et, plus tard, le Comité européen de la protection des données ont publié des lignes directrices soulignant que les bannières de cookies ne devraient pas masquer ou obscurcir l'option de désinscription. Le principe est clair : **accepter les cookies doit être un choix positif, et non un par défaut de refus**.

Contexte Mondial : États-Unis et Autres

En revanche, en dehors de l'Europe, le paysage juridique est assez différent. Aux États-Unis, **il n'existe pas de loi fédérale exigeant des bannières de consentement aux cookies**. La réglementation en matière de vie privée est sectorielle et au niveau des États. Le California Consumer Privacy Act (CCPA/CPRA) accorde aux utilisateurs des droits tels que « ne pas vendre mes données », mais il n'impose *pas* explicitement les bannières de cookies ni l'obtention du consentement pour les cookies de suivi courants (Source: cookie-compliance.co). Les lois fédérales comme l'ECPA ou le COPPA restreignent certaines utilisations des données de communication (notamment le COPPA exige le consentement parental pour le suivi des enfants via des cookies) mais n'imposent pas d'exigence générale d'opt-in pour les sites web. Comme le note une FAQ juridique, « en vertu des lois américaines

sur la vie privée, il n'y a pas d'exigence claire pour le consentement aux cookies », bien que les entreprises soient souvent conseillées d'utiliser des bannières volontairement pour éviter les actions de la FTC ou les recours collectifs (Source: cookie-compliance.co).

Certains pays non membres de l'UE ont adopté des lois comportant des éléments de consentement. Par exemple, le PDPA de Singapour et le PIPEDA du Canada exigent un consentement « significatif » pour la collecte de données personnelles, ce qui pourrait inclure les cookies, mais ils manquent de règles détaillées spécifiques aux cookies. Le projet de loi indien sur la protection des données personnelles (pas encore en vigueur) exigerait le consentement pour le traitement des données personnelles, mais les spécificités de mise en œuvre sont en attente. En général, cependant, c'est le **régime ePrivacy/RGPD centré sur l'UE** qui a conduit à l'adoption mondiale du consentement par bannière comme pratique courante – et les lourdes sanctions pour non-conformité que nous voyons aujourd'hui proviennent principalement des régulateurs européens qui appliquent ces lois.

Mécanismes d'Application et Sanctions

Si un opérateur de site web ne parvient pas à présenter une bannière de consentement aux cookies valide (et n'obtient donc pas de consentement légal), les sanctions se présentent généralement sous deux formes principales : les **amendes administratives** en vertu du droit de la protection des données, et les **ordonnances injonctives** ou autres mesures d'exécution. En Europe, les principaux organismes d'application sont les Autorités nationales de protection des données (APD) ou les régulateurs des communications. Dans d'autres régions, l'application peut impliquer des agences de données ou des organismes de protection des consommateurs.

Amendes en vertu des Lois sur la Protection des Données

En vertu du RGPD (et des dispositions miroirs dans les lois nationales), les APD peuvent imposer des amendes substantielles pour les violations. Pour les infractions liées aux cookies, les dispositions pertinentes relèvent généralement de l'Article 83 du RGPD. Les amendes maximales sont échelonnées : les violations des obligations fondamentales de consentement et de transparence (telles que le non-respect des options de désinscription aux cookies) peuvent entraîner des amendes allant jusqu'à **20 millions d'euros ou 4 % du chiffre d'affaires mondial** (le montant le plus élevé étant retenu) (Source: www.reuters.com). Les infractions moins graves peuvent entraîner jusqu'à 10 millions d'euros ou 2 % (par exemple, le non-respect de certaines exigences spécifiques). En pratique, de nombreuses violations des bannières de cookies ont été considérées comme suffisamment graves pour justifier des amendes de plusieurs millions, voire de centaines de millions d'euros.

L'application la plus stricte de l'UE à ce jour est venue de la CNIL française. Fin 2023 et en 2025, la CNIL a imposé des sanctions record à de grandes entreprises pour des violations de cookies. Par exemple, en décembre 2023, la France a infligé à Yahoo une amende de 10 millions d'euros pour ses pratiques en matière de cookies (Source: www.cnil.fr). Et en septembre 2025, la CNIL a infligé **325 millions d'euros** à Google et **150 millions d'euros** à Shein pour ne pas avoir obtenu de consentement valide (Source: www.lemonde.fr) (Source: www.reuters.com). Ces amendes étaient remarquables non seulement par leur montant, mais aussi par leur justification : elles citaient explicitement des défaillances en matière de consentement aux cookies. La CNIL a déclaré que Google avait « contraint » les utilisateurs à accepter les cookies (un « mur de cookies ») lors de la création de comptes, et avait inséré des cookies de suivi dans Gmail sans consentement librement donné (Source: www.lemonde.fr). Shein a été sanctionné pour avoir placé des cookies de suivi même après que les utilisateurs se soient désinscrits, et pour des mécanismes de retrait inadéquats (Source: www.lemonde.fr) (Source: www.reuters.com). Selon la CNIL, les deux entreprises « n'ont pas obtenu le consentement libre et éclairé des utilisateurs » avant le placement des cookies (Source: www.lemonde.fr). Ces cas illustrent l'extrémité du spectre des sanctions – des amendes équivalant à environ 2 à 4 % des revenus des entreprises (Source: www.reuters.com).

D'autres APD européennes ont émis des amendes ou des ordonnances de moindre envergure. Par exemple, en Belgique, l'Autorité de protection des données a infligé au groupe de presse Roularta une amende de **50 000 €** (environ 2 % de la sanction demandée pour la conformité de soutien aux consommateurs) pour des violations du consentement aux cookies (Source: iapp.org). L'APD a constaté que Roularta ne remplissait pas les conditions d'obtention du consentement de l'utilisateur (elle stockait simplement des cookies de suivi sans opt-in clair). Bien que plus petite en termes absolus, cette amende (imposée en mai 2022) reflète l'application par la Belgique des règles du RGPD : il ne s'agissait pas d'une sanction pénale mais d'une amende administrative en vertu du droit de la protection des données.

Les amendes potentielles varient d'un État membre de l'UE à l'autre, selon la manière dont le droit national transpose le RGPD. En France, par exemple, l'article 82 de la Loi Informatique et Libertés aborde spécifiquement les « cookies publicitaires » et permet à la CNIL d'imposer des sanctions en cas d'utilisation abusive (comme vu ci-dessus) (Source: www.cnil.fr). Au Royaume-Uni, des violations similaires relèvent des Privacy and Electronic Communications Regulations (PECR) et du RGPD britannique. Historiquement, les infractions aux PECR pouvaient être poursuivies ou sanctionnées d'une amende allant jusqu'à 500 000 £, mais de nos jours, le régime d'amendes de l'ICO suit les niveaux du RGPD (jusqu'à 17,5 millions de £ / 4 % pour les infractions les plus graves). Aucune amende importante liée aux cookies n'a encore été annoncée publiquement par l'ICO, mais fin 2023, l'ICO a averti les grandes entreprises britanniques dont les bannières n'étaient pas conformes de les corriger sous peine de mesures d'exécution (Source: syrenis.com) (Source: www.mishcon.com) (plus de détails ci-dessous).

