NEWSLETTER

IT

Février 2025

SOMMAIRE

ACTUALITÉ

ACTUALITÉ

CONTENUS ILLICITES EN LIGNE : JUSQU'OU PEUT ALLER LA RESPONSABILITE DES HEBERGEURS ?

L'arrêt de la Cour de cassation du 15 janvier 2025 (n° 23-14.625) **vient préciser les contours de la responsabilité des hébergeurs de contenus, en affirmant que des obligations contractuelles plus strictes que celles prévues par la loi** pour la confiance dans l'économie numérique (LCEN) peuvent leur être imposées.

Le cadre juridique et les faits de l'affaire

Les obligations de l'hébergeur selon la LCEN

L'article 6 de la **LCEN (loi n° 2004-575 du 21 juin 2004),** dans sa version applicable aux faits de l'affaire, prévoit que l'hébergeur ne peut être tenu responsable des contenus illicites stockés sur sa plateforme tant qu'il n'en a pas eu connaissance. Dès notification, il doit agir promptement pour retirer ces contenus. Cependant, la loi n'impose pas à l'hébergeur d'instaurer des mesures de filtrage proactives, le principe étant une obligation de réaction et non de surveillance générale.

Le litige entre Dstorage et la Société Générale

Dans cette affaire, la société Dstorage, exploitante de la plateforme de stockage en ligne « 1fichier.com », avait conclu un contrat monétique avec la Société Générale, lui permettant d'offrir un service de paiement en ligne à ses utilisateurs. Le contrat incluait deux clauses essentielles :

- L'engagement de Dstorage à **s'abstenir de toute activité illicite**, incluant la contrefaçon d'œuvres protégées par des droits de propriété intellectuelle.
- Le droit pour la Société Générale de **résilier le service sans préavis** dans le cas où elle aurait eu connaissance de contenu illicite sur le site 1fichier.com.

Après signalement de contenus contrefaits sur 1fichier.com par le groupe Mastercard, la Société Générale a mis en demeure Dstorage de supprimer les fichiers incriminés. Malgré une première suppression, de nouveaux fichiers illégaux ont été détectés, entraînant la résiliation du contrat de paiement par la Société Générale.

La décision de la Cour de cassation

La position de la Cour de cassation

Dstorage a tenté de contester la résiliation, arguant qu'elle avait respecté la LCEN en supprimant les contenus après notification. Toutefois, la Cour de cassation a confirmé les décisions des juridictions précédentes, en soulignant que la société avait signé un contrat engageant sa responsabilité au-delà des exigences légales. **Les juges ont ainsi retenu que Dstorage n'avait pas pris les mesures techniques appropriées** et imposées contractuellement par la Société Générale, pour empêcher la récidive de contenus illicites.

Cette décision confirme qu'un hébergeur peut être tenu à des obligations contractuelles plus contraignantes que celles prévues par la loi, notamment en matière de prévention des infractions.

Conséquences pratiques pour les hébergeurs

Cet arrêt souligne l'importance pour les hébergeurs de :

- Analyser minutieusement les termes de leurs contrats avec leurs partenaires, notamment les clauses relatives à la conformité légale.
- Lorsque cela leur est imposé contractuellement, mettre en place des dispositifs de surveillance proactive, même si la loi ne l'exige pas, afin de prévenir la récidive de contenus illicites.
- Anticiper les risques de rupture contractuelle, en tenant compte des obligations imposées par les fournisseurs de services tiers (ex. : banques, processeurs de paiement).

L'arrêt du 15 janvier 2025 marque une évolution dans la responsabilité des hébergeurs de contenus, en confirmant que les obligations contractuelles peuvent aller au-delà des exigences légales de la LCEN. Les prestataires de services doivent ainsi redoubler de vigilance lors de la négociation de leurs contrats, sous peine de voir leur activité fragilisée par des résiliations unilatérales.

Source : ici

LE PRESTATAIRE QUI LIVRE UN SYSTEME INFORMATIQUE NE CORRESPONDANT PAS AUX BESOINS DE SON CLIENT MANQUE A SON DEVOIR D'INFORMATION ET DE CONSEIL

Le prestataire informatique doit s'attacher, lors de la conclusion du contrat, à faire émerger une analyse précise des besoins du client. Le constat que le système informatique livré ne correspondait pas auxdits besoins caractérise un manquement au devoir de conseil de la part du prestataire, susceptible d'engager sa responsabilité.

Le débat récurrent sur le devoir de conseil du prestataire face à une solution informatique jugée inadaptée par le client à ses besoins

Une société spécialisée dans le commerce de caisses enregistreuses, solutions informatiques de gestion et monétique, signe, avec une société exploitant un bar-brasserie, un contrat de fourniture et d'installation de matériels informatiques, dont des écrans devant permettre aux clients de commander et de régler les consommations à distance, pour un montant total d'environ 70K euros.

Le matériel est livré et installé mais ne répond pas aux attentes du client qui met en avant des retards de mise en service et des dysfonctionnements. Ce dernier, après plusieurs mises en demeure, assigne son prestataire devant le tribunal de commerce aux fins de se voir condamner à rembourser la somme versée et réparer la perte d'exploitation en résultant.

- Le prestataire fait valoir le respect de ses obligations contractuelles, l'installation conforme du matériel informatique, le retard étant imputable au client, et chacune de ses interventions ayant fait l'objet d'un bon validé et signé par le client. Il relève en particulier que le client n'avait jamais remis le cahier des charges sollicité.
- Le client fait le constat que le matériel n'a jamais correctement fonctionné et considère notamment que les difficultés rencontrées dans la mise en œuvre des solutions techniques caractérisaient un manquement à l'obligation de conseil et de délivrance conforme de la part du prestataire.

Le tribunal de commerce de Bordeaux va donner partiellement raison au client et la cour confirme le jugement.

Le prestataire informatique, professionnel averti, doit rechercher les informations nécessaires et analyser avec précision les besoins du client

D'une part, la question de la délivrance conforme est écartée car la demande était fondée sur le code de la consommation, non applicable s'agissant de ventes entre professionnels.

