

COLLOQUE

Journée d'actualisation du droit de l'internet

**En partenariat avec l'Association Française
des Juristes d'Entreprises
(AFJE)**

Vendredi 20 mars 2026

Dossier Documentaire
Faculté de Droit et de Science Politique de Montpellier



Nous souhaitons tout d'abord exprimer notre gratitude à Madame Agnès Robin pour son engagement à organiser chaque année cette journée et pour le temps qu'elle a consacré à la préparation de ce colloque.

Nos remerciements s'adressent également à l'Association Française des Juristes d'Entreprise, partenaire de cet événement, ainsi qu'à l'ensemble des intervenants, qu'ils soient professionnels ou universitaires, pour leur précieuse contribution à la réussite de celui-ci.

Rédaction assurée par :
Inès ABAOUBIDA
Hayat AMEUR
Sara BROSSY
Julie DELORT
Émilie DOUMENC
Marieme PEDANDOLA
Mexcan FAYE
Elcia HENNUIN
Lia LAVERGNE
Angèle MANDINE
Léa MARCELLIN
Lola PASCALIS
Rosalba REGEA
Urielle TOHOZIN
Meriem ZIDANE



SOMMAIRE

Internet et responsabilité des prestataires techniques

Par Arnaud Diméglio, Docteur en Droit, Avocat à la Cour, Montpellier

- ❖ CA Paris, pôle 5, ch. 11, 24 janv. 2025, n° 21/10238 : *JurisData* n° 2025-002109 ; *Comm. com. électr.* 2025, comm. 32, G. Loiseau
- ❖ Cass. 1re civ., 26 févr. 2025, n° 23-16.762, FS-B+R : *JurisData* n° 2025-002117 ; *Comm. com. électr.* 2025, comm. 31, G. Loiseau
- ❖ TJ Rennes, réf., 16 déc. 2024, n° 24/00325 : *Comm. com. électr.* 2025, alerte 92.
- ❖ TJ Paris, réf., 31 déc. 2024, n° 24/57566 : *Comm. com. électr.* 2025, alerte 93.
- ❖ CA Colmar, 2e ch. A, 25 oct. 2024, n° 23/03252 : *JurisData* n° 2024-019856 ; *Comm. com. électr.* 2025, alerte 19, Cabinet Racine.
- ❖ CE, 1er avr. 2025, n° 494511, 494583 et 495174 : *JurisData* n° 2025-004277 ; *Dr. adm.* 1er juillet 2025, comm. 24, G. Eveillard ; *Comm. com. électr.* 2025, comm. 68, E. Raschel ; *Procédures* 2025, comm. 165, N. Chiffot.
- ❖ ARCOM, délib. n° 2024-20, 9 oct. 2024, relative au référentiel : *JO* 22 oct. 2024, texte n° 50 ; *Comm. com. électr.* 2024, comm. 110, E. Raschel.

Internet et protection des données personnelles

Par Laura Tomasso, Docteure en droit privé, Post-Doctorante (LICeM)

- ❖ CJUE, 4 sept. 2025, aff. C-413/23 P, *CEPD c/ CRU* : *JurisData* n° 2025-017721
- ❖ Cass. soc., 26 mars 2025, n° 23-16.068, F-B : *JurisData* n° 2025-003380 ; *JCP S* 2025, 1170, B. Gauriau
- ❖ CJUE, 4 oct. 2024, aff. C-446/21, *Schrems* : *Europe* 2024, comm. 485, note M. Glinel
- ❖ CJUE, 9 janv. 2025, aff. C-394/23, *Mousse* : *JurisData* n° 2025-001551 ; *Comm. com. électr.* 2025, comm. 38, A. Danis-Fatôme

Internet et droit de la propriété intellectuelle

Par Sandrine Roose-Grenier, Maître de conférences à l'Université de Montpellier

- ❖ CJUE, 1re ch., 17 oct. 2024, aff. C-159/23, *Sony Computer Entertainment Europe Ltd c/ Datel Design and Development Ltd, Datel Direct Ltd, JS*, *Comm. com. électr.* 2024, comm. 104, P. Kamina ; *Europe* 2024, comm. 480, C. Grudler
- ❖ Cass. com., 15 janv. 2025, n°23-14.625, FS-B : *JurisData* n°2005-000198 ; *JCP E* 2025, 1172 P. Storrer ; *Comm. com. électr.* 2025, comm. 20, P. Kamina ; *Comm. com électr.* 2025, comm. 23, G Loiseau ; *Resp. civ et assur.* 2025, comm. 58, L. Bloch
- ❖ TJ Marseille, 20 mars 2025, n° 23/00046.

- ❖ CA Paris, pôle 1, ch. 2, 25 septembre 2025, n° 24/17261 : *JurisData* n° 2025-019599
- ❖ Cass. com., 26 mars 2025, n° 23-13.589, FS-B : *JurisData* n° 2025-003413 ; *JCP E* 2025, act. 312
- ❖ United States Court of Appeals for the District of Columbia Circuit, 18 mars 2025, n° 23-5233, *S. Thaler v. S. Perlmutter*

Internet et droit de la consommation

Par Malo Depincé, Professeur en Droit privé à l'Université de Montpellier, Directeur du LICeM

- ❖ TJ Paris, 22 oct. 2024, n° 17/06842 : *Comm. com. électr.* 2025, alerte 12.
 - ❖ CAA Paris, 9e ch., 7 févr. 2025, n° 23PA03283, inédit.
 - ❖ D. n° 2024-753, 7 juill. 2024 *modifiant le Code de la consommation en ce qui concerne les obligations d'information des fournisseurs de comparateurs en ligne, de places de marché en ligne et d'agrégateurs de contenus d'actualité en ligne.*
 - ❖ D. n° 2025-9, 3 janv. 2025, *désignant l'autorité administrative chargée de la concurrence et de la consommation compétente en matière de saisine de la juridiction civile en application de l'article L. 133-2 du Code de la consommation et compétente en application de l'article 7 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.*
- **Services numériques**
 - ❖ PE et Cons. UE, dir. (UE) 2024/2853, 23 oct. 2024, *relative à la responsabilité du fait des produits défectueux et abrogeant la directive 85/374/CEE du Conseil : JOUE L*, 18 nov. 2024
 - ❖ Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 *concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) n° 168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828, JOUE L*, 20 nov. 2024.
- **Pouvoirs de la DGCCRF**
 - ❖ TA Lyon, 6e ch., 19 mars 2024, n° 2204832, inédit.
 - ❖ CAA Paris, 9e ch., 7 févr. 2025, n° 23PA03283, inédit.
 - ❖ DGCCRF, « *Fast fashion : SHEIN sanctionné d'une amende de 40 millions d'euros* », communiqué de presse, 3 juillet 2025.
 - ❖ DGCCRF, « *Amende transactionnelle de 600 000 euros à l'encontre de la société SHOWROOMPRIVE.COM* », communiqué de presse, 11 juillet 2025.
 - ❖ DGCCRF, injonction faite à Booking le 10 juillet 2025 de mettre en conformité ses CGU avant fin décembre 2025.
- **Influenceurs**
 - ❖ Ord. n° 2024-978, 6 nov. 2024, *modifiant la loi n° 2023-451 du 9 juin 2023 visant à encadrer l'influence commerciale et à lutter contre les dérives des influenceurs sur les réseaux sociaux : JO* 7 nov. 2024, texte n° 18

Internet et droit du travail

Par Axel Saint-Martin, Avocat, cabinet ASM, Montpellier

- ❖ Cass. soc., 26 novembre 2025, 23-22.415.
- ❖ Cass. soc., 5 novembre 2025, 24-16.208.
- ❖ Cass. soc., 26 février 2025, 22-18.179.
- ❖ Cass. soc., 19 mars 2025, 23-19.154.
- ❖ Cass. soc., 22 janv. 2025, n° 22-15.793, F-D : *JurisData* n° 2025-000530.
- ❖ Cass. soc., 25 sept. 2024, n° 23-11.860, FS-B : *JurisData* n° 2024-016437 ; *Comm. com. électr.* 2024, alerte 336, Cabinet Racine ; *JCP S* 2024, 1331, G. Loiseau.
- ❖ Cass. soc., 25 sept. 2024, n° 23-13.992, FS-B : *JurisData* n° 2024-016440 ; *JCP E* 2024, 1359, B. Bossu.