Astreintes et injonctions de conformité

Outre les amendes uniques, les régulateurs utilisent souvent des **astreintes** pour assurer la conformité future. Notamment, dans l'affaire CNIL contre Google, le régime d'amendes incluait une injonction selon laquelle Google devait corriger ses pratiques dans un délai de six mois, sous peine d'une **amende de 100 000 € par jour** (Source: www.cnil.fr). La décision officielle de la CNIL (sept. 2025) a explicitement stipulé que si Google n'implémentait pas les mesures requises (cesser d'injecter des publicités et assurer un consentement valide aux cookies) dans le délai imparti, elle encourrait cette astreinte journalière (Source: www.cnil.fr). Ce mécanisme d'« astreinte » (amende judiciaire) est une sanction forte pour garantir que les entreprises corrigent effectivement leurs bannières rapidement.

Les autorités belges ont également assorti leurs décisions d'astreintes journalières. En 2024, l'APD belge a ordonné à quatre grands sites d'information (exploités par Mediahuis) d'ajouter un bouton « refuser » clair à leurs bannières et de corriger les choix de conception trompeurs. L'ordonnance était assortie d'une pénalité de **50 000 € par jour et par site web** en cas de non-conformité quotidienne (Source: noyb.eu). En d'autres termes, si l'un de ces sites n'implémentait pas les changements requis à temps, l'éditeur devrait 50 000 € pour chaque jour de retard et pour chaque site (Source: noyb.eu). C'est l'une des menaces d'« amende journalière » les plus élevées observées dans l'application des règles relatives aux cookies, et cela souligne la gravité avec laquelle les régulateurs considèrent le refus de consentement.

D'autres régulateurs de l'UE ont utilisé des outils similaires. Par exemple, dans le cadre du règlement belge mentionné ci-dessus, une petite « amende » de 10 000 € était essentiellement un paiement initial pour éviter d'imposer la conformité, illustrant que même des sommes symboliques peuvent être utilisées comme moyen de dissuasion (bien que cette résolution ait été largement critiquée par les activistes comme étant trop clémente (Source: noyb.eu). Les régulateurs peuvent également suspendre le traitement ou ordonner des interdictions temporaires sur certains cookies jusqu'à ce que les mécanismes de consentement soient corrigés, bien que ces détails ne soient pas toujours explicitement rendus publics.

Études de cas sur l'application des règles

Nous passons maintenant en revue des cas représentatifs et des annonces réglementaires qui illustrent la manifestation de ces sanctions.

- **France/CNIL (Géants bleus et rouges)** – Les exemples les plus frappants proviennent de la CNIL. En janvier 2024, la CNIL a infligé à Yahoo! une amende de **10 millions d'euros** pour ne pas avoir respecté les préférences des utilisateurs en matière de cookies (Source: www.cnil.fr). La CNIL avait reçu des dizaines de plaintes selon lesquelles Yahoo laissait des cookies de suivi actifs même lorsque les utilisateurs avaient refusé, et rendait très difficile le retrait du consentement par la suite. Plus récemment, en septembre 2025, la CNIL a annoncé des amendes de **325 millions d'euros** et **150 millions d'euros** contre Alphabet/Google et Shein, respectivement (Source: www.lemonde.fr) (Source: www.cnil.fr). Ces deux sanctions concernaient explicitement des violations liées aux cookies. Pour Google, la CNIL a cité « l'insertion de publicités dans Gmail » et le fait de « contraindre les utilisateurs » à accepter les cookies via un mur de cookies (Source: www.cnil.fr) (Source: www.techradar.com). Pour Shein, elle a relevé le dépôt de cookies sans consentement et l'ignorance des choix des utilisateurs (Source: www.cnil.fr) (Source: www.reuters.com). Ces amendes illustrent que les grandes entreprises mondiales peuvent faire face au **plafond des amendes du RGPD** pour quelque chose d'aussi apparemment anodin que les bannières de cookies, lorsque le consentement est manifestement négligé. (L'amende de Google représentait une petite fraction de ses revenus mais était justifiée par

l'impact élevé sur les utilisateurs et les manquements répétés à la conformité ; celle de Shein représentait environ 2 % de son chiffre d'affaires dans l'UE (Source: www.reuters.com).) La CNIL a également ordonné aux deux entreprises de cesser les pratiques identifiées dans un délai de six mois, sous peine d'astreintes journalières supplémentaires (Source: www.cnil.fr).

- **Belgique/APD (Mediahuis et Roularta)** – Mi-2022, l'APD belge a infligé une amende de **50 000 €** à Roularta (Source: iapp.org) pour avoir placé des cookies de suivi sans consentement valide sur deux de ses sites web. L'APD a noté que Roularta « ne remplissait pas les conditions de recueil du consentement des utilisateurs pour le placement de cookies » en vertu des dispositions du RGPD (Source: iapp.org). Cette amende, bien que modeste, montre que même un éditeur de presse national ne peut ignorer les règles de consentement. Plus récemment (sept. 2024), suite à des plaintes de l'ONG de protection de la vie privée NOYB, l'autorité belge a ordonné à quatre grands médias (faisant partie du groupe Mediahuis) d'implémenter un bouton de refus bien visible sur les bannières de cookies (Source: noyb.eu). Ces sites ont été critiqués pour des conceptions de bannières « trompeuses ». L'ordonnance a explicitement averti de sanctions de **50 000 € par jour** en cas de non-conformité persistante (Source: noyb.eu). (Il est à noter qu'un traitement antérieur avait permis à ces sites de payer des règlements de 10 000 € sans modifier leurs bannières – un résultat que NOYB a fustigé comme leur permettant de « s'acheter une exemption du RGPD » (Source: noyb.eu).)

- **Pays-Bas/Autoriteit Persoonsgegevens (AP)** – En avril 2025, l'APD néerlandaise a signalé une vaste campagne d'application des règles. Elle a envoyé des **lettres d'avertissement** à plus de 50 organisations (détaillants, médias, assureurs) à travers les Pays-Bas, indiquant que leurs bannières de cookies étaient trompeuses ou qu'elles plaçaient des cookies de suivi sans consentement (Source: www.hoganlovells.com). Ces lettres donnaient aux entreprises trois mois pour corriger leurs pratiques ou risquer des enquêtes formelles et des amendes (Source: www.hoganlovells.com). Bien qu'aucune amende spécifique n'ait encore été annoncée, la communication de l'APD néerlandaise a souligné qu'elle traitait les violations avec sérieux et pouvait imposer des amendes administratives pour les infractions à la loi néerlandaise sur les télécommunications (qui met en œuvre les règles ePrivacy de l'UE) et aux règles parallèles du RGPD (Source: www.hoganlovells.com). Les analystes juridiques ont noté que cela fait partie d'une campagne financée visant à appliquer plus vigoureusement les règles relatives aux cookies aux Pays-Bas. (L'AP a souligné que les cookies utilisés à des fins de marketing ne sont légaux qu'avec un consentement préalable, et que les entreprises qui ne se conforment pas s'exposent à toute la panoplie des sanctions prévues par le RGPD et ePrivacy.)