D'autre part, la cour, sur le fondement des article 1103 , 1104 et 1112-1 du code civil rappelle les contours du devoir d'information.

La cour relève que le prestataire informatique est un professionnel averti dans ce domaine. Il lui incombait un **devoir de conseil lors de la conclusion du contrat** et **il lui appartenait de définir les besoins de son client pour le projet concerné en recherchant les informations nécessaires**.

La cour va déduire de l'ensemble des éléments produits, en particulier la proposition commerciale remise avant la signature du contrat ainsi que les courrier échangés, que :

- le client souhaitait la mise en place d'une interface personnalisée permettant la commande en libre-service et le paiement des consommations ;

- Le fait que le client n'ait pas mentionné de réserve dans l'encart 'observations et conseils' des bons d'intervention n'est pas de nature à prouver avec certitude qu'il était satisfait des prestations ;
- le client a remis les éléments sollicités par le prestataire ;
- un procès-verbal de constat, établi par un huissier de justice, établit le caractère non fonctionnel du système de commande à distance depuis les tables.

Ainsi, il apparaît que **le système informatique livré ne correspondait pas aux besoins du client, ce qui caractérise un manquement au devoir de conseil** de la part du prestataire, susceptible d'engager sa responsabilité.

C'est donc à bon droit que le tribunal de commerce a jugé que **le prestataire était un professionnel de la prestation informatique et devait s'attacher, lors de la conclusion du contrat, à faire émerger une analyse précise des besoins du client, tant en matière technique que graphique.**

La cour, sur le fondement des articles 1217 et 1231-1 du code civil va faire droit à la demande de remboursement au regard des manquements contractuels du prestataire établis.

L'indemnisation pour perte d'exploitation sera cependant écartée. Le client avait posté des photos sur les réseaux sociaux démontrant que l'établissement était en travaux, il n'est donc pas établi que le retard pris dans l'installation du matériel informatique avait eu pour conséquence de décaler l'ouverture de l'établissement.

Source : ici

LA CLAUSE LIMITATIVE DE RESPONSABILITE ECARTEE EN CAS DE MANQUEMENT A L'OBLIGATION DE CONSEIL DU PRESTATAIRE IT EN COURS D'EXECUTION DU CONTRAT : UNE DERIVE QUI MET A MAL LA CLAUSE LIMITATIVE

La clause exonérant le prestataire de sa responsabilité « au titre de tous dommages ou préjudices indirects ou immatériels qui pourraient résulter de l'inexécution ou de l'exécution défectueuse des services » ne trouve pas à s'appliquer dans la mesure où c'est un défaut d'information et de conseil qui est reproché au prestataire et non une défaillance de son interface.

Fourniture d'une solution de paiements à distance et opérations frauduleuses : le prestataire tente de s'exonérer de sa responsabilité

Une société développant une solution de chèque cadeau dématérialisé contractualise avec un prestataire informatique pour la fourniture d'une interface de gestion lui permettant d'accepter des opérations de paiement par carte en vente à distance, s'appuyant sur un dispositif nommé « Smart 3-D Secure » consistant à calculer en temps réel un score de risque associé à tout paiement de manière à prévenir les opérations bancaires frauduleuses.

Le client, victime d'une série d'opérations frauduleuses, met en demeure son prestataire en lui demandant de réparer le préjudice résultant des fraudes. Face au refus de ce dernier de faire droit à ses demandes indemnitaires, le client l'assigne en réparation devant le tribunal de commerce de Paris. Le prestataire, condamné à payer une somme correspondant au montant des transactions frauduleuses, interjette appel, faisant fait valoir que sa responsabilité contractuelle ne peut être engagée.

Le prestataire soutient notamment que :

- le client a expressément accepté une **clause exonératoire de responsabilité** en cas de fraude, lequel est une reprise des dispositions du code monétaire et financier ;
- il **n'a pas manqué à son devoir d'information précontractuelle** dans la mesure où le client, spécialiste de la vente à distance et du prépaiement, est un **professionnel averti** et qu'il était en tout état de cause **parfaitement informé** des avantages et inconvénients liés à l'utilisation de l'authentification 3D Secure, du « Smart 3-D Secure » et de la facilité de paiement sans authentification en « one click » ;
- le client aurait **choisi délibérément** d'activer un mode de paiement simplifié pour ses clients.

Le client considère que l'appelante a manqué à son **obligation précontractuelle d'information** en ce qu'elle a présenté son système « Smart 3-D Secure » comme un outil efficace alors qu'il n'offrait manifestement pas des garanties suffisantes en matière de sécurité et qu'il appartenait au prestataire de conseiller le client sur la meilleure manière d'assurer la sécurité de sa plate-forme de vente.

Le client soutient également que :

- l'algorithme de détection des fraudes recommandé n'a pas fonctionné ;
- Il doit être qualifié de **professionnel non-averti** s'agissant d'un outil novateur et exclusif du prestataire ;

- l'obligation d'information incombant au prestataire consistait à jouer un **rôle actif** pour s'adapter à la situation de sa cliente ;
- le prestataire a manqué à son devoir de conseil **au cours de l'exécution du contrat,** n'ayant pas été en mesure de lui conseiller à partir du moment où des fraudes ont été détectées, les mesures de nature à y mettre un terme et conseillant même de ne rien faire au motif que le risque était assuré ;
- la clause d'exonération de responsabilité prévue par les conditions générales de vente ne peut s'appliquer en cas de manquement à son devoir d'information et de conseil.

Le client réclame la réparation du préjudice que lui a causé ce défaut de conseil et qui représente le montant découlant des fraudes qui auraient pu être évitées si le système sécurisé avait été mis en place sur toutes les transactions.

Les limitations de responsabilité contractuelles inefficaces en cas de manquement à l'obligation de conseil du prestataire

La cour rappelle que les dispositions antérieures à la réforme du droit des contrats trouvent ici application. C'est donc sur le fondement des anciens articles 1134 et 1147 du code civil qu'elle va condamner le prestataire.