INTERNET ET RESPONSABILITÉ DES PRESTATAIRES TECHNIQUES

Par Arnaud Diméglio, Docteur en Droit, Avocat à la Cour, Montpellier

CA Paris, pôle 5, ch. 11, 24 janv. 2025, n° 21/10238

Par un arrêt rendu le 24 janvier 2025, la cour d'appel de Paris a jugé que la société Google pouvait légitimement désactiver le compte Gmail et Google Drive d'un avocat ayant stocké sur ce service des images de mineurs à caractère pédopornographique, même lorsque ces fichiers provenaient de dossiers pénaux dans lesquels il intervenait en qualité de défenseur.

Faits - En l'espèce, M. B, avocat, disposait d'un compte de messagerie Gmail associé au service de stockage en ligne Google Drive, utilisé à la fois à des fins personnelles et professionnelles. Sur cet espace de stockage, il conservait notamment des fichiers d'images de mineurs à caractère pédopornographique provenant de dossiers pénaux dans lesquels il intervenait comme avocat de la défense.

En janvier 2021, les sociétés Google ont détecté la présence de ces fichiers et ont ainsi suspendu le compte de l'intéressé, au motif qu'il « *semblait être utilisé d'une manière enfreignant gravement les règles de Google* ». La société Google Ireland a également procédé au signalement de ces contenus à l'association américaine National Center for Missing and Exploited Children (NCMEC), spécialisée dans la lutte contre l'exploitation sexuelle des mineurs.

Selon la cour d'appel de Paris, la présence d'images pédopornographiques sur le compte Google Drive de l'utilisateur constituait une violation des conditions d'utilisation du service et justifiait la mise en œuvre de la clause résolutoire permettant la suspension du compte. La juridiction relève que la société Google, en sa qualité d'hébergeur, est tenue d'agir promptement afin de retirer ou rendre inaccessible les contenus manifestement illicites dont elle a connaissance, conformément à la loi pour la confiance dans l'économie numérique (LCEN).

La cour estime en outre qu'il n'appartenait pas à la plateforme de vérifier la légitimité de la détention de ces fichiers par l'utilisateur ni d'apprécier s'ils étaient conservés dans le cadre de l'exercice des droits de la défense. Elle juge également que le signalement de ces contenus à l'association NCMEC ne constitue pas une faute, cette démarche s'inscrivant dans les obligations de lutte contre la diffusion de contenus pédopornographiques.

- Extraits -

« En tout état de cause, l'analyse intellectuelle de la détention des fichiers litigieux à des fins légitimes n'étant pas requise, la seule présence matérielle des 77 images d'images de mineurs à caractère pornographique sur le compte Google Drive de M. [B], portant atteinte aux droits des victimes, est sanctionnée tant par la loi que par les conditions particulières de Google Drive de sorte que la société Google pouvait légitimement se prévaloir de la clause résolutoire.

« Ainsi, la société Google ayant eu connaissance du caractère manifestement illicite des contenus stockés par M. [B] sur son compte Google Drive, elle était fondée à mettre en œuvre sans délai la clause résolutoire en raison de sa qualité d'hébergeur et de son obligation légale d'agir promptement pour retirer des données dont ils connaissent le caractère illicite ou pour

en rendre l'accès impossible et ceci, sous peine d'engager sa responsabilité en cas de manquement à cette obligation ainsi que le prescrit l'article 6, I, 2° de la LCEN précité. »

Cass. 1^{re} civ., 26 févr. 2025, n° 23-16.762, FS-B+R

Par un arrêt du 26 février 2025, la première chambre civile de la Cour de cassation s'est prononcée sur la responsabilité d'un hébergeur de contenus en ligne. Elle a rejeté le pourvoi formé par la société DStorage contre l'arrêt de la cour d'appel de paris du 12 avril 2023, qui avait retenu sa responsabilité pour ne pas avoir retiré des contenus manifestement illicites signalés par les titulaires de droits sur plusieurs jeux vidéo.

Faits – La société Nintendo Co., Ltd., qui commercialise notamment les jeux vidéo tels que « *Pokémon* » et d'autres jeux célèbres, invoquait être co-titulaire de droits d'auteur avec les sociétés The Pokémon Company, Creatures Inc. et Game Freak Inc.

Elles ont constaté que des liens permettant de télécharger des copies non autorisées de plusieurs jeux vidéo étaient accessibles via le service d'hébergement exploité par DStorage sur le site 1fichier.com. Par lettres recommandées des 22 et 30 janvier 2018, les sociétés co-titulaires ont notifié à DStorage la présence de ces contenus et ont demandé leur retrait. Les liens étant toujours accessibles, elles ont assigné la société DStorage en responsabilité et indemnisation et en retrait des liens sous astreinte.

La cour d'appel de Paris a considéré que les notifications adressées à l'hébergeur étaient valables et que celui-ci n'avait pas agi promptement pour retirer les contenus signalés. Elle a donc retenu sa responsabilité en qualité d'hébergeur et lui a ordonné de retirer ou bloquer l'accès aux contenus litigieux sous astreinte.

La Cour de cassation confirme cette solution et rejette le pourvoi.

Elle rappelle que, selon la Loi pour la confiance dans l'économie numérique (LCEN), la responsabilité d'un hébergeur peut être engagée s'il ne retire pas promptement des contenus dont le caractère manifestement illicite lui a été notifié.

Elle approuve la cour d'appel d'avoir considéré que les notifications adressées à DStorage répondaient aux exigences légales et permettaient à l'hébergeur d'avoir connaissance du caractère manifestement illicite des contenus signalés.

Elle juge également que la mesure ordonnée (retrait ou blocage de l'accès à certains contenus déterminés) ne constitue pas une obligation générale de surveillance mais une surveillance ciblée et temporaire, conforme à la LCEN.

- Extraits -

« 9. La loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN), dans sa rédaction issue de la loi n° 2016-444 du 13 avril 2016, prévoit que les personnes physiques ou morales, qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services, peuvent voir leur responsabilité civile engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces services seulement si, dès le moment où elles ont eu connaissance de leur caractère manifestement illicite, elles n'ont pas agi promptement pour retirer ces données ou en rendre l'accès impossible.

18. Si, selon l'article 6-I.7 de la LCEN dans sa rédaction issue de la loi n° 2016-444 du 13 avril 2016, les personnes morales, qui assurent le stockage en ligne de signaux, d'écrits,

d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services, ne sont pas soumises à une obligation générale de surveiller les informations qu'elles transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites, elles peuvent se voir imposer une activité de surveillance ciblée et temporaire par l'autorité judiciaire.