- **Royaume-Uni/ICO** – Le Commissaire à l'information du Royaume-Uni s'est jusqu'à présent montré relativement prudent en ce qui concerne les amendes directes pour les cookies. Cependant, mi-2023, l'ICO a publiquement averti les entreprises que les bannières non conformes ne seraient pas tolérées (Source: www.mishcon.com). Le Commissaire adjoint Stephen Bonner a explicitement déclaré que l'absence d'une option claire « tout refuser » constitue une violation de la loi britannique (PECR), et qu'il n'y a « aucune excuse » à la non-conformité (Source: www.mishcon.com). L'ICO a également indiqué qu'elle pourrait adopter une approche progressive (« étapes d'intervention ») avant de passer aux amendes. Notamment, en novembre 2023, des rapports ont fait état de l'envoi par l'ICO d'avis officiels à plusieurs des plus grands sites web du Royaume-Uni (y compris des entreprises de médias et de technologie) exigeant des améliorations de leurs bannières dans les 30 jours, sous peine de mesures d'exécution (Source: syrenis.com). Bien que ces affaires n'aient pas encore donné lieu à des amendes publiques, les commentateurs juridiques observent que l'application des règles par l'ICO (autrefois considérée comme laxiste) s'intensifie ; en effet, un blog juridique exhorte les entreprises à anticiper que l'ICO commencera à émettre des amendes plutôt que de simples conseils (Source: www.dataprotectionlawhub.com). (De récentes propositions législatives britanniques augmentent même les enjeux : le prochain projet de loi sur la protection des données et l'information numérique autoriserait des amendes beaucoup plus importantes en vertu des PECR, s'alignant sur les niveaux supérieurs du RGPD (Source: www.mishcon.com).)

- **Autres APD de l'UE** – Plusieurs autres autorités européennes ont prononcé des sanctions liées aux cookies ces dernières années. Par exemple, en Italie, le Garante a abordé la conception des cookies dans ses lignes directrices et a lancé des enquêtes, bien que les amendes importantes spécifiquement pour les bannières aient été moins médiatisées. En Allemagne, des associations de consommateurs ont poursuivi de grands éditeurs en justice pour la conception de leurs bannières (par exemple, l'affaire « Focus Online » a jugé sa bannière invalide, ce qui signifie que le consentement n'avait pas été légalement obtenu (Source: blog.eprivacy.eu) (Source: blog.eprivacy.eu). L'APD espagnole a infligé des amendes à des dizaines de sites web par le passé pour manque de consentement ou bannières cachées (pour des totaux à cinq chiffres, selon les rapports). Le DSB autrichien a également examiné le consentement aux cookies, émettant des ordres pour corriger les bannières trompeuses. Le point essentiel est que, dans toute l'UE, presque toutes les APD traitent désormais le consentement aux cookies comme un élément central de la conformité en matière de vie privée : les violations sont passibles d'amendes administratives et d'injonctions de conformité.

- **États-Unis (Recours collectifs et examen de la FTC)** – Encore une fois, il est important de noter qu'il n'existe pas de *loi fédérale sur les cookies* aux États-Unis. Cependant, les entreprises ciblant des utilisateurs de l'UE ou utilisant des normes de type RGPD peuvent toujours courir des risques si elles appliquent une politique de confidentialité à large portée et déclarent ainsi leur conformité au RGPD/CCPA partout. Séparément, les procureurs généraux de certains États ou la Federal Trade Commission (FTC) pourraient éventuellement contester les entreprises pour pratiques de confidentialité trompeuses si une bannière de cookies est fallacieuse (en tant que pratique déloyale ou trompeuse), mais de tels cas ne sont pas prédominants. Les principales « sanctions » américaines liées aux cookies sont apparues sous la forme de **recours collectifs** en vertu de diverses théories de la responsabilité civile et de la protection des consommateurs (atteinte à la vie privée, pratiques commerciales déloyales, etc.). Récemment, des cabinets d'avocats américains ont lancé de nombreux recours collectifs liés aux cookies, alléguant généralement que les bannières ou les politiques des sites web induisent les consommateurs en erreur. Ces poursuites peuvent aboutir à des règlements monétaires (souvent de quelques millions), mais leur viabilité ultime n'a pas encore été testée par les tribunaux (Source: ipwatchdog.com). Contrairement aux amendes du RGPD, ces recours collectifs sont généralement beaucoup plus modestes au total – et le gouvernement américain lui-même n'a pas imposé de grosses amendes uniquement pour les bannières de cookies en 2025.

En résumé, les **sanctions pour l'absence ou la mauvaise configuration d'une bannière de consentement aux cookies** peuvent être sévères, en particulier en Europe. Au minimum, un site web non conforme pourrait recevoir l'ordre de corriger sa bannière ou de cesser d'utiliser des cookies, et s'il ne le fait pas, il peut encourir des astreintes journalières. Dans le pire des cas, les APD ont démontré qu'elles utiliseront l'étendue de leurs pouvoirs d'amende (jusqu'à 2 à 4 % du chiffre d'affaires) lorsque la violation est flagrante et généralisée (Source: www.reuters.com) (Source: www.cnil.fr). Nous présentons un tableau des cas notables ci-dessous :

PAYS / RÉGULATEUR	ANNÉE	ENTITÉ (ENTREPRISE/ORGANISATION)	SANCTION/ACTION	VIOLATION
France (CNIL)	2025	Google (Alphabet)	Amende de 325 millions d'euros ; injonction de conformité de 6 mois ; astreinte de 100 000 €/jour si non corrigé (Source: www.cnil.fr) (Source: www.cnil.fr)	Insertion de publicités et placement de cookies de suivi sans consentement valide (« mur de cookies » coercitif) (Source: www.lemonde.fr) (Source: www.techradar.com).
France (CNIL)	2025	Shein (Infinite Styles Services)	Amende de 150 millions d'euros (Source: www.cnil.fr)	Placement de cookies publicitaires sans consentement, ignorance des refus (Source: www.reuters.com) (Source: www.cnil.fr).
France (CNIL)	2023	Yahoo! (Yahoo EMEA)	Amende de 10 millions d'euros (Source: www.cnil.fr)	Ignorance du refus des cookies par les utilisateurs sur yahoo.com et Yahoo Mail (consentement non respecté) (Source: www.cnil.fr).