Les juges analysent en détail le bon de commande et le contenu des dispositions contractuelles, ainsi que les échanges entre les parties en cours d'exécution du contrat. Il en ressort que le prestataire a dispensé des conseils sur l'utilisation de son interface et surtout le niveau de sécurisation souhaité par son client, en conseillant de baisser le niveau de sécurité afin de réduire le taux d'échec des opérations, et en recommandant de ne rien changer après le constat d'un comportement suspect d'un acheteur.

Or les fraudes se sont poursuivies et l'utilisation inadéquate de son interface n'a pas permis d'enrayer ce phénomène, de sorte que le client a été contraint de rembourser une partie du montant issu de la fraude aux utilisateurs.

Ainsi, contrairement à ce que soutient le prestataire, sa cliente avait émis le souhait d'un niveau de sécurisation important et **ne peut être considérée**, alors qu'en tant que prestataire de services elle l'invitait constamment à baisser son niveau de sécurisation afin d'avoir un rendement optimal, **comme une professionnelle avertie dûment informée des risques d'un tel choix.**

Le prestataire a ainsi, **en cours d'exécution du contrat**, prodigué moult conseils qui se sont révélés inadaptés puisqu'ils n'ont permis ni d'empêcher ni d'enrayer les fraudes survenues.

S'agissant de la **clause limitative de responsabilité**, la Cour considère qu'elle n'a pas vocation à s'appliquer dans la mesure où la responsabilité de la société n'est pas recherchée en sa qualité de prestataire de services de paiement, en raison d'une défaillance de l'interface, mais en tant que fournisseur de cette interface pour l'utilisation de laquelle elle fournissait des conseils au client en cours d'exécution du contrat.

S'agissant de la **clause exclusive de responsabilité**, qui écartait explicitement la responsabilité dans le cas d'un « phishing » ou d'une opération de « carding », elle est également inapplicable car elle comportait dans sa rédaction une condition selon laquelle les fraudes constatées devaient résulter d'escroquerie en bande organisée, ce qui n'est pas démontré en l'espèce.

La Cour ajoute que l'exonération de responsabilité contractuellement prévue « au titre des dommages ou préjudices indirects ou immatériels » pouvant résulter d'une mauvaise exécution des services ne saurait non plus s'appliquer. Les juges rappellent, à cet égard, que ce qui est ici reproché n'est pas une défaillance de l'interface, mais un défaut d'information et de conseil de la société.

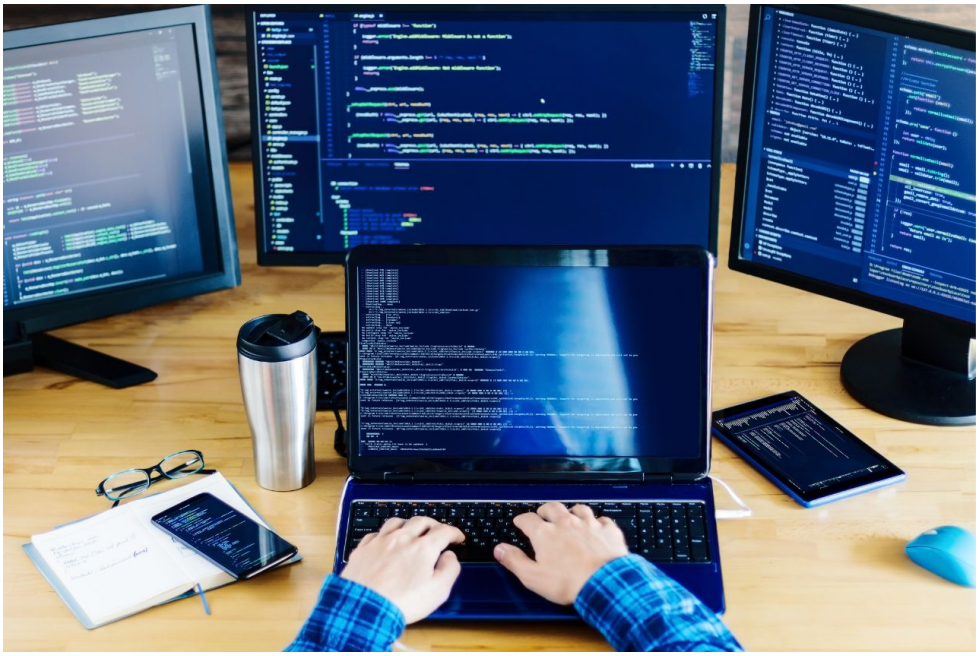
Le jugement est par conséquent confirmé en ce qu'il a retenu la responsabilité contractuelle du prestataire et écarté l'application de la clause limitative des conditions générales de vente.

Il sera également confirmé s'agissant du montant du préjudice subi.

Cette décision surprend dans la mesure où l'obligation de conseil contractuelle est généralement considérée comme accessoire de l'obligation principale de délivrance conforme. En ce sens, si la clause limitative de responsabilité a vocation à s'appliquer en cas de violation de l'obligation principale, pourquoi ne s'appliquerait-elle pas en cas de violation de l'obligation de conseil qui est son accessoire ?

En tout état de cause, cet arrêt impactera la rédaction des clauses limitatives de responsabilité figurant dans vos contrats…

Source : ici



L'ACTION EN CONTREFAÇON DE LOGICIEL FACE A LA RESPONSABILITE CONTRACTUELLE

Un éditeur de logiciel peut-il agir en contrefaçon tout en demandant des dommages et intérêts pour violation du contrat de licences ?

Devant le Tribunal Judiciaire de Lyon 12 novembre 2024 N° 19/02639, une société éditrice de logiciels, revendiquant des droits d'auteur sur un logiciel de gestion de caisses de paiement, reprochait à son cocontractant et licencié des actes de contrefaçon et de concurrence déloyale. Elle alléguait notamment que cette dernière avait reproduit et distribué son logiciel sans autorisation et avait favorisé son utilisation frauduleuse. BOS MONETIQUE, en tant que licencié, contestait ces accusations, invoquant le principe de non-cumul des responsabilités.