19. C'est à bon droit que la cour d'appel a retenu que la mesure ordonnée, consistant en un retrait du site internet de la société DStorage « <https://1fichier.com> » ou un blocage de l'accès aux contenus constituant des copies des jeux vidéo précités, sous une astreinte limitée à six mois, n'imposait à cette société qu'une activité de surveillance ciblée sur des contenus très précis et temporaire.

20. Le moyen n'est donc pas fondé.

PAR CES MOTIFS, la Cour : REJETTE le pourvoi »

TJ Rennes, réf., 16 déc. 2024, n° 24/00325.
--

Par un jugement du 16 décembre 2024, le tribunal judiciaire de Rennes a déclaré le cabinet d'avocats irrecevable en ses prétentions dirigées contre Google, estimant qu'il ne disposait pas d'un motif légitime suffisant pour obtenir la communication par l'hébergeur de données techniques de connexion.

Faits - Des avis négatifs ont été publiés sur la fiche professionnelle du cabinet d'avocats CIME AVOCATS, spécialisé en droit des affaires à Rennes, accessible via le moteur de recherche GOOGLE.

Le cabinet d'avocat a saisi le tribunal judiciaire de Rennes par une procédure en référé afin d'obtenir la communication de données permettant d'identifier les auteurs de ces avis, notamment les données techniques de connexion (adresse IP et informations relatives aux équipements terminaux), à l'encontre des sociétés GOOGLE, sur le fondement de l'article 10 du code civil et de l'article 145 du code de procédure civile.

Selon le tribunal, la publication d'avis négatifs sur une fiche professionnelle en ligne ne constitue pas un motif légitime, au sens de l'article 145 du Code de procédure civile, justifiant la communication des données techniques de connexion permettant d'identifier leurs auteurs. Le demandeur est en conséquence débouté de ses demandes et condamné aux dépens.

Le juge fait une lecture combinée de l'article 145 du code de procédure civile, de l'article 6-II de la loi du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) et des dispositions du code des postes et des communications électroniques que les hébergeurs de contenus sur internet ne sont tenus de communiquer, sur le fondement de l'article 145, que certaines informations relatives à l'utilisateur. Ainsi, peuvent être communiquées les informations relatives à l'identité civile de l'utilisateur, les données fournies lors de la création du compte ou de la souscription du service, ainsi que les informations relatives au paiement. En revanche, les données techniques permettant d'identifier la source de la connexion, notamment l'adresse IP ou les informations relatives aux équipements terminaux utilisés, sont exclues de cette communication. Ces données ne peuvent être conservées et communiquées que pour les besoins de la lutte contre la criminalité et la délinquance grave, de la prévention des menaces grâce contre la sécurité publique ou de la sauvegarde de la sécurité nationale.

- Extraits -

« Il résulte de la combinaison de ces textes qu'il peut être ordonné à une partie (Civ. 2^{ème}, 06 novembre 2008 n° 07-17.398 Bull. 2008, II, n° 234) ou à des tiers (Civ. 2^{ème}, 26 mai 2011 n° 10-20.048 Bull 2011, II, n° 118), sur requête ou en référé, de produire tous documents et données qu'ils détiennent s'il existe un motif légitime de conserver ou d'établir avant tout procès la preuve des faits dont pourrait dépendre la solution d'un litige.

Il résulte de la combinaison de ces textes et de l'article 145 du code de procédure civile susvisé que les hébergeurs de contenus sur internet ne sont tenus de communiquer, pour les besoins des procédures pénales, que les informations relatives à l'identité civile de l'utilisateur et les autres informations fournies par lui lors de la souscription du contrat ou de la création du compte ainsi que les informations relatives au paiement, à l'exclusion des données techniques permettant d'identifier la source de la connexion ou de celles relatives aux équipements terminaux utilisés, notamment l'adresse IP. Ces dernières données ne peuvent être conservées et communiquées que pour les besoins de la lutte contre la criminalité et la délinquance grave, de la prévention des menaces graves contre la sécurité publique et de la sauvegarde de la sécurité nationale. »

TJ Paris, réf., 31 déc. 2024, n° 24/57566
--

Par une ordonnance de référé du 31 décembre 2024, le tribunal judiciaire de Paris a enjoint à la société TWITTER INTERNATIONAL UNLIMITED COMPANY de communiquer les données permettant d'identifier l'auteur de messages de menaces de mort publiés anonymement sur le réseau social X. Cette décision illustre l'articulation entre le droit à la preuve dans la perspective d'un procès pénal, fondé sur l'article 145 du code de procédure civile, et les conditions légales de communication des données personnelles conservées par les hébergeurs en application du code des postes et des communications électroniques. Elle apporte également une précision notable sur la notion de « délinquance grave » permettant la communication des données techniques d'identification de la source de connexion, et sur la nécessité d'assurer l'exécutabilité concrète de l'injonction en ordonnant la communication de l'horodatage exact à la seconde, rendue indispensable par la généralisation des adresses IP « nattées ».

Faits – Le litige oppose ici M. C., agissant en son nom personnel et en qualité de représentant légal de son fils mineur J. C., ainsi que Mme L., en qualité de représentante légale du même enfant, à la société Twitter International Unlimited Company. En l'espèce, à la suite de la diffusion d'une photographie de M. C. sur le réseau X, un utilisateur anonyme titulaire du compte litigieux a publié le 10 septembre 2024 plusieurs commentaires évoquant des actes de vengeance à l'encontre de M. C. et de son fils, enfant scolarisé en école maternelle. L'auteur des messages indiquait notamment rechercher l'adresse et les horaires de l'école de l'enfant, se référant à plusieurs reprises à des actes de vengeance violents et à une référence tirée d'un animé japonais mettant en scène un duel à mort. Souhaitant pouvoir identifier l'auteur anonyme de ces messages afin d'engager des poursuites pénales du chef de menaces de mort, M. C. et Mme L. ont assigné la société Twitter International Unlimited Company devant le juge des référés du tribunal judiciaire de Paris sur le fondement de l'article 145 du code de procédure civile, aux fins d'obtenir la communication des données d'identification du titulaire du compte litigieux, ainsi que des données techniques permettant d'identifier la source des connexions, et notamment l'horodatage exact des publications. La société TWITTER INTERNATIONAL UNLIMITED COMPANY s'opposait à titre principal à toute

communication, contestant l'existence d'un motif légitime faute de menaces de mort caractérisées, et subsidiairement à la communication des données techniques au motif que les faits visés ne relevaient pas de la « délinquance grave » au sens de l'article L. 34-1 du code des postes et des communications électroniques. Elle contestait également la légalité de la communication des horaires et fuseaux horaires de connexion, selon elle réservée à la seule sauvegarde de la sécurité nationale. La question qui se posait au juge des référés était donc de savoir si les conditions de l'article 145 du code de procédure civile étaient réunies pour ordonner la communication de ces données, notamment si les faits dénoncés relevaient de la « délinquance grave » et si le juge pouvait, pour assurer l'exécutabilité de sa décision, ordonner la communication de l'horodatage à la seconde près des publications litigieuses. Le juge des référés a fait droit à la demande dans son ensemble, à l'exception de la communication de l'adresse IP de destination et du prononcé d'une astreinte, considérant que le délit de menace de mort, puni de trois ans d'emprisonnement et commis à l'encontre d'un père et de son fils mineur via un réseau social assurant anonymat et diffusion rapide, relevait bien de la délinquance grave, et que l'horodatage exact constituait une précision technique nécessaire à l'exécution de l'injonction.

- Extraits -

« Selon l'article 145 du code de procédure civile, s'il existe un motif légitime de conserver ou d'établir avant tout procès la preuve de faits dont pourrait dépendre la solution d'un litige, les mesures d'instruction légalement admissibles peuvent être ordonnées à la demande de tout intéressé ».