| Belgique (APD) | 2024 | Mediahuis (éditeur de 4 titres) | Ordre de corriger les bannières (ajouter « refuser ») ; pénalité de 50 000 €/jour en cas de non-conformité (Source: noyb.eu) | Utilisation de bannières de cookies trompeuses sans option de refus claire (Source: noyb.eu). | | Belgique (APD) | 2022 | Groupe de presse Roularta | Amende de 50 000 € (Source: iapp.org) | Non-respect des exigences de consentement lors du placement de cookies sur les sites web (Source: iapp.org). | | Pays-Bas (AP) | 2025 | 50 entreprises (détaillants, médias, etc.) | Lettres d'avertissement ; délai de 3 mois pour se conformer ou faire face à des amendes (Source: www.hoganlovells.com) | Bannières de cookies trompeuses ou placement de cookies de suivi sans consentement valide (Source: www.hoganlovells.com). | | Royaume-Uni (ICO) | 2023 | Divers sites de premier plan (actualités, technologie) | Mises en

demeure émises ; 30 jours pour se conformer ou faire face à des mesures d'exécution (Source: syrenis.com) | Bannières de cookies sans options claires (« tout refuser ») en violation du PECR/RGPD (Source: syrenis.com) (Source: www.mishcon.com). | | Juridictions à l'échelle de l'UE (variables) | 2023–24 | Divers sites web | Ordres de conformité par les APD ; petites amendes ou engagements | Utilisation de « dark patterns » ; blocage du contenu sauf acceptation (« murs de cookies ») ; informations insuffisantes. | | *(À titre de comparaison)* États-Unis† | — | — | Pas d'amende fédérale pour les cookies ; réglementations d'opt-out CCPA ; avertissements possibles de la FTC | Pas de mandat de consentement explicite ; poursuites en matière de vie privée en responsabilité délictuelle (actions collectives) observées. | † Aux États-Unis, l'application est régie par les lois étatiques sur la protection de la vie privée et la FTC plutôt que par un régime de sanctions de type européen (Source: cookie-compliance.co).

Preuves et analyse des données

Taux de conformité et études

De nombreuses études ont documenté une non-conformité généralisée aux règles de consentement aux cookies :

- **Enquêtes académiques** : Kampanos & Shahandashti (2021) ont systématiquement interrogé 17 000 sites web en Grèce et au Royaume-Uni et ont constaté que, bien qu'environ 60 % des sites émettent des cookies de suivi tiers, *moins de 50 %* affichaient une notification de cookies (Source: arxiv.org). Même parmi ceux qui avaient des bannières, la majorité incitait les utilisateurs à « accepter » ou rendait le refus plus difficile, très peu offrant une option de refus simple (Source: arxiv.org). Cela suggère qu'une grande partie des sites enfreignent simplement la loi en n'informant pas du tout les utilisateurs. Une autre étude de Matte et al. (2019) a exploré près de 23 000 sites européens utilisant le cadre IAB TCF et a trouvé au moins une violation légale sur *54 % des sites* testés (Source: arxiv.org). Les infractions courantes comprenaient des cases de consentement pré-cochées et le non-respect d'une sélection de refus (environ 27 sites ont même stocké un consentement positif après un refus explicite) (Source: arxiv.org). Ces résultats indiquent qu'une majorité de sites, du moins dans les populations échantillonnées, ne respectaient pas correctement les exigences de consentement.

- **Outils de détection automatisée** : Des chercheurs ont développé des outils (par exemple, « Cookiescanner » (Source: arxiv.org) pour détecter et évaluer les bannières de cookies à grande échelle. Leurs conclusions confirment que de nombreuses bannières sont mal implémentées. Gundelach & Herrmann (2023) notent que « de nombreux opérateurs de sites web ne respectent pas la loi et suivent les utilisateurs avant toute interaction avec l'avis de consentement, ou tentent de tromper les utilisateurs pour obtenir leur consentement par le biais de « dark patterns » » (Source: arxiv.org). Cette étude a scanné les 10 000 principaux sites web et a constaté que les filtres manuels manquaient souvent des bannières (suggérant que le problème est généralisé) et que la détection automatique des boutons « refuser » reste difficile. Globalement, une analyse spécialisée a révélé de nombreux cas où les bannières ne proposaient pas d'option de refus ou peinaient à accorder un poids égal aux choix de refus/acceptation (Source: arxiv.org). Ces analyses systématiques fournissent un soutien empirique aux actions d'exécution : les régulateurs avaient anticipé que la conformité serait laxiste, et les données montrent qu'en effet plus de la moitié des sites présentaient un problème de bannière.

- **Plaintes en matière de vie privée et attention réglementaire** : Les agences de régulation elles-mêmes rapportent que l'application est **motivée par les plaintes**. Par exemple, un blog de cabinet d'avocats spécialisé dans la protection de la vie privée résume que l'attention accrue de l'ICO en 2023 a été déclenchée en partie par « l'augmentation des plaintes des personnes concernées » et des campagnes de sensibilisation (Source: www.dataprotectionlawhub.com). Les enquêtes auprès des citoyens soutiennent également le besoin de transparence : une consultation publique de l'UE a révélé que plus de 96 % des répondants souhaitent être interrogés avant que des cookies tiers ne soient utilisés sur leur appareil. En bref, la pression publique ascendante et les changements politiques descendants (comme le projet de règlement ePrivacy) convergent vers un consensus selon lequel le consentement aux cookies doit être pris au sérieux.

Statistiques des amendes

Bien qu'il n'existe pas de répertoire centralisé de toutes les amendes liées aux cookies, les exemples connus permettent une certaine quantification :

- **Ampleur** : Les amendes imposées par les APD pour les violations de cookies ont varié de dizaines de milliers à des centaines de millions d'euros. Outre Google/Shein (centaines de M€) et Yahoo (10 M€), de nombreuses amendes entre 2019 et 2023 se situaient dans la fourchette des centaines de milliers d'euros. Par exemple, les amendes antérieures de la CNIL comprenaient

150 000 € à 200 000 € contre des sites plus petits. Les décisions françaises commencent souvent autour de 100 000 à 150 000 € pour les sites de taille moyenne (Source: www.cnil.fr). De même en Italie et en Espagne, des amendes d'environ 100 000 € ont été signalées pour les primo-délinquants ou les contrevenants de taille moyenne. L'amende de 50 000 € infligée à Roularta en Belgique était dans la fourchette basse mais restait significative pour un éditeur de taille moyenne (Source: iapp.org).

- **Pourcentage du chiffre d'affaires** : Dans les cas importants, les amendes approchent les limites légales. Notamment, la CNIL a présenté les amendes Google/Shein comme représentant **environ 2 % du chiffre d'affaires européen** (Source: www.reuters.com). (Shein a explicitement noté que ses amendes correspondaient à environ 2 % de son chiffre d'affaires de 2023 dans l'UE (Source: www.reuters.com).) Cela suggère que les APD sont en effet enclines à appliquer la tranche maximale pour les violations flagrantes du consentement par les acteurs majeurs. Les petites organisations reçoivent généralement des amendes absolues relativement plus faibles, mais toujours proportionnelles à leur taille en vertu du mandat du RGPD « effectif, proportionné et dissuasif ».