Le non-cumul des responsabilités contractuelles et délictuelles

Il s'agissait ici de savoir si un éditeur de logiciel pouvait agir en contrefaçon devant le Tribunal Judiciaire alors que les parties étaient liées par un contrat et donc soumises au régime de la responsabilité contractuelle.

En l'espèce, le tribunal de Lyon, dans les motifs de sa décision, a rappelé que ce **principe interdit de combiner responsabilité contractuelle et délictuelle** lorsque le préjudice allégué découle de l'inexécution d'obligations contractuelles.

Toutefois, le Tribunal souligne que des actes portant atteinte à des droits de propriété intellectuelle, comme la contrefaçon, relèvent d'un régime distinct. En s'appuyant sur les directives européennes 2004/48/CE et 2009/24/CE et dans la lignée de l'arrêt de la CJUE du 18 décembre 2019, C-666/18 (IT Development contre Free), le tribunal a cependant estimé que l'action en contrefaçon était ici recevable, permettant au titulaire de droits de bénéficier de mesures spécifiques telles que des dommages-intérêts élevés et des saisies-contrefaçon.

Le Tribunal de Lyon a précisé, pour ce qui concerne la détermination des dommages et intérêts que : *« En effet si selon l'article 1231-1 du code civil le débiteur peut, en cas d'inexécution de ses obligations nées du contrat, être condamné à des dommages-intérêts, ceux-ci ne peuvent excéder ce qui était prévisible ou ce que les parties ont prévu conventionnellement.* »

La recevabilité de l'action en contrefaçon

L'action en contrefaçon est donc recevable dans le cadre d'une relation contractuelle et des dommages et intérêts peuvent être demandés pour violation du contrat.

Le tribunal a finalement conclu que BOS MONETIQUE (Licencié) avait commis des actes de contrefaçon en reproduisant le logiciel CLYO SYSTEMS sur plusieurs postes de travail sans droit suffisant. La société a été condamnée à verser 25 000 € de dommages-intérêts et à cesser la reproduction du logiciel sous astreinte. En revanche, les demandes fondées sur l'utilisation frauduleuse du logiciel et la concurrence déloyale ont été rejetées, faute de preuve suffisante.

Cette décision illustre l'incursion de la protection des droits de propriété intellectuelle et donc des actions en contrefaçon sur le terrain de la responsabilité contractuelle. Ce jugement vient confirmer un arrêt de la Cour de Cassation du 5 octobre 2022 ainsi qu'un récent arrêt de la Cour d'appel de Paris du 8 décembre 2023 (n°21/19696). Une action en contrefaçon, donc délictuelle par nature, est recevable devant le tribunal judiciaire alors même que les parties sont liées par un contrat dont les termes ont été violé par licencié. Encore une fois, l'action en contrefaçon peut reposer tant sur le fondement de la responsabilité contractuelle, que délictuelle !

Source : ici

OPENAI CONDAMNEE POUR NON-RESPECT DU RGPD PAR L'AUTORITE ITALIENNE DE PROTECTION DES DONNEES

Le 2 novembre 2024, l'autorité italienne de protection des données (la Garante) a rendu une décision condamnant OpenAI, l'éditeur du modèle d'intelligence artificielle à usage général GPT-3, pour violation du Règlement général sur la protection des données (RGPD). Au cœur du débat, la question de la formation et de l'entrainement du modèle d'intelligence artificielle (IA) à partir de données d'individus, massivement collectées sur internet (scraping).

La condamnation du 2 novembre 2024 intervient directement dans le prolongement de l'interdiction temporaire de ChatGPT en Italie, en avril 2023.

Petit retour en arrière : début 2023, quelques mois seulement après le lancement de son modèle d'intelligence artificielle GPT-3 et des services ChatGPT au grand public, plusieurs enquêtes étaient ouvertes en Europe pour violation du RGPD. Par plusieurs décisions de mars et avril 2023, l'autorité de protection italienne interdisait de manière immédiate et temporaire ChatGPT en Italie, avant de se raviser quelques semaines plus tard, au regard des mesures correctives mises en place par l'éditeur.

La décision du 2 novembre 2024 intervient après plusieurs mois d'enquêtes et constitue la première condamnation financière d'OpenAI en Europe pour non-respect du RGPD. Elle met en lumière plusieurs points cruciaux pour les acteurs du secteur de l'IA et, plus largement, pour les entreprises qui utilisent l'IA à des fins professionnelles.

La première condamnation financière d'OpenAI

La confirmation de la violation des principes fondamentaux du RGPD

L'autorité italienne a relevé une série de manquements au RGPD (ex : défaut de notification d'une violation de données, absence de vérification de l'âge de l'utilisateur…). Les plus graves consistent en :

- **l'absence d'identification et de choix de la base juridique du traitement**, **avant le début du traitement**, notamment pour ce qui concerne la phase d'apprentissage de ChatGPT. OpenAI ne pouvant se prévaloir a posteriori d'un intérêt légitime, elle a violé le RGPD ;

- la **violation des droits des personnes intéressées, en particulier de l'obligation d'information** des personnes concernant les traitements réalisés aux fins de formation des modèles et plus généralement le **manque de transparence**.

En particulier, OpenAI s'est abstenue d'informer les individus dont les données étaient scrapées sur internet, et qui n'étaient pas utilisateurs de ses services, du traitement de leurs données personnelles à des fins de formation du modèle d'IA.

Pour ce qui concerne les utilisateurs, la politique de confidentialité était difficilement accessible en anglais, ce qui ne permettait pas une information adéquate des personnes.

Certains manquements étant continus et encore en cours, l'autorité saisit par ailleurs l'autorité irlandaise de plusieurs sujets.