« Contrairement à ce que soutient la société TWITTER INTERNATIONAL UNLIMITED COMPANY, les propos extraits des messages litigieux, dont la réalité n'est pas contestée, peuvent ressortir de la qualification pénale du délit de menaces de morts prévu par l'article 222-17 du code pénal qui dispose que « la menace de commettre un crime ou un délit contre les personnes dont la tentative est punissable est punie de six mois d'emprisonnement et de 7 500 euros d'amende lorsqu'elle est, soit réitérée, soit matérialisée par un écrit, une image ou tout autre objet ».

« Ainsi, en application de ces textes, les hébergeurs sont tenus de conserver, pour les besoins de toutes les procédures pénales, les informations relatives à l'identité civile de l'utilisateur, les autres informations fournies par l'utilisateur lors de la souscription d'un contrat ou de la création d'un compte et les informations relatives au paiement, les premières pendant cinq ans et les autres pendant un an à compter de la fin de validité du contrat ou de la clôture du compte ».

« Enjoignons à la société TWITTER INTERNATIONAL UNLIMITED COMPANY de communiquer, dans un délai maximum de 10 jours à compter de la notification de la présente décision, à M. [M] [C], en son nom personnel et en qualité de représentant légal de son fils mineur [J] [C], et à Mme [K] [L], en qualité de représentante légale de son fils mineur [J] [C], l'ensemble des données d'identification en sa possession, telles que visées à l'article R.10-13 I. II. III. et IV du Code des postes et des communications électroniques, comprenant l'horodatage exact, à la seconde près, et le fuseau horaire de connexion des adresses IP utilisées pour les publications des contenus litigieux, permettant d'identifier - le titulaire du compte ».

Dans cet arrêt, les juges de la Cour d'appel de Colmar confirment une ordonnance rendue par le juge des référés du Tribunal Judiciaire de Strasbourg le 10 août 2023, dans laquelle l'association franco-iranienne d'Alsace a été déboutée de sa demande faite aux sociétés Google France et Google Ireland Limited de retirer des avis négatifs publiés sur un service accessible par le biais de leur moteur de recherche, ainsi que de conserver et de communiquer les données d'identification des auteurs de ces avis. Dans cette ordonnance, il a été déclaré qu'un hébergeur dont l'activité est d'offrir un accès à des services de communication en ligne ne peut voir sa responsabilité engagée s'il n'assure pas la gestion ou le fonctionnement du service concerné, mais exerce uniquement une activité de support marketing dessus. De surcroît, dans cette ordonnance de référé, il a été rappelé qu'en vertu des articles 6, I, 2^{ème}, 6, I, 5^{ème} et 6, I, 7^{ème} de la Loi en la Confiance dans l'Économie Numérique (LCEN) n° 2004-575 du 21 juin 2004, dans leur ancienne version, les hébergeurs et prestataires de services ne sont pas soumis à une obligation générale de surveillance des contenus diffusés sur leurs services. Par ailleurs, les juges rappellent que les dispositions de l'ancien article 6, II de la LCEN et de l'article L.34-1, II, bis, du Code des postes et des communications électroniques, prévoyant une conservation et communication de données relatives à l'identification de certains internautes dans certains cas relevant d'une procédure pénale, ne peuvent pas être d'application dans le cas d'une procédure civile.

Faits - Le 23 août 2023, l'association franco-alsacienne d'Alsace a interjeté appel de l'ordonnance rendue par le juge des référés du Tribunal Judiciaire de Strasbourg le 10 août 2023 à la Cour d'appel de Colmar, dans une affaire l'opposant aux sociétés *Google France* et *Google Ireland Limited* à la suite de trois avis négatifs laissés sur la fiche d'établissement de son service de transports, accessible sur le service "*Google My Business*" grâce au moteur de recherche "*Google Search*", ayant donné lieu à l'agression d'un conducteur travaillant pour son service. L'association a auparavant adressé une notification de contenu illicite à ces dernières et leur a fait sommation de retirer les avis litigieux ainsi que de communiquer les données d'identification des auteurs de ces avis. Dans ses prétentions, l'association demande le retrait des avis litigieux, l'interdiction de diffusion ultérieure des commentaires disponibles aux URL mentionnés et la communication des données permettant l'identification des auteurs des avis litigieux, en se fondant sur l'article 1240 du Code civil notamment. Dans l'ordonnance, le juge des référés s'est fondé sur les articles précités de la LCEN et du Code des postes et des communications électroniques pour décréter qu'il n'y a pas lieu à référé et a débouté l'association de son action puisque seule la responsabilité de la société *Google Ireland Limited* peut être recherchée, la société *Google France* n'exploitant pas le moteur de recherche "*Google Search*" qui permet d'accéder au service "*Google My Business*" et n'assurant pas la gestion et le fonctionnement de ce service-ci. Le juge des référés rappelle que les hébergeurs ne sont pas soumis à une obligation générale de surveillance des informations transmises ou stockées, ni à une obligation de rechercher des faits ou des circonstances révélant des activités illicites et que la communication des données d'identification des auteurs doit être justifiée par un intérêt légitime qui ne peut relever d'une procédure civile. Les juges de la Cour d'appel de Colmar ont confirmé l'ordonnance de référé au visa des articles précités de la LCEN, L.34-1 du Code des postes et des communications électroniques ainsi que 835 alinéa 1, 145 et 700 du Code de procédure civile, rappelant que l'action ne peut être menée contre la société *Google France* puisqu'elle n'exerce pas une activité de gestion ou de fonctionnement du support "*Google My Business*" et qu'il ne peut être demandé à un hébergeur ou à un prestataire de services de prendre des mesures pour éviter la diffusion ultérieure de tels avis

puisque cela s'apparenterait à une obligation de surveillance et nécessiterait la mise en place d'un dispositif de blocage sans limitation de temps, ce qui est disproportionné en l'espèce. Ils rappellent aussi que l'association n'ayant pas l'intention de recourir à une procédure pénale, elle ne peut se prévaloir des dispositions de l'article L.34-1 précité, qui dérogent aux obligations d'effacement ou/et d'anonymisation des données et de secret professionnel prévu à l'article 6, III, 2^{ème} de la LCEN. Les magistrats précisent par ailleurs que le fait qu'un hébergeur indique être encore en possession des données permettant l'identification des internautes, ne constitue pas un motif légitime à la demande de leur communication.

Sur le fond de l'affaire, l'association évoque notamment l'article 6, I, de la LCEN qui pose une présomption de connaissance des faits litigieux par l'hébergeur dès lors que les faits litigieux lui ont été notifiés par toute personne lésée ou intéressée, pour rappeler que la société *Google* étant un prestataire technique, et a fortiori un hébergeur, dont l'activité est d'offrir un accès à des services de communication en ligne, elle peut voir sa responsabilité engagée et a déclaré qu'en dépit des dispositions prévues par l'article L.34-1 du Code des postes et des communications électroniques, elle dispose d'un motif légitime à sa demande puisque la société *Google* peut communiquer les données d'identification des auteurs, les ayant en sa possession. Les juges ont donc voulu rappeler les contours de ces dispositions.

- Extraits -

« Pour statuer ainsi, il a retenu que la société Google Ireland Ltd était seule exploitante du service de recherche sur internet comprenant le moteur de recherche 'Google search' permettant d'accéder aux fiches des entreprises et aux avis laissés par les utilisateurs de services ou clients, et qu'il n'était pas démontré que la société Google France avait une responsabilité directe dans le fonctionnement de ce moteur de recherche.