- **Données agrégées** : L'application des règles relatives aux cookies ne s'étant intensifiée qu'au cours des dernières années, des données systématiques pourraient apparaître plus tard. Cependant, les avis réglementaires et les communiqués de presse indiquent que l'*inactivité de l'ère COVID* (2019-2020) a cédé la place à une multitude de cas entre 2021 et 2025. Par exemple, la CNIL française avait un plan d'action de « répression des cookies » à partir de 2019, et en 2022-2023, elle imposait des amendes presque mensuellement (d'autant plus que son délai légal exigeait que les sites majeurs se conforment d'ici septembre 2020 (Source: www.cnil.fr). Au Royaume-Uni, les actions de l'ICO restent plus consultatives, mais les feuilles de calcul des avis PECR montrent une augmentation des cas liés aux cookies enregistrés en 2023-24. La tendance générale est claire : **l'application de la loi augmente fortement**, et les sanctions s'intensifient.

CATÉGORIE	EXEMPLES / DONNÉES
Études de conformité académiques	Kampanos & Shahandashti ont constaté que <50 % des sites affichent une notification de cookies, même si >60 % utilisent des cookies tiers (Source: arxiv.org). Matte et al. ont constaté qu'environ 54 % des sites testés violaient les exigences de consentement (Source: arxiv.org). Ces études à grande échelle confirment des taux de non-conformité élevés.
Amendes majeures (UE)	Amendes CNIL : Google 325 M€, Shein 150 M€ (2025) (Source: www.lemonde.fr) (Source: www.cnil.fr) ; Yahoo 10 M€ (2023) (Source: www.cnil.fr) ; nombreuses amendes plus petites (à 5-6 chiffres) à d'autres. APD belge : Roularta 50 k€ (2022) (Source: iapp.org). (Les amendes atteignent souvent ~2–4 % du chiffre d'affaires (Source: www.reuters.com).)
Tendances en matière d'application	La CNIL a annoncé des dizaines d'ordres de conformité pour les sites. L'AP néerlandaise a émis des avertissements à 50 entreprises (2025) (Source: www.hoganlovells.com). L'ICO britannique a envoyé des avis aux principaux sites (2023) (Source: syrenis.com). L'ONG de protection de la vie privée NOYB a déposé environ 500 plaintes dans l'UE ciblant les bannières (Source: www.sovy.com).
Mécanismes de sanction	Les APD utilisent : des amendes uniques, des **amendes journalières** (par exemple, Google : 100 000 €/jour (Source: www.cnil.fr) ; actualités belges : 50 000 €/jour (Source: noyb.eu), injonctions/ordres de correction. Les règlements (par exemple, les médias belges ont payé 10 000 € chacun au lieu de se conformer (Source: noyb.eu) soulignent la créativité de l'application.

Études de cas et exemples

Pour illustrer la manière dont la loi est appliquée, nous décrivons quelques exemples détaillés d'actions réglementaires :

- **Google (France, 2025)** : L'action d'exécution la plus médiatisée a sans doute concerné Google. Le 1er septembre 2025, la CNIL a annoncé une amende de 325 M€ (Source: www.cnil.fr). L'enquête a été déclenchée par une plainte de NOYB ; les inspecteurs de la CNIL ont examiné le service Gmail de Google et le processus d'inscription aux comptes (Source: www.cnil.fr) (Source: www.cnil.fr). Les conclusions étaient frappantes : Google insérait des publicités dans les boîtes de réception Gmail, déguisées en e-mails personnels, mais plus pertinent ici était la manière dont il gérait les cookies. La CNIL a reproché à Google d'avoir « contraint » les utilisateurs à accepter des cookies de suivi (un « mur de cookies ») lors de la création de comptes, et

que l'interface de Gmail incitait les utilisateurs au consentement (Source: www.techradar.com) (Source: www.cnil.fr). En bref, la bannière/le design privait les utilisateurs de leur libre choix. En imposant l'amende, la CNIL a cité la négligence répétée (Google avait déjà été condamné pour des problèmes similaires en 2020 et 2021), l'ampleur des utilisateurs affectés (plus de 74 millions) et les revenus élevés de Google. Il est important de noter que les sanctions comprenaient une injonction à Google de mettre en œuvre les changements nécessaires dans un délai de six mois ; à défaut, Google s'expose à une pénalité supplémentaire de 100 000 € par jour (Source: www.cnil.fr). Google a répondu publiquement en s'engageant à apporter des modifications aux analyses, soulignant que seule une petite fraction des utilisateurs voit des « publicités » dans Gmail. (Cette affaire souligne que même la plus grande entreprise technologique n'est pas à l'abri : le respect des règles de consentement est obligatoire quelle que soit la taille de l'entreprise.)

- **Shein (France, 2025)** : Dans la même annonce, la CNIL a infligé une amende de 150 M€ à la filiale européenne de Shein (Source: www.cnil.fr). Shein est un détaillant de mode rapide en ligne ciblant les consommateurs français (environ 12 millions de visiteurs mensuels en France, selon la CNIL). Une inspection du site web en 2023 a révélé des violations généralisées : Shein plaçait des cookies de suivi sur les appareils des visiteurs *sans leur consentement*. Les utilisateurs qui refusaient étaient ignorés, et la bannière ne permettait pas un retrait facile du consentement (Source: www.reuters.com) (Source: www.cnil.fr). Les régulateurs ont spécifiquement mentionné « le placement de certains cookies sans le consentement des internautes, en ne respectant pas leurs choix et en ne les informant pas correctement » (Source: www.cnil.fr). Shein a contesté l'amende comme étant disproportionnée et politiquement motivée (arguant qu'elle avait depuis corrigé ses pratiques et que son modèle commercial dépendant de la publicité avait été injustement ciblé) (Source: www.reuters.com). Les frais correspondaient à environ 2 % du chiffre d'affaires de Shein pour l'exercice 2023 en Europe (Source: www.reuters.com). Shein a indiqué qu'elle ferait appel, mais l'amende envoie un message fort : les grands acteurs du commerce électronique sont soumis à un examen minutieux en matière de conformité au consentement, tout comme les plateformes technologiques.

- **Yahoo (France, 2023)** : Avant les décisions concernant Google/Shein, la CNIL avait déjà démontré sa volonté de sanctionner les grands acteurs pour des manquements liés aux cookies. Le 29 décembre 2023, la CNIL a infligé une amende de 10 millions d'euros à Yahoo EMEA (Source: www.cnil.fr). Selon ses propres déclarations, Yahoo n'avait pas "respecté le choix des internautes qui refusaient les cookies sur son site web 'Yahoo.com'" et avait rendu impossible le retrait du consentement sur Yahoo Mail (Source: www.cnil.fr). L'amende faisait suite à des dizaines de plaintes d'utilisateurs. Encore une fois, le problème était essentiellement que les sites de Yahoo continuaient à déposer des cookies de suivi même après un refus, et que les utilisateurs étaient contraints au consentement par des astuces d'expérience utilisateur. La CNIL a noté qu'elle avait émis une mise en demeure dès 2020, mais que les problèmes persistaient. L'amende de 10 millions d'euros était notable en tant que cas rare contre une grande marque technologique américaine (Yahoo fait désormais partie d'Apollo), et elle a démontré que les anciennes obligations conservaient leur poids. Yahoo a affirmé s'être conformé fin 2023, mais avait échoué auparavant. La sanction a contraint Yahoo à retravailler ses bannières pour donner un poids égal au bouton "refuser".