A commencer par la **violation du principe d'exactitude et de la fiabilité des traitements**, question brulante qui demeure à date « ouverte ». Certes, compte tenu de la nature probabiliste du système, l'autorité italienne reconnait que ChatGPT n'a pas pour finalité de fournir des résultats fiables, ce dont OpenAI a informé les utilisateurs. Elle souligne également qu'OpenAI a bien mis en œuvre des mesures pour identifier et supprimer les informations inexactes (identification des informations inexactes à chaque phase de formation du modèle, instruction au modèle de refuser de traiter des informations personnelles ou sensibles, possibilité pour les individus de notifier les inexactitudes et de solliciter leur correction) et s'est engagé à améliorer de manière continue la fiabilité de son modèle. Mais, malgré cela, l'autorité italienne considère qu'Open AI continue d'être en infraction à ce principe, ce qui justifie le transfert des éléments à l'autorité irlandaise chef de file, compétente à date pour les manquements au RGPD en vertu du mécanisme du guichet unique, Open AI disposant désormais d'une filiale en Union Européenne.

La condamnation : une amende administrative de 15 millions d'euros

La Garante condamne Open AI à une amende administrative de 15 millions d'euros et à la réalisation d'une nouvelle campagne de sensibilisation à destination du public italien (fonctionnement de ChatGPT, impacts des traitements de données sur la vie privée, droits offerts par le RGPD...).

Si l'amende prononcée par l'autorité italienne peut, dans un premier temps, paraitre élevée, qui plus est au regard de la durée des infractions concernées (l'autorité compétente pour tout manquement à compter de février 2024 étant l'autorité irlandaise chef de file), ce montant doit être relativisé[1].

Qui plus est à l'aune de la tendance actuelle de **multiplication des condamnations à l'encontre des GAFAMs**.

Open AI considérant la sanction comme disproportionnée a indiqué faire appel de cette décision.

A noter que les autorités européennes pourraient néanmoins ne pas s'arrêter là ; l'autorité irlandaise, chef de file, ayant ouvert une enquête et une task force ayant été constituée au niveau européen (dont les premières conclusions ont été publiée le 23 mai 2024).

Quels enseignements en tirer ?

Les enjeux pour les éditeurs de modèles et systèmes d'intelligence artificielle

Anticiper dès la phase de conception du modèle ou du système d'IA la conformité au RGPD mais également à l'IA Act, est essentiel.

Cette condamnation rappelle aux éditeurs de modèle et de système d'IA Générative qu'une attention particulière doit être apportée concernant les traitements de données personnelles réalisés à des fins de formation. Si une interprétation plus souple du RGPD semble possible (comme le laissent entendre les recommandations de la CNIL et du RGPD en matière d'intelligence artificielle), les traitements doivent être licites, transparents et proportionnés. Le nombre de personnes dont les données sont scrappées sur internet ne justifierait par ailleurs aucune exonération du respect du devoir d'information.

En outre, informer les utilisateurs que leurs données et prompts peuvent être réutilisés à des fins d'amélioration des services ne suffit pas.

L'Autorité considère que l'éditeur est tenu d'informer les personnes de la finalité spécifique, innovante et particulière de formation des modèles d'IA. Un élément essentiel à considérer lors de la rédaction des mentions d'information, qui devront être précises.

Quelles conséquences pour les entreprises utilisatrices de systèmes d'IA en général et de ChatGPT en particulier ?

Les entreprises qui déploient des modèles et des systèmes d'IA doivent être conscientes des implications juridiques de cette décision. En tant que responsables de traitement de données personnelles, elles doivent s'assurer que les traitements réalisés au moyen de ces systèmes (comme ChatGPT), lors de la phase de déploiement, respectent le RGPD.

Comme le rappelle le CEPD dans son avis du 17 décembre 2024 (voir notre article ici) sur les modèles d'IA, l'entreprise déployant un modèle d'IA se doit de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données (« principe d'accountability »). Il est ainsi recommandé de réaliser une **évaluation appropriée** en amont du choix et du déploiement du système, pour démontrer la conformité des traitements réalisés aux principes essentiels du RGPD et leur licéité.

Le CEPD considère par ailleurs que, **lorsqu'un modèle d'IA a été développé et entrainé avec des données personnelles traitées illégalement, cela peut avoir des conséquences sur la licéité de son déploiement et de son utilisation, sauf à ce que le modèle ait été anonymisé** de manière effective.

Or, pour qu'un modèle soit considéré comme anonyme, selon le CEPD, deux conditions cumulatives doivent être réunies. Il doit être très peu probable :

- d'identifier directement ou indirectement les personnes dont les données ont été utilisées pour créer le modèle ; et
- qu'il soit possible d'obtenir, d'extraire ces données personnelles du modèle par le biais de requêtes.

Concrètement, les déployeurs devront donc s'assurer que le modèle d'IA déployé n'a pas été développé grâce à un traitement illicite de données à caractère personnel ou que le modèle d'IA soit effectivement anonymisé.

Cela implique-t-il que tout utilisateur de Chat GPT serait en écart avec la règlementation européenne et passible de sanctions ?

Concernant GPT-3, compte tenu de la décision de condamnation italienne et du rapport du CEPD de mai 2024, les déployeurs ne pourront ignorer que le traitement initial mis en œuvre par Open AI a été contraire au RGPD. Mais en serait-il de même pour GPT-4 ?

Ceci relance encore une fois le débat d'une difficile articulation entre le respect strict de la règlementation de protection des données et le risque de retard européen à l'innovation et à l'adoption des IA Génératives. Affaire à suivre donc, le déploiement des IA génératives étant massif au sein des entreprises, posant concrètement la question des risques réellement encourus par les entreprises utilisatrices.

Sources : Décision Garante Open AI du 2 novembre 2024 (en italien) ; Communiqué de presse de la Garante du 20 décembre 2024.