Il a ajouté qu'il n'y avait pas lieu à référé sur la demande d'interdiction de toute diffusion ultérieure, non explicitée, qui présentait un caractère général et était manifestement disproportionnée, outre que, selon l'article 6, I, 7° de LCEN, les hébergeurs ne sont pas soumis à une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites.

Se fondant sur les articles 6, II de la LCEN et L.34-1, II bis, du code des postes et communications électroniques, il a énoncé que la possibilité d'accéder aux données permettant l'identification est cantonnée dans des limites strictes, notamment en termes de finalités étrangères à la procédure civile.

3. [...] Ainsi, sauf à méconnaître ces textes, il ne peut être ordonné à un hébergeur ou à des prestataires de services de référencement de prendre toutes mesures utiles pour prévenir toutes nouvelles mises en ligne des avis litigieux, sans nouvelle notification régulière, et de lui interdire de les diffuser, une telle mesure aboutissant à les soumettre, au-delà de la seule faculté d'ordonner une mesure propre à prévenir ou à faire cesser le dommage lié au contenu actuel du site en cause, à une obligation générale de surveillance des images qu'ils stockent et de recherche des reproductions illicites, et à leur prescrire, de manière disproportionnée par rapport au but poursuivi, la mise en place d'un dispositif de blocage sans limitation dans le temps. »

Dans cet arrêt, les juges font droit à une requête conjointe de trois individus souhaitant faire annuler pour excès de pouvoir une décision prise par le Premier ministre d'interrompre l'accès au service de communication en ligne « TikTok », qui s'inscrit dans un contexte d'état d'urgence en Nouvelle-Calédonie. Malgré le fait qu'une telle mesure soit possible dans le cadre de circonstances exceptionnelles, les juges rappellent ici qu'elle doit se conformer à certaines conditions pour être valable, en raison de son caractère attentatoire aux droits et libertés d'expression, de communication des idées et opinions ainsi que d'accès à l'information.

Faits – Le 14 mai 2024, le Premier ministre a pris la décision d'interrompre l'accès aux services de communication au public en ligne « TikTok » sur le territoire de la Nouvelle-Calédonie en raison de circonstances exceptionnelles de troubles à l'ordre public relevant d'une certaine gravité, s'inscrivant dans un contexte de révision constitutionnelle portant modification du corps électoral au congrès et aux assemblées de province de la Nouvelle-Calédonie, qui a entraîné des émeutes ainsi que de violents affrontements entre des groupes armés conduisant à plusieurs décès, à des destructions et dégradations de bâtiments et d'infrastructures publics, ainsi qu'à des agressions et affrontements directs avec des personnes tentant de traverser les barrages bloquant les voies de circulation. Mais également, une mutinerie s'est produite et des tentatives d'évasion au centre pénitentiaire de Nouméa ont eu lieu. Tous ces événements se sont déroulés les 14 et 15 mai 2024. La décision a été appliquée à partir du 15 mai 2024 par le recours à des dispositifs techniques mis en œuvre par l'Office des postes et télécommunications de Nouvelle-Calédonie entre autres, l'état d'urgence ayant été déclaré en conseil des ministres sur le territoire de la Nouvelle-Calédonie ce même jour, qui a été levé douze jours plus tard. A la suite de cette mesure, trois requêtes en demande d'annulation pour excès de pouvoir ont émané de la Ligue des droits de l'homme, de l'association « *La Quadrature du net* » ainsi que de trois individus. Ces requêtes ont été jointes par les juges du Conseil d'État. Dans leur décision, les magistrats décident d'annuler la décision prise par le Premier ministre le 14 mai 2024 visant à interrompre l'accès au service de communication au public en ligne « TikTok » en Nouvelle-Calédonie et condamnent l'État à verser une somme de 3 000 euros en vertu de l'article L.761-1 du Code de justice administrative aux requérants, tout en prévoyant la notification de cette décision à ces derniers et de l'adresser en copie aux ministres des Outre-Mer et de l'Intérieur. Pour statuer de la sorte, les magistrats du Conseil d'État ont en premier lieu rappeler que toute mesure prise par une autorité administrative pour pourvoir aux besoins nécessaires dans le cadre d'une situation d'urgence, doit être indispensable à la situation concernée à la date de la décision et doit faire l'objet d'un contrôle entier de la part du juge administratif. Ils se fondent sur l'article 1^{er} de la loi du 3 avril 1955 relative à l'état d'urgence et sur l'article 11 de la Déclaration des droits de l'Homme et du Citoyen de 1789 qui comprend la liberté d'accéder aux services de communication au public en ligne et de pouvoir s'y exprimer, précisant que dans certains cas prévus par la loi, dans le cadre de circonstances exceptionnelles notamment, ces services puissent être interrompus provisoirement si aucune autre mesure moins attentatoire à cette liberté n'est possible et que la durée de cette interruption n'excède pas celle requise pour rechercher et mettre en place une autre mesure. Ils se fondent également sur les dispositions de l'article 11, II, de la loi du 3 avril 1955 qui prévoient que le ministre de l'Intérieur peut prendre toute mesure permettant d'assurer l'interruption de tout service de communication au public en ligne exhortant à la commission d'actes de terrorisme ou en en faisant l'apologie et qu'en l'occurrence, même s'il n'est pas question de terrorisme, le Premier ministre peut

décider de recourir à cet article si d'autres mesures moins attentatoires aux droits et libertés ne sont de nature à pourvoir aux nécessités de la situation. Malgré le fait que les juges reconnaissent que l'autorité administrative ait le droit de décider d'interrompre l'accès à un service de communication en ligne dans un contexte de circonstances exceptionnelles, ils décident de tout de même annuler la décision rendue par le Premier ministre puisqu'elle prévoit une interruption totale du service « *TikTok* » pour une durée indéterminée, qui est uniquement liée à la persistance des troubles à l'ordre public et non justifiée par l'impossibilité de trouver des mesures alternatives moins attentatoires aux droits et libertés concernés.

- Extraits -

« 6. En l'état actuel des moyens de communication [...] la libre communication des pensées et des opinions, garantie par l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789, implique la liberté d'accéder à ces services et de s'y exprimer.

7. Eu égard aux atteintes portées à la libre communication des pensées et des opinions, à la liberté d'expression et à tous les autres droits et libertés dont un service de communication au public en ligne permet l'exercice, notamment le droit à la vie privée et familiale et la liberté du commerce et de l'industrie, l'autorité administrative ne saurait décider, en dehors des cas prévus par la loi, de l'interruption de l'accès à un tel service. Elle peut cependant recourir à une telle mesure, en cas de circonstances exceptionnelles, si elle est indispensable pour répondre aux nécessités du moment. Dans ce cadre, une interruption complète du service en cause ne saurait être légalement décidée qu'à titre provisoire, à la condition, d'une part, qu'aucun moyen technique ne permette, dans l'immédiat, de prendre des mesures alternatives moins attentatoires aux droits et libertés en cause, et, d'autre part, que l'interdiction soit prise pour une durée n'excédant pas celle requise pour rechercher et mettre en œuvre de telles mesures.