- **Mediahuis (Belgique, 2024)** : En septembre 2024, suite à des plaintes de NOYB, l'APD belge (Commission de la Protection de la Vie Privée) a rendu des décisions contre l'éditeur Mediahuis (qui exploite des sites d'information tels que De Standaard, Het Nieuwsblad). L'APD a ordonné à chaque site d'ajouter un bouton "refuser" clairement étiqueté dans la première couche de la bannière de cookies et de supprimer tout codage couleur trompeur (par exemple, rendre "refuser" gris sur fond gris) (Source: noyb.eu). Auparavant, NOYB avait accusé ces sites d'utiliser des bannières illégales pendant des années, mais les autorités s'étaient précédemment contentées d'accepter un simple paiement de 10 000 € de Mediahuis – sans aucune correction de conformité (Source: noyb.eu). Sous pression, l'APD a fait marche arrière et a imposé des conditions strictes : "Si Mediahuis ne se conforme pas, il s'expose à une pénalité de 50 000 € par jour et par site web" (Source: noyb.eu). Cela a créé une puissante incitation à redessiner les bannières. Ce cas met en évidence moins l'amende monétaire (l'ordonnance elle-même n'avait pas de somme punitive fixe, juste la menace de 50 000 €/jour), mais le **levier d'application spectaculaire** donné aux régulateurs.

- **Roularta (Belgique, 2022)** : Comme exemple belge antérieur, en mai 2022, l'APD a infligé une amende de 50 000 € à Roularta (Source: iapp.org). Roularta (propriétaire de magazines et de sites web) n'avait pas obtenu de consentement valide pour les cookies, comme l'exigent le RGPD/ePrivacy. La Chambre Contentieuse de l'APD a explicitement déclaré que Roularta "ne remplissait pas les conditions de collecte du consentement des utilisateurs" pour les cookies (Source: iapp.org). Bien que 50 000 € soient une petite somme pour un groupe de presse (bien que probablement un pourcentage significatif de leurs revenus publicitaires sur ces sites), il s'agissait d'une mesure d'application de la protection des données – et l'APD a averti les autres que de nouvelles plaintes pourraient entraîner des amendes plus importantes. Ce cas souligne que même les entreprises de médias traditionnels doivent respecter les règles de consentement numérique.

Dans chacun de ces exemples, l'**absence ou l'insuffisance d'une bannière de cookies** était le nœud de la violation. Les sanctions allaient des ordres de conformité et des amendes relativement modestes (Belgique, 50 000 €) à des amendes record (France, 325 millions d'euros). Les organisations sanctionnées comprenaient souvent un mélange d'entreprises nationales et internationales – et dans de nombreux cas, les actions en justice étaient motivées par la juridiction de l'UE (par exemple, les infractions de Google et Shein ont été examinées en vertu du droit français parce que ces entreprises ciblaient le marché français).

Perspectives Multiples et Contexte

En examinant la question des sanctions, il est important de reconnaître plusieurs points de vue :

- **Perspective des régulateurs** : Les autorités de protection des données (APD) considèrent le consentement aux cookies comme une base essentielle de la vie privée. Elles soulignent que l'autonomie de l'utilisateur en matière de suivi est non négociable. Les lourdes amendes en France et ailleurs envoient un message dissuasif selon lequel même les grands acteurs ne peuvent pas bafouer les règles de consentement. Les APD soulignent également que le consentement aux cookies est souvent la "première étape" vers une conformité RGPD complète : ignorer les bannières est souvent corrélé à d'autres abus de données. Par exemple, la CNIL française a imposé des amendes pour les cookies dans le cadre d'une campagne plus large sur la non-conformité au suivi (Source: www.cnil.fr). Les régulateurs ont ouvertement averti les entreprises : "aucune excuse" n'existe pour ne pas offrir une option de refus appropriée (Source: www.mishcon.com). Ils reconnaissent également les plaintes des utilisateurs – les APD notent le flot de plaintes concernant les bannières comme justification de leur action. Comme l'a résumé un expert, les régulateurs européens ont réagi à la "colère" des utilisateurs face aux bannières persistantes ou trompeuses en sévir (des étiquettes comme "clickspamageddon" reflètent le sentiment public). Dans les directives réglementaires, l'accent est mis sur la transparence et la facilité de refus : refuser les cookies doit être "tout aussi facile" que les accepter (Source: www.cnil.fr).

- **Perspective des entreprises** : Du côté des entreprises, les opinions varient. De nombreuses entreprises acceptent à contrecœur les bannières de cookies comme une nécessité légale, bien qu'elles les considèrent souvent comme un fardeau pour l'expérience utilisateur et une barrière au marketing basé sur les données. Certains dirigeants se sont publiquement plaints que les règles dégradent l'expérience utilisateur, provoquent une fatigue des bannières et entravent la publicité en ligne. En effet, des groupes professionnels en Europe ont fait pression pour des règles plus souples (par exemple, exempter les cookies d'analyse du consentement, ou les autoriser par défaut). Par exemple, le projet de loi britannique sur la réforme des données proposait que les cookies d'analyse soient "autorisés sans consentement", reflétant la pression de l'industrie pour réduire les exigences des bannières (bien que les critiques affirment que cela sape le choix de l'utilisateur) (Source: www.mishcon.com). De nombreux sites utilisent des solutions de bannières fournies par des plateformes de gestion du consentement (CMP), et les blogs de l'industrie discutent fréquemment des "taux de consentement" et des moyens de maximiser les opt-ins. Néanmoins, le point de vue dominant des entreprises est que la conformité est obligatoire : après les amendes de Google/Shein, les entreprises ayant un trafic européen voudront des flux de consentement robustes pour éviter un sort similaire. Certaines entreprises se plaignent que les régulateurs accordent un avantage injuste aux concurrents locaux qui se conforment, par exemple Shein qualifiant son amende de "politiquement motivée" parce qu'elle est en concurrence avec des détaillants français (Source: www.reuters.com). Mais finalement, l'avis est qu'ignorer les bannières risque des amendes et des atteintes à la réputation.