[1] Il représente à peine plus de 1.5 % du chiffre d'affaires mondial d'Open AI. Bien loin donc de la sanction encourue, équivalant au montant le plus élevé entre 4% du chiffre d'affaires mondial ou 20 millions d'euros. L'autorité a d'ailleurs souligné la collaboration d'Open AI et la mise en œuvre à compter du mois de mars 2023 de mesures correctives dans le prolongement de la sanction temporaire d'interdiction du service.

ATTEINTE A LA VIE PRIVEE ET AU DROIT A L'IMAGE : PAS D'OBLIGATION DE SUPPRIMER ET DE DEREFERENCER UN ARTICLE DE PRESSE

Jugeant l'atteinte à la vie privée et au droit à l'image d'une célèbre actrice constituée, le Président du Tribunal judiciaire de Nanterre n'ordonne toutefois pas la suppression ou le déréférencement de l'article litigieux.

Les atteintes aux droits de la personnalité constituées selon une appréciation classique du Président du Tribunal judiciaire de Nanterre

Le contenu dont la publication était reprochée à l'éditeur du journal Madame Figaro, est un article relatif à un diner entre une célèbre actrice et un humoriste français bien connu du public. L'article était accompagné de plusieurs photographies des protagonistes. Considérant qu'une telle publication portait atteinte à ses droits de la personnalité, l'actrice, sujet de l'article, a assigné le Figaro en référé devant le Président du Tribunal judiciaire de Nanterre afin d'obtenir (i) la réparation du préjudice allégué ainsi que (ii) la suppression et le déréférencement de l'article.

Conformément à la jurisprudence établie en la matière, l'ordonnance de référé juge l'atteinte constituée : « *toute personne, quelles que soient sa notoriété, sa fortune ou ses fonctions* [a] *le droit au respect de sa vie privée et le droit à la protection de son image* ».

Une indemnisation nettement revue à la baisse

L'ordonnance de référé prend notamment en considération l'absence d'allusion à une éventuelle relation sentimentale des protagonistes, le ton « *particulièrement neutre de l'article* » ou le caractère peu exposé de l'article qui ne figure pas en page d'accueil du site Internet.

A la lumière de ces éléments, il est décidé de ne pas faire droit à la demande de dommage et intérêts de l'actrice, s'élevant à 10 000 euros, et de lui allouer une provision de 1 500 euros à titre de réparation du préjudice moral découlant de l'atteinte à sa vie privée et 1 500 euros au titre de l'atteinte à son droit à l'image.

L'absence de condamnation à supprimer ou déréférencer l'article

Après avoir rappelé que les ingérences dans la liberté de presse ne sont justifiées que si elles constituent des mesures nécessaires au regard de l'atteinte considérée, l'ordonnance de référé déboute l'actrice de ses demandes visant à la suppression et au déréférencement de l'article. Elle considère en effet que de telles mesures sont disproportionnées au regard du préjudice subi, en outre intégralement réparé par l'allocation de dommages et intérêts.

Le Président rappelle « *la très forte volatilité des informations contenues par la publication litigieuse* » et la « *reprise* [des informations] *par de nombreux autres médias* » pour justifier la solution.

Si plusieurs juridictions ont déjà refusé d'ordonner la suppression ou le déréférencement de contenus portant atteinte à la vie privée, cette motivation peut toutefois être remarquée par son caractère général. Elle rappelle par ailleurs la protection qui doit être accordée à la presse qui bénéficie d'un statut particulier dans le cadre d'une société démocratique.

Source : ici

MENACES ET MESSAGES VIOLENTS EN LIGNE : LE RESEAU SOCIAL X (EX-TWITTER) CONDAMNE A COOPERER EN COMMUNIQUANT LES DONNEES D'IDENTIFICATION DES PRESUMES AUTEURS

Le réseau social X a été condamné à communiquer les données d'identification d'utilisateurs ayant proféré des menaces et des messages haineux et violents en ligne. Une nouvelle jurisprudence qui illustre les bénéfices de l'article 145 du Code de procédure civile au service des victimes de cyber-infractions.

La démonstration de l'intérêt légitime pour la communication des données d'identification

La reconnaissance d'un motif légitime par le Tribunal judiciaire de Paris

A la suite de la publication de messages haineux, violents et menaçants sur le réseau social X par un auteur anonyme, visant un père et son fils mineur de six ans, le père souhaite engager des poursuites pénales à l'encontre de cet auteur. Néanmoins, il doit d'abord l'identifier.

Il assigne alors la société Twitter, en son nom personnel et en qualité de représentant légal de son fils mineur, devant le Président du Tribunal judiciaire de Paris, statuant en référé, aux fins d'ordonner la **communication des données d'identification** et techniques.

S'agissant des données d'identification, le Tribunal judiciaire rappelle que l'utilisation de l'article 145 du Code de procédure civile requiert la démonstration d'un motif légitime d'établir ou de conserver, avant tout procès, des faits dont pourrait dépendre la solution du litige.

En l'espèce, le demandeur soutient que les messages reçus pouvaient être pénalement qualifiés de « menaces de mort » tandis que la société Twitter souligne l'absence de caractère explicite des propos, estimant qu'ils seraient, tout au plus, constitutifs de faits contraventionnels.

Le Tribunal judiciaire de Paris reconnaît cependant l'existence d'un motif légitime à rechercher l'identité de l'auteur des messages litigieux, en vue d'engager un procès pénal contre lui, et considère donc que les conditions de l'article 145 du Code de procédure civile sont réunies.

Quand la procédure civile sert le procès pénal

Pour décider de l'application de l'article 145 du Code de procédure civile, le juge des référés se prononce sur la qualification pénale des faits, en énonçant que les propos « *peuvent ressortir de la qualification pénale du délit de menaces de morts prévu par l'article 222-17 du Code pénal* ». Il précise également qu'il existe, à ce stade de la procédure, « *un procès pénal en germe non manifestement voué à l'échec* ».

Néanmoins, il convient de rappeler que l'essence même de l'article 145 du Code de procédure civile est de préparer le procès au fonds (mesures d'instruction in futurum). Dès lors, en se positionnant sur la qualification des propos qui relèveraient, à son sens, du délit de menaces de morts, pour analyser l'intérêt légitime, le juge civil ne se prononce -il pas déjà indirectement sur le fond du litige pénal ?