10. [...] Or la décision attaquée procède à une interruption totale du service pour une durée indéterminée, liée seulement à la persistance des troubles à l'ordre public, sans subordonner son maintien à l'impossibilité de mettre en œuvre des mesures alternatives. Les requérants sont, par suite, fondés à soutenir que le Premier ministre a ainsi porté une atteinte disproportionnée à la liberté d'expression, à la liberté de communication des idées et opinions et à la liberté d'accès à l'information. »

ARCOM, délib. n° 2024-20, 9 oct. 2024, relative au référentiel

La présente délibération de l'ARCOM relative au référentiel traite d'une question d'actualité majeure : le respect de la protection des données à caractère personnel par les systèmes de vérification de l'âge mis en place par des prestataires de services et de solutions techniques, en l'occurrence dans le cadre de services diffusant des contenus à caractère pornographique.

Contexte - Cette délibération relative au référentiel résulte d'une série de travaux et d'études de la part de la CNIL, de l'ARCOM et du PEReN portant sur la protection des mineurs en ligne dans le cadre d'accès à des services proposant des contenus à caractère pornographique. Cette délibération a été adoptée à la suite de la directive 2015/1535/UE rendue par le Parlement et le Conseil Européen le 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de l'information, de la loi LCEN du 21 juin 2004, de la notification 2024/0208/Fr adressée à la Commission européenne le 15 avril 2024 et de ses observations en date du 15 juillet 2024,

ainsi que de la délibération du 26 septembre 2024 de la CNIL portant avis sur un projet de référentiel de l'ARCOM relatif aux systèmes de vérification de l'âge mis en place pour l'accès à certains services permettant l'accès à des contenus pornographiques. Par l'adoption de cette délibération, l'ARCOM, dans une optique de protection des mineurs, a souhaité établir un référentiel des règles que les prestataires de services et de solutions techniques doivent respecter pour concilier cette régulation avec la protection des données à caractère personnel. Ce référentiel répertorie pléthore de règles qui sont réparties en quatre parties.

Dans la première partie relative aux considérations générales relatives à la fiabilité des systèmes de vérification de l'âge, sont énoncées les règles auxquelles ces systèmes doivent répondre pour être considérés comme fiables, telles qu'à l'article 1^{er} de la loi SREN du 21 mai 2024 n° 2024-449, qui prévoit que les services diffusant des contenus à caractère pornographique sont tenus d'afficher un écran ne comportant aucun contenu de ce type tant que l'âge de l'utilisateur n'a pas été vérifié en recourant à une protection telle que le floutage complet de la page d'accueil du service, à la prévention et à l'exclusion de tout risque d'erreur et de fraude, au respect de la vérification de l'âge pour chaque accès ainsi qu'au respect de l'article 21 de la Charte des droits fondamentaux de l'Union Européenne pour éviter tout effet discriminatoire.

La deuxième partie de la délibération est relative à la protection de la vie privée, dans laquelle son importance est rappelée en prévoyant que les services concernés et les prestataires de solution technique de vérification de l'âge doivent la concilier avec la sécurité des systèmes de vérification de l'âge. Il est prévu que ces derniers doivent respecter les articles 5 et 25 du RGPD relatifs à la protection de la vie privée, ainsi que ces principes-ci : l'exactitude, la proportionnalité et la minimisation des données collectées ; donner une information concise, transparente, compréhensible et facilement accessible des utilisateurs ; le respect d'une durée de conservation des données appropriées ; la possibilité pour les personnes d'exercer leurs droits d'accès, d'opposition, de rectification, de limitation du traitement, d'effacement et de portabilité des données et la sécurité à l'état de l'art pour les systèmes d'information utilisés dans le cadre de traitements de données à caractère personnel. Mais également, il est prévu que tous les systèmes de vérification de l'âge doivent respecter ces exigences minimales : l'indépendance du prestataire de système de vérification de l'âge vis-à-vis des services visés diffusant de tel contenu ; la confidentialité des données traitées des avis de prestataires de génération de preuve d'âge et d'éventuels autres tiers impliqués ainsi que le respect des mesures de sauvegarde des droits et libertés des personnes en vertu de l'article 22, paragraphe 2, b, du RGPD. Il est aussi prévu que ces services doivent mettre en place un dispositif de vérification de l'âge conforme au mécanisme de « *double-anonymat* » qui a été proposé par la CNIL dans son communiqué de juillet 2022, qui vient renforcer cette protection car il veille à ce que ces services n'aient pas accès à l'identité complète de l'internaute et que les prestataires ne savent pas quels sites il consulte. Il faut aussi que l'utilisateur soit informé si un tiers participe à ce processus et que le recours à ce mécanisme soit affiché de manière claire et lisible. Enfin, sont également préconisés des objectifs souhaitables et des bonnes pratiques à suivre mais qui ne sont pas exigibles pour être en conformité avec le référentiel, qui sont énoncés à la suite des exigences spécifiques prévues pour les systèmes répondant au mécanisme du « *double-anonymat* ».

Dans la troisième partie relative aux solutions de génération de preuve dérogatoires acceptées à titre temporaire, il est prévu, en vertu de l'article 10 de la LCEN, que si les services concernés n'ont pas mis en place un système de vérification de l'âge conforme aux règles de ce référentiel dans un délai de trois mois à compter de sa publication, ils disposent d'une période transitoire de trois mois durant laquelle ils peuvent recourir à une solution nécessitant l'utilisation d'une carte bancaire, sous réserve qu'elle soit mise en œuvre par un tiers indépendant et que ce dernier veille à sa sécurité pour éviter tout risque d'hameçonnage,

s'assure de la validité de la carte bancaire et mette en place une authentification forte conformément à la directive « DSP2 » n° 2015/2366, telle qu'une authentification à double facteur. Enfin, dans la quatrième partie de la délibération, il est énoncé des règles pour l'audit et l'évaluation de ces solutions, prévoyant notamment : que l'ARCOM puisse exiger des éditeurs et fournisseurs de services qu'ils conduisent un audit pour attester de la conformité des systèmes de vérification de l'âge aux exigences de ce référentiel, que l'ARCOM a pour mission de les évaluer et que les services qui diffusent de tels contenus doivent s'assurer que les solutions mises en place sont systématiquement en mesure de répondre aux exigences du référentiel.

- Extraits -

« Le présent document s'inscrit dans le contexte de travaux engagés ces dernières années par la CNIL sur les solutions de vérification d'âge permettant de concilier protection des mineurs et respect de la vie privée. »

« Afin de préserver les exigences en matière de protection de la vie privée qui visent à limiter la capacité des services à identifier les personnes, de telles mesures doivent être mises en place non par le service visé diffusant des contenus à caractère pornographique, mais par le prestataire de solution technique de vérification de l'âge, qu'il soit le fournisseur d'attribut ou l'émetteur de preuve. »

« Le service visé diffusant des contenus à caractère pornographique est tout de même tenu, comme les prestataires de solution technique de vérification de l'âge, de se conformer aux obligations en matière d'information imposées par le RGPD et doit prévenir les utilisateurs de la possibilité d'exercer un recours auprès du fournisseur de la solution de vérification de l'âge. »

« Les services visés diffusant des contenus à caractère pornographique sont tenus de s'assurer que les solutions mises en place sont systématiquement en mesure de répondre aux exigences du référentiel en adaptant, le cas échéant, leurs principes et leurs paramètres de fonctionnement. »

INTERNET ET PROTECTION DES DONNEES PERSONNELLES

Par Laura Tomasso, Docteure en droit privé, Post-Doctorante (LICeM)

CJUE, 4 sept. 2025, aff. C-413/23 P, CEPD c/ CRU

Dans l'arrêt du 4 septembre 2025 CEPD c/ CRU, la Cour de justice de l'Union européenne (CJUE) juge que la pseudonymisation de données ne fait pas sortir les données pseudonymisées du champ de données à caractère personnel. Les juges précisent que néanmoins la qualification dépend du contexte et de la capacité réelle de réidentifier les personnes concernées pour le destinataire au regard des moyens raisonnablement susceptibles d'être utilisés. La Cour souligne ensuite que le responsable du traitement demeure tenu de respecter son obligation de transparence en informant dès la collecte les personnes concernées de la transmission de leurs données à un tiers. Elle censure ainsi l'analyse du Tribunal de l'Union européenne en rappelant que la pseudonymisation n'exonère pas le responsable du traitement de ses obligations d'information prévues par le règlement (UE) 2018/1725.