- **Perspective des consommateurs/défenseurs de la vie privée** : Les activistes de la vie privée et de nombreux consommateurs considèrent les bannières de cookies elles-mêmes avec ambivalence ou agacement, mais soutiennent généralement le concept selon lequel le consentement doit être significatif. Des organisations comme NOYB se concentrent sur le fait que ces bannières respectent réellement l'autonomie de l'utilisateur. Elles condamnent les "murs de cookies" du type "à prendre ou à laisser" et les boutons de désinscription cachés. Le slogan de la campagne de NOYB faisait référence à la "terreur des bannières de cookies" et a déjà entraîné des centaines de plaintes (Source: www.sovy.com) (Source: noyb.eu). Les ONG de défense de la vie privée soutiennent que l'utilisation de "dark patterns" par les entreprises sape l'intention de la loi. Une position militante courante est que toute barrière au service si les cookies sont refusés (un mur de cookies "dur") ne constitue jamais un consentement valide. Cette perspective pousse à une application stricte et a influencé l'application par la CNIL des murs de cookies comme des violations de la protection des données (Source: www.lemonde.fr). Du côté des utilisateurs, les preuves montrent que la plupart des gens cliquent simplement sur "accepter" juste pour se débarrasser de l'avis, suggérant que les avis de consentement ne servent de toute façon pas beaucoup la vie privée. Néanmoins, les défenseurs soutiennent que le cadre juridique doit imposer une meilleure conception : comme l'a dit une légende de procès, "les utilisateurs devraient

avoir une option claire, oui ou non" (Source: www.sovy.com). NOYB et d'autres ont explicitement déclaré qu'ils considéraient les amendes comme le règlement de Mediahuis (10 000 €, pas de changements) comme inacceptables ; ils veulent un véritable changement appliqué par les APD (Source: noyb.eu). En bref, du point de vue de la vie privée, la question de la "sanction" est moins une question de montants en dollars que de savoir si l'application conduira *finalement* à une véritable conformité plutôt qu'à des règlements symboliques.

- **Perspective juridique/académique** : Les juristes notent que les lois sur le consentement aux cookies sont techniquement complexes. Par exemple, il y a débat sur la question de savoir si le consentement au suivi pourrait parfois être obtenu sur la base d'un "intérêt légitime" plutôt que d'un opt-in (une opinion rejetée par la plupart des APD). Il y a eu plusieurs affaires judiciaires : le tribunal régional de Munich (Allemagne, 2020-21) a jugé que la bannière d'un site d'information (Focus Online) n'obtenait *pas* un consentement valide car elle ne rendait pas le refus aussi facile que le consentement (Source: blog.eprivacy.eu) (Source: blog.eprivacy.eu). À un niveau supérieur, les universitaires se concentrent sur les tests utilisateurs et les contrôles de conformité automatisés. Ils concluent que l'application est justifiée : par exemple, les recherches de Gundelach et Herrmann indiquent que de nombreux sites suivent les utilisateurs *avant* l'interaction avec la bannière, confirmant que les régulateurs pourraient déjà enquêter sur ces problèmes précis (Source: arxiv.org). Les avocats soulignent également que, comme les amendes de l'article 83 du RGPD sont exprimées en pourcentages maximums, les autorités nationales ont une marge de manœuvre. Les premières affaires de cookies tendaient vers des amendes plus petites, peut-être en raison de la nouveauté de l'application, mais le récent passage à des pénalités de plusieurs millions suggère que les autorités interprètent "efficace, proportionné" comme signifiant "dissuader d'autres entreprises en les frappant fort".

- **Analystes de l'industrie / Perspective future** : Une dernière perspective concerne l'avenir du consentement aux cookies lui-même. Certains experts se demandent maintenant si les bannières de cookies (l'"approche ePrivacy" traditionnelle) sont durables. En effet, les fonctionnaires de la Commission européenne ont reconnu la "fatigue du consentement". Il existe des propositions de refonte de la directive ePrivacy (le soi-disant règlement ePrivacy, en discussion depuis 2017). Un article de presse a rapporté que l'UE prévoit de réviser les règles relatives aux cookies d'ici 2025 à la lumière des plaintes des utilisateurs (le soi-disant "clickspamageddon") (Source: www.tomshardware.com). Les changements potentiels incluent l'exemption des cookies d'analyse ou le développement de signaux de consentement standardisés au niveau du navigateur. Le résultat pourrait modifier les sanctions à venir : par exemple, si les cookies d'analyse deviennent un "consentement implicite", certains comportements actuellement sanctionnés par des milliards pourraient devenir légaux. Cependant, la plupart des experts en consentement avertissent que l'application d'un *consentement transparent et non coercitif* restera centrale, même si certaines règles sont assouplies. Tout changement futur préservera probablement le choix de l'utilisateur en matière de suivi (cookies publicitaires/de suivi), de sorte que le fait de ne pas afficher de bannière (ou de fournir une fausse bannière) pourrait toujours être punissable.

Implications et Orientations Futures

Implications Pratiques pour les Organisations

L'implication immédiate de ces sanctions est que **les organisations doivent traiter les bannières de cookies comme des projets de conformité sérieux**. L'époque où un opérateur de site web pouvait considérer les cookies comme "juste un désagrément" est révolue, du moins si l'entreprise est exposée aux marchés de l'UE/Royaume-Uni. Les entreprises devraient auditer leurs bannières et l'utilisation des cookies de manière proactive. Cela signifie s'assurer que *tous* les cookies non essentiels sont derrière une bannière qui répond aux tests légaux : informer l'utilisateur, offrir un "refuser" facile ou des choix granulaires, et enregistrer un consentement valide avant de déclencher tout script de suivi. Les équipes de conformité devraient suivre les annonces des actions d'application et modéliser leurs bannières sur les meilleures pratiques (par exemple, donner une importance et un style égaux à l'acceptation et au refus, et éviter les "murs de cookies" qui forcent l'acceptation). Certaines entreprises passeront à de nouvelles plateformes de gestion du consentement. Les avocats conseillent également de documenter les journaux de consentement et les décisions de conception des bannières comme preuve des efforts de conformité, en cas de futures enquêtes.

Compte tenu des enjeux croissants, les gestionnaires de risques recalculent l'exposition. Une petite entreprise en Europe pourrait encourir des amendes de l'ordre de **dizaines de milliers** d'euros pour non-conformité, une entreprise de taille moyenne dans les **centaines de milliers** d'euros, et les grandes multinationales pourraient faire face à des pénalités de **huit ou neuf chiffres** si des violations flagrantes persistent. Les produits d'assurance pour les risques cyber/vie privée pourraient commencer à prendre en

compte l'obligation de consentement aux cookies dans leurs polices. De plus, étant donné que les APD se coordonnent souvent (le Comité européen de la protection des données peut faciliter l'application transfrontalière), même les entreprises opérant principalement dans un seul pays devraient adopter l'approche la plus stricte : très probablement le modèle français à l'heure actuelle. Les multinationales, comme nous l'avons vu avec Google, peuvent être frappées dans toute juridiction où leurs produits ou services sont présents.

Au-delà des amendes, les entreprises doivent noter que les dommages à la réputation sont également une sanction. La couverture médiatique des grosses amendes peut affaiblir la confiance des utilisateurs. Au minimum, une erreur dans une politique de confidentialité ou de cookies déclenche un flux de plaintes d'utilisateurs, ce qui à son tour invite les régulateurs. Le **coût d'opportunité** de ne pas afficher de bannière est multiple : amendes réglementaires, dépenses de remédiation (refonte du site web dans un court délai), perte de confiance des utilisateurs et éventuelles poursuites civiles. Dans les secteurs fortement réglementés comme la finance ou la santé, le consentement aux cookies est un aspect de l'examen global du traitement des données ; des échecs répétés pourraient même amener les autorités à auditer d'autres pratiques. En résumé, le coût de la conformité (investir dans une bannière et une conception appropriées) est bien inférieur aux sanctions encourues.