L'apport de précisions sur les données techniques devant être communiquées

La communication de données techniques en plus des données d'identification

Au sens des articles L34-1 et R10-13 du Code des postes et des communications électroniques, il peut être fait droit à la demande de **communication des données techniques**, telles que l'adresse IP et le port source associé par exemple, si la procédure pénale envisagée relève de la « délinquance grave ».

Le juge des référés considère que les propos litigieux, pouvant être assimilés au délit de menaces de morts, relèvent de la délinquance grave, et qu'il convient en ce sens de faire droit à la demande de communication des données techniques.

La communication des horaires et fuseaux horaires exacts de connexion

Les demandeurs formaient une demande complémentaire de communication visant, notamment, à obtenir la **communication des horaires et fuseaux horaires exacts des connexions**.

Bien que ces données ne soient pas expressément listées par l'article R10-13 du Code des postes et des communications électroniques, le juge des référés déclare qu'en raison de l'utilisation désormais généralisée d'adresses IP « nattées » (mutualisées pour plusieurs utilisateurs), la précision de l'horaire exact et du fuseau horaire de la connexion est une nécessité technique pour parvenir à identifier l'utilisateur de l'adresse IP.

Il est donc fait droit à la communication des données techniques, comprenant l'horodatage exact à la seconde près ainsi que le fuseau horaire de connexion des adresses IP utilisées pour les publications des contenus litigieux. **On peut toutefois reprocher que cette condamnation ne soit pas assortie d'une astreinte financière par jour de retard…**

Le recours aux pseudonymes sur internet n'offre pas l'impunité escomptée par les cyber-délinquants et ne les protège pas des éventuelles poursuites judiciaires… L'alliance entre juge civil et juge pénal dans ce jugement en est une parfaite illustration.

Source : ici

TEMU SOUS ENQUETE DES REGULATEURS EUROPEENS POUR VIOLATION DU DROIT DES CONSOMMATEURS ET DU DSA

La Commission Européenne a précisé le 31 octobre 2024, avoir ouvert une procédure formelle à l'encontre de la place de marché en ligne TEMU, spécialisée dans les produits à bas prix au Digital Service Act (DSA). Cette décision fait également écho à des enquêtes des régulateurs européens qui font état d'infractions par TEMU au droit des consommateurs.

L'enquête préliminaire menée par le réseau coopération en matière de protection des consommateurs (Réseau CPC) à l'encontre de TEMU

Rappel sur le rôle du Réseau CPC

En vertu du règlement du 12 décembre 2017 sur la coopération en matière de protection des consommateurs, les autorités nationales de protection des consommateurs des 27 États membres de l'UE, ainsi que de la Norvège et de l'Islande, forment le « Réseau CPC » pour enquêter et appliquer les lois européennes en matière de protection des consommateurs contre les infractions transfrontalières. La Commission européenne facilite et, dans certaines circonstances, coordonne ces enquêtes et actions conjointes.

Le Réseau CPC est ainsi chargé d'appliquer l'arsenal législatif européen en matière de droit de la consommation, particulièrement fourni, comprenant notamment :

- La directive sur les pratiques commerciales déloyales **(**Directive 2005/29/CE**)**,
- La directive sur les droits des consommateurs (Directive 2011/83/UE),
- la directive sur l'indication des prix (Directive (UE) 2019/2161 modifiant la directive 93/13/CEE et les directives 98/6/CE, 2005/29/CE et 2011/83/UE),
- la directive sur le commerce électronique (Directive 2000/31/CE)
- la directive sur les clauses contractuelles abusives (Directive 93/13/CEE).
- Le règlement général sur la sécurité des produits (GPSR), en vigueur depuis décembre 2024, qui impose aux plateformes de garantir la sécurité des produits vendus et qui permet aux autorités nationales de surveillance du marché d'émettre un ordre de retrait pour retirer un produit d'Internet si elles estiment qu'il est dangereux.

Les infractions relevées contre TEMU par le Réseau CPC

Selon une enquête préliminaire menée par le CPC et la Commission européenne, plusieurs pratiques de TEMU constituent des violations du droit de la consommation, relevant notamment :

- l'affichage de réductions inexistantes pour inciter à l'achat ;
- des annonces trompeuses sur des stocks limités ou des délais d'achat fictifs pour faire pression sur les internautes ;
- La publication d'avis clients falsifiés ;
- un manque de clarté et de transparence sur les droits de retour et les remboursements.
- L'absence de moyens accessibles pour que les consommateurs posent des questions ou déposent des réclamations.
- Une conception addictive des services, notamment à travers des programmes de récompenses gamifiés.
- Un manque de transparence sur les critères des systèmes de recommandation et absence d'une option accessible pour les utilisateurs souhaitant désactiver le profilage.

- Le non-respect des obligations liées à la mise à disposition des données accessibles au public, notamment sur les algorithmes de recommandation.

De plus, le Réseau CPC a demandé des informations supplémentaires à TEMU pour évaluer la conformité de l'entreprise avec d'autres obligations légales européennes, telles que :

- l'obligation d'informer clairement les consommateurs si le vendeur d'un produit est un commerçant ou non ;
- l'obligation de garantir que les classements, avis et notes des produits ne sont pas présentés de manière trompeuse ;
- l'obligation d'assurer que les réductions de prix sont annoncées et calculées correctement ; et
- l'obligation de vérifier que toute allégation environnementale est précise et justifiée.

La procédure formelle ouverte par la Commission Européenne à l'encontre de TEMU

Les domaines de la procédure formelle

TEMU dépasse les 45 millions d'utilisateurs réguliers au sein de l'UE, et a par conséquent, été désigné comme une très grande plateforme en ligne, le 31 mai 2024 en vertu du DSA.

Conformément au DSA, TEMU était tenu de fournir un rapport d'évaluation des risques liés à l'utilisation de sa plateforme. Ce rapport a fait l'objet de demandes formelles d'informations par la Commission les 28 juin et 11 octobre 2024.

Au regard des informations partagées, d'une part, par TEMU, et d'autre part, par le Réseau CPC, la Commission Européenne a décidé d'ouvrir une procédure formelle à l'encontre de la plateforme.

La procédure se concentre sur les domaines suivants :

- Les systèmes que TEMU a mis en place pour limiter la vente de produits non conformes dans l'Union européenne. Cela concerne, entre autres, les systèmes conçus pour limiter la réapparition de commerçants frauduleux suspendus par le passé, connus pour avoir vendu des produits non conformes, ainsi que les systèmes visant à limiter la réapparition de produits non conformes.
- Les risques liés à la conception addictive du service, y compris les programmes de récompenses à caractère ludique, et les systèmes que TEMU a mis en place pour atténuer les risques découlant de cette conception addictive, qui pourraient entraîner des conséquences négatives sur le bien-être physique et mental des personnes.
- Le respect des obligations prévues par le DSA (Digital Services Act) en lien avec la manière dont TEMU recommande des contenus et des produits aux utilisateurs. Cela inclut l'exigence de divulguer les principaux paramètres utilisés dans les systèmes de recommandation de TEMU et de fournir aux utilisateurs au moins une option facilement accessible qui ne soit pas basée sur le profilage.
- Le respect de l'obligation prévue par le DSA permettant aux chercheurs d'accéder aux données publiquement accessibles de TEMU.

Les prochaines étapes de la procédure formelle

TEMU disposait d'un mois pour répondre aux conclusions de la Commission Européenne et proposer des engagements sur la manière dont elle compte résoudre les manquements au DSA.

On attend désormais que la Commission Européenne, mais en fonction de la réponse de TEMU, les autorités nationales pourront prendre des mesures coercitives pour garantir la conformité de TEMU. Cela inclut la possibilité d'imposer des amendes basées sur le chiffre d'affaires annuel de TEMU dans les États membres concernés (jusqu'à 6 % de son chiffre d'affaires mondial annuel au cours de l'exercice précédent).

D'autres actions nationales sont en cours contre TEMU pour violation des droits des consommateurs, et plusieurs autorités ont indiqué surveiller étroitement la plateforme :

- l'Autorité hongroise de la concurrence,
- l'Office polonais de la concurrence et de la protection des consommateurs et
- la Direction générale de la politique de concurrence, des affaires des consommateurs et de la répression des fraudes en France.

Sources :

- Source 1
- Source 2

MARCHES PUBLICS : LA CJUE PRECISE LES MODALITES D'APPRECIATION DE LA RESPONSABILITE DE L'ACHETEUR DANS L'EXISTENCE D'UNE SITUATION D'EXCLUSIVITE

Dans l'arrêt du 9 janvier 2025, la Cour de justice de l'Union européenne (CJUE) a clarifié les conditions de recours à la procédure négociée sans publication préalable d'un avis de marché, notamment en ce qui concerne la protection des droits d'exclusivité.

Contexte de l'affaire

La Direction générale des finances (DGF) de la République tchèque a attribué un marché public à la société IBM pour la maintenance d'un système informatique de gestion des impôts, en recourant à une procédure négociée sans publication préalable.

L'utilisation de cette procédure était justifiée par des raisons techniques et la protection des droits d'auteur d'IBM sur le code source du système. L'autorité de la concurrence tchèque a contesté cette procédure, estimant que la situation d'exclusivité était imputable au comportement antérieur du ministère des Finances, prédécesseur de la DGF, dès lors que le contrat initial stipulait qu'IBM était titulaire des droits de licence du système.

Analyse de la CJUE

La CJUE rappelle que le recours à la procédure négociée sans publication préalable est une exception aux principes de publicité et de mise en concurrence, et doit être interprété de manière stricte. Pour invoquer la protection des droits d'exclusivité en tant que justification, deux conditions cumulatives doivent être remplies :

1. **Existence de raisons techniques ou de droits d'exclusivité** : le marché doit être attribué à un opérateur déterminé en raison de spécifications techniques ou de droits d'exclusivité liés à l'objet du marché.
2. **Nécessité absolue d'attribuer le marché à cet opérateur** : il doit être démontré que l'attribution à un autre opérateur est impossible.

La Cour ajoute une troisième condition implicite :

3. **Absence d'imputabilité de la situation d'exclusivité au pouvoir adjudicateur** : le pouvoir adjudicateur ne doit pas être responsable de la situation d'exclusivité invoquée.

En l'espèce, cette dernière condition doit s'apprécier en tenant compte des circonstances entourant la conclusion du contrat initial et de la période précédant le recours à la procédure négociée. **Le pouvoir adjudicateur doit démontrer qu'il ne disposait pas de moyens réels et raisonnables pour mettre fin à la situation d'exclusivité avant de recourir à cette procédure**.

Ainsi, s'agissant de la responsabilité du pouvoir adjudicateur dans l'existence d'une situation d'exclusivité, la CJUE invite la juridiction nationale à déterminer :

- Si le comportement du pouvoir adjudicateur est à l'origine de l'apparition d'une situation d'exclusivité,

- Si la perpétuation d'une telle situation d'exclusivité jusqu'à la décision de suivre la procédure négociée sans mise en concurrence est due à l'action ou à l'inaction de ce même pouvoir adjudicateur.

Cette décision souligne l'importance pour les pouvoirs adjudicateurs de justifier rigoureusement le recours à la procédure négociée sans publication préalable, en démontrant non seulement l'existence de raisons techniques ou de droits d'exclusivité, mais aussi l'absence de responsabilité dans la création ou le maintien de la situation d'exclusivité.

Cette décision appelle à une grande vigilance dans la rédaction des contrats informatiques, notamment des contrats de licence, afin de concilier la nécessité de transparence et les impératifs techniques des acheteurs dans leurs choix de procédure de passation.

Source : ici