Faits – L'affaire opposait le Contrôleur Européen de la Protection des données (CEPD) et le Conseil de Résolution Unique (CRU) sur un litige relatif à la qualification des données pseudonymisées et à l'obligation d'information des personnes concernée par le responsable de traitement des données. Le CRU, autorité européenne chargée de la résolution des banques en difficulté, avait demandé à des actionnaires et créanciers affectés de formuler des commentaires sur une décision de résolution bancaire concernant une banque espagnole en difficulté (Banco Popular Español). Le CRU, après pseudonymisation des commentaires, les a ensuite transmis à la société Deloitte, prestataire externe chargé d'analyser les informations pour assister l'autorité. La pseudonymisation consistait en la suppression des éléments permettant d'identifier directement les personnes, et en les remplaçant par des codes alphanumériques auxquels la société Deloitte n'avait pas accès.

A la suite de réclamations faites par les personnes concernées par la collecte des commentaires, le CEPD a estimé par une décision du 24 juin 2020 que le CRU avait manqué à son obligation d'informer ces personnes que leurs données seraient transmises à Deloitte, et a donc considéré que cela constituait une violation du règlement (UE) 2018/1725 relatif à la protection des données. Il va par ailleurs être saisi à nouveau par le CRU pour une révision de la décision et finit par maintenir sa position en précisant néanmoins qu'il ne procéderait pas à des mesures correctrices.

Le Tribunal de l'Union Européenne, saisi par requête du CRU le 1^{er} septembre 2020, a partiellement annulé la décision du CEPD en jugeant qu'étant donné que la société Deloitte n'a pas les moyens de réidentifier les personnes, les données pseudonymisées reçues par celle-ci ne constituaient pas des données à caractère personnel.

C'est ainsi que le CEPD, appuyé par le Comité européen de la protection des données, forme un pourvoi devant la CJUE en soutenant que le tribunal avait mal interprété la notion de données à caractère personnel en considérant que les données pseudonymisées transmises ne constituaient pas des données personnelles et que le tribunal avait également commis une erreur de droit en subordonnant l'existence de l'obligation d'information du responsable du traitement à la capacité du destinataire à identifier les personnes.

- Extraits -

« 60. Il s'ensuit que le Tribunal a commis une erreur de droit en jugeant, aux points 73 et 74 de l'arrêt attaqué, que le CEPD, pour conclure que les informations ressortant des commentaires transmis à Deloitte « se rapportaient », au sens de l'article 3, point 1, du règlement 2018/1725, aux personnes ayant soumis ces commentaires, aurait dû examiner le contenu, la finalité ou les effets desdits commentaires, dès lors qu'il était constant que ceux-ci exprimaient l'opinion ou le point de vue personnel de leurs auteurs.

86. Il s'ensuit que, contrairement à ce que soutient le CEPD, des données pseudonymisées ne doivent pas être considérées comme constituant, en toute hypothèse et pour toute personne, des données à caractère personnel aux fins de l'application du règlement 2018/1725, dans la mesure où la pseudonymisation peut, selon les circonstances de l'espèce, effectivement empêcher des personnes autres que le responsable du traitement d'identifier la personne concernée de telle manière que, pour elles, celle-ci n'est pas ou n'est plus identifiable.

112. Il en résulte que (...) l'obligation d'information incombant au CRU s'appliquait en l'espèce en amont du transfert des commentaires en cause et indépendamment de leur caractère personnel ou non, du point de vue de Deloitte, après leur éventuelle pseudonymisation.

113. (...) la question de savoir si le responsable du traitement a, à ce moment, respecté son obligation d'information ne saurait dépendre des possibilités d'identification de la personne concernée, dont disposerait, le cas échéant, un éventuel destinataire après un transfert ultérieur des données en cause.

115. Partant, le Tribunal a commis une erreur de droit en jugeant (...) que, pour apprécier si le CRU avait respecté son obligation d'information au titre de l'article 15, paragraphe 1, sous d), du règlement 2018/1725, le CEPD aurait dû examiner si les commentaires transmis à Deloitte constituaient, du point de vue de ce dernier, des données à caractère personnel ».

Cass. soc., 26 mars 2025, n° 23-16.068, F-B
--

Dans cet arrêt, la Cour de cassation casse partiellement l'arrêt rendu par la cour d'appel de Paris en rappelant que le droit à la preuve peut justifier la production d'éléments portant atteinte aux droits et libertés fondamentaux d'autrui, notamment à la protection des données à caractère personnel, à condition que cette production soit indispensable à l'exercice de ce droit et que l'atteinte soit strictement proportionnée au but poursuivi. Elle précise que la communication de données personnelles de salariés tiers, sollicitée sur le fondement de l'article 145 du code de procédure civile, peut être ordonnée par le juge des référés lorsqu'elle est nécessaire à l'établissement d'une discrimination alléguée. La Cour reproche ainsi à la cour d'appel d'avoir rejeté la demande de communication d'informations sans procéder à une mise en balance concrète entre le droit à la preuve de la salariée et le droit au respect de la vie privée et à la protection des données personnelles des autres salariés, tels que garantis notamment par le règlement général sur la protection des données. Dès lors, la cour d'appel, qui n'a pas recherché si les mesures sollicitées étaient proportionnées et strictement nécessaires à l'exercice du droit à la preuve, a violé les textes susvisés.

Faits – Le litige opposait une salariée de la société Systra, exerçant les fonctions de spécialiste GED, gestionnaire de projet, position 2.2, coefficient 130 de la classification de la convention collective des bureaux d'études. S'estimant victime d'une discrimination syndicale, elle a saisi la formation de référé de la juridiction prud'homale, sur le fondement de l'article 145 du code de procédure civile, afin d'obtenir la communication par son employeur de diverses

informations relatives à la situation professionnelle de dix salariés comparables, dans le but d'établir une comparaison.

Par une ordonnance rendue en référé, la juridiction prud'homale a statué sur cette demande. La salariée a interjeté appel de cette décision devant la cour d'appel de Paris, laquelle, par un arrêt rendu le 16 février 2023, statuant en référé, a rejeté sa demande. La salariée a alors formé un pourvoi en cassation contre cet arrêt.

- Extraits -

« 1. [...] en statuant ainsi, sans rechercher si cette communication n'était pas nécessaire à l'exercice du droit à la preuve de la discrimination alléguée et proportionnée au but poursuivi, la cour d'appel a violé l'article 145 du code de procédure civile [...]

2. [...] sans vérifier si les éléments dont elle demandait communication sont de nature à porter atteinte à la vie personnelle d'autres salariés, quelles mesures étaient indispensables à l'exercice de son droit à la preuve et proportionnées au but poursuivi[...]

5. [...] Il appartient au juge saisi d'une demande de communication de pièces sur le fondement de l'article 145 du code de procédure civile, d'abord, de rechercher si cette communication n'est pas nécessaire à l'exercice du droit à la preuve de la discrimination alléguée et proportionnée au but poursuivi et s'il existe ainsi un motif légitime de conserver ou d'établir avant tout procès la preuve de faits dont pourrait dépendre la solution d'un litige [...] ».

CJUE, 4 oct. 2024, aff. C-446/21, <i>Schrems</i>

Par son arrêt du 4 octobre 2024, la Cour de Justice de l'Union européenne (CJUE) affirme que le principe de minimisation des données énoncé à l'article 5 paragraphe 1 point c) du RGPD s'oppose à ce qu'un opérateur de plateforme de réseau social en ligne, telle que Meta, puisse agréger, analyser et traiter, sans limitation dans le temps et sans distinction selon leur nature, toutes les données à caractère personnel obtenues auprès de la personne concernée ou de tiers, tant sur ladite plateforme qu'en dehors de celle-ci aux fins de publicité ciblée. Sur le second point, la Cour interprète l'article 9 paragraphe 2 point e) du RGPD en ce sens que le fait qu'une personne ait évoqué publiquement son orientation sexuelle lors d'un débat public ne saurait autoriser l'exploitation d'autres données relatives à cette orientation, collectées hors de cette plateforme pour proposer de la publicité personnalisée.

Faits – Sur les faits, M. Schrems, un utilisateur autrichien du réseau social Facebook géré par Meta Platforms Ireland Ltd, conteste devant les juridictions autrichiennes le traitement de ses données personnelles à des fins de publicité personnalisée, arguant des violations multiples du RGPD, notamment des articles 5, 6, 7 et 9. Facebook reposait sur un modèle gratuit financé par la publicité ciblée, fondé sur un profilage détaillé à partir de données collectées sur la plateforme et hors de celle-ci via des cookies, les social plugins, des pixels, et l'utilisation d'autres services du groupe (comme Instagram et WhatsApp). Meta renvoyait pour le traitement des données aux politiques de données et cookies intégrées par référence dans les conditions générales d'utilisation. Les données ainsi collectées permettaient de suivre le comportement en ligne de M. Schrems, y compris sur des sites de partis politiques et des pages destinées à un public homosexuel et des messages politiques, alors qu'il n'avait ni renseigné de données sensibles sur son profil Facebook, ni rendu publics son journal ou sa liste d'amis, ni autorisé explicitement l'utilisation, ni autorisé explicitement l'utilisation de certaines

rubriques de son profil à des fins publicitaires, et qu'il contestait avoir consenti au traitement de données obtenues auprès de tiers. Il soutenait que son consentement, donné sous la contrainte de perdre l'accès à son compte, n'était pas libre ni conforme aux articles 6 paragraphe 1 a) et 7 du RGPD, et que le traitement de données sensible au sens de l'article 9 était dépourvu de base légale. Pour sa part, Meta soutenait que l'ensemble du traitement y compris la publicité personnalisée était nécessaire à l'exécution du contrat d'utilisation au sens de l'article 6 paragraphe 1 b) RGPD et conforme au principe de minimisation. Après un premier renvoi préjudiciel par arrêt du 25 janvier 2018 et après décisions de rejets et des décisions de rejet du tribunal de Vienne du 30 juin 2020 et de la Cour d'Appel, M. Schrems saisit la Cour Suprême qui par décision du 23 juin 2021 saisit à son tour la CJUE de plusieurs questions préjudicielles sur l'interprétation des articles 5, 6, 7 et 9 RGPD afin de déterminer notamment si l'ampleur du traitement par Meta respecte le principe de minimisation et si la mention ponctuelle par M. Schrems de son orientation sexuelle lors d'une table ronde à Vienne devant la représentation de la Commission européenne en Autriche suffit à considérer que ses données relatives à l'orientation sexuelle ont été manifestement rendus publics au sens de l'article 9 paragraphe 2 e) RGPD.

- Extraits -

« 65. Compte tenu de ce qui précède, il y a lieu de répondre à la deuxième question que l'article 5, paragraphe 1, sous c), du RGPD, doit être interprété en ce sens que le principe de la « minimisation des données », prévu à cette disposition, s'oppose à ce que l'ensemble des données à caractère personnel qui ont été obtenues par un responsable du traitement, tel que l'exploitant d'une plateforme de réseau social en ligne, auprès de la personne concernée ou de tiers et qui ont été collectées tant sur cette plateforme qu'en dehors de celle-ci, soient agrégées, analysées et traitées à des fins de publicité ciblée, sans limitation dans le temps et sans distinction en fonction de la nature de ces données.

83. Eu égard à ce qui précède, il y a lieu de répondre à la quatrième question que l'article 9, paragraphe 2, sous e), du RGPD, doit être interprété en ce sens que la circonstance qu'une personne se soit exprimée sur son orientation sexuelle lors d'une table ronde, dont la participation est ouverte au public, n'autorise pas l'exploitant d'une plateforme de réseau social en ligne à traiter d'autres données relatives à l'orientation sexuelle de cette personne, obtenues, le cas échéant, en dehors de cette plateforme à partir d'applications et de sites Internet de tiers partenaires, en vue de l'agrégation et l'analyse de celles-ci, afin de lui proposer de la publicité personnalisée. »

CJUE, 9 janv. 2025, aff. C-394/23, Mousse
--

Dans son arrêt du 9 janvier 2025, la Cour de Justice juge que la collecte obligatoire de la civilité par une entreprise de transport, dans un seul but de personnaliser la communication commerciale en fonction de l'identité de genre, n'est ni objectivement indispensable ni essentielle à la bonne exécution du contrat, et ne peut donc pas être justifiée par la base légale de l'exécution du contrat de l'article 6 paragraphe 1 b) RGPD. Elle considère également que cette collecte ne peut reposer sur l'intérêt légitime du responsable prévu par l'article 6 paragraphe 1 f) RGPD lorsque cet intérêt n'a pas été clairement indiqué aux clients, lorsque le traitement dépasse ce qui est strictement nécessaire pour atteindre cet intérêt ou lorsque compte tenu du risque notamment de discrimination liée à l'identité de genre, les droits et libertés des personnes concernées prévalent.

Enfin, la Cour précise que pour apprécier la nécessité du traitement au titre de l'intérêt légitime, on ne peut pas invoquer l'existence du droit d'opposition de l'article 21 RGPD pour rattraper un traitement qui n'est pas en lui-même nécessaire ni conforme au principe de minimisation.

Faits – Le litige oppose l'association Mousse à la CNIL et à la société SNCF Connect à propos de l'obligation pour les clients qui achètent en ligne des billets, abonnements ou cartes de réduction sur le site ou les applications SNCF, d'indiquer leur civilité en cochant « Monsieur » ou « Madame ». Estimant que cette collecte systématique de données relatives à la civilité n'était pas conforme au RGPD (notamment par absence de base de licéité, violation du principe de minimisation, manquement aux obligations de transparence et d'information), Mousse a saisi la CNIL d'une réclamation. Par décision du 23 mars 2021, la CNIL a rejeté la réclamation en considérant que le traitement était licite sur le fondement de l'article 6 paragraphe 1 b) RGPD (nécessaire à l'exécution du contrat de transport) et conforme au principe de minimisation, la personnalisation par la civilité correspondant aux usages admis dans les communications commerciales, civiles et administratives. Mousse a alors formé un recours en annulation devant le Conseil d'État le 21 mai 2021, faisant valoir que l'obligation de choisir « *Monsieur* » ou « *Madame* » n'était ni nécessaire à l'exécution du contrat, ni justifiée par un intérêt légitime, portait atteinte au droit de voyager sans révéler sa civilité, portait atteinte au respect de la vie privée, à la liberté d'exprimer son genre et créait un risque de discrimination