Contexte Plus Large et Développements

Plusieurs forces plus larges façonneront l'évolution de l'application du consentement aux cookies :

- **Évolution des lois sur la vie privée** : En Europe, le futur règlement ePrivacy (s'il est adopté) codifiera probablement de nombreuses normes de consentement dans un seul règlement. Les changements proposés incluent la clarification des définitions de "mur de cookies" et l'éventuelle extension des exemptions (par exemple, pour certaines analyses). S'il est adopté, il pourrait également remplacer ou intégrer les lois nationales sur les cookies. Quelle que soit sa forme finale, les pouvoirs d'application sont susceptibles d'augmenter. De même, au Royaume-Uni, le projet de loi sur la protection des données et l'information numérique signale des sanctions plus sévères (et pourrait assouplir certaines règles relatives aux cookies, par exemple le consentement aux analyses). Les organisations devraient surveiller ces pistes législatives car elles auront un impact sur les obligations de conformité et les sanctions potentielles.

- **Évolutions technologiques** : L'industrie technologique s'éloigne des cookies tiers pour le suivi (par exemple, la dépréciation des cookies tiers par Google dans Chrome et les changements axés sur la confidentialité dans les navigateurs). Dans les années à venir, moins de sites pourraient utiliser la publicité basée sur les cookies ; au lieu de cela, de nouvelles méthodes (API de navigateur ou stockage local) pourraient apparaître. Les régulateurs ont signalé que les "paywalls de consentement ou de paiement" ne devraient pas être autorisés, même en utilisant de nouvelles technologies. Ainsi, même si les moyens techniques changent, le principe du choix de l'utilisateur demeure. Le chiffrement, le "fingerprinting" et le suivi côté serveur seront probablement ciblés par la loi avec des règles de consentement similaires (le RGPD couvre tout "traitement" de données personnelles, pas seulement les cookies).

- **Tendances internationales** : En dehors de l'Europe, certains pays commencent à se concentrer sur le consentement de l'utilisateur. Par exemple, le projet de loi PDP de l'Inde (une fois promulgué) mettra l'accent sur le consentement de l'utilisateur pour les données personnelles. En Asie-Pacifique, la connaissance des règles européennes en matière de cookies est croissante. Il est intéressant de noter que certaines entreprises multinationales appliquent simplement un consentement de type RGPD partout pour simplifier leur politique (ainsi, en pratique, de nombreux sites non-UE affichent désormais des bannières de cookies). Si davantage de lois sur la vie privée (lois des États américains ou de l'Asie-Pacifique) commencent à mentionner explicitement le suivi, la notion de "pénalité de bannière" pourrait se répandre à l'échelle mondiale. Cependant, à l'heure actuelle, les sanctions les plus sévères restent européennes.

- **Campagnes d'application** : Les APD ont indiqué que les revenus des cookies sont une campagne spéciale. Par exemple, le "plan d'action cookies" 2019-2025 de la CNIL a impliqué l'émission de lignes directrices, de mises en demeure et d'amendes par vagues. Les ONG de défense de la vie privée comme NOYB galvanisent davantage de plaintes (la "campagne de bannières de cookies" de NOYB a déposé 850 plaintes à travers l'Europe). Il est probable que les APD continueront d'utiliser à la fois la carotte (orientations, sursis temporaires) et le bâton (amendes, annonces publiques) dans un avenir prévisible. Comme l'a noté le blog Stephenson Harwood, les régulateurs considèrent l'application des règles relatives aux cookies comme un domaine prioritaire (Source: www.dataprotectionlawhub.com) (Source: www.dataprotectionlawhub.com).

- **Précisions judiciaires** : Les tribunaux continueront de clarifier les questions litigieuses. Déjà, la CJUE (en 2020) a indiqué que les cases pré-cochées et les informations accessibles uniquement par lien constituaient des formes de consentement invalides. Les juridictions inférieures (comme dans l'affaire Focus Online à Munich) poursuivent cette tendance. Si les juridictions supérieures des États membres (et potentiellement la CJUE) abordent les questions de conception des bandeaux de cookies, la jurisprudence solidifiera les contours de la responsabilité. Ces décisions pourraient avoir un impact sur l'évaluation des sanctions : si un tribunal juge un bandeau illégal, un régulateur pourra imposer une amende en toute confiance, sachant que la base juridique est solide.

Conclusion

La sanction pour l'absence d'un bandeau de consentement aux cookies conforme peut être sévère. En vertu des lois de confidentialité en vigueur, un bandeau manquant ou déficient signifie que le consentement de l'utilisateur n'a pas été valablement obtenu – une violation qui peut déclencher l'application de l'ensemble des sanctions en matière de protection des données. En Europe, les régulateurs traitent explicitement les violations du consentement aux cookies comme des infractions au RGPD, passibles des amendes les plus élevées. Des études de cas ont montré des sanctions allant de dizaines de milliers d'euros à des centaines de millions, selon l'ampleur et l'intention de la violation. Nous avons vu les régulateurs imposer des amendes massives (par exemple, 325 millions d'euros à Google, 150 millions d'euros à Shein en 2025) et des astreintes journalières (par exemple, 100 000 euros par jour) pour le non-respect de l'obtention du consentement aux cookies (Source: www.lemonde.fr) (Source: www.cnil.fr). Des amendes plus courantes (de l'ordre de quelques centaines de milliers d'euros) ont également été fréquentes pour les acteurs plus modestes.

Ces résultats reflètent un message constant : **le consentement aux cookies n'est pas facultatif, et les autorités l'appliqueront avec vigueur**. Les organisations qui négligent les exigences relatives aux bandeaux risquent non seulement des sanctions financières, mais aussi des changements opérationnels forcés (suppression des cookies non autorisés) et des atteintes à leur réputation. Il incombe aux opérateurs de sites web de s'assurer que leurs mécanismes de consentement respectent les normes légales d'un consentement éclairé, libre et facilement révocable (Source: ico.org.uk) (Source: www.cnil.fr).

À l'avenir, bien que l'expérience utilisateur des bandeaux de cookies puisse évoluer (avec d'éventuelles réformes réglementaires visant à réduire la « fatigue des bandeaux »), l'attente fondamentale demeure : les utilisateurs doivent avoir un contrôle clair sur les cookies de suivi. Les régulateurs ont signalé que la non-conformité continuera d'attirer l'attention et les sanctions. En somme, la « sanction » est que l'absence d'affichage d'un bandeau conforme constitue une violation de la loi – et ces violations sont de plus en plus souvent assorties de **sanctions strictes, souvent très lourdes** (Source: www.reuters.com) (Source: www.cnil.fr). Les organisations seraient bien avisées non seulement d'afficher des bandeaux de consentement aux cookies, mais aussi de les mettre en œuvre conformément aux directives et aux précédents d'application.

Étiquettes: penalites-consentement-cookies, rgpd, loi-cookies, directive-eprivacy, protection-donnees, cnil, conformite-cookies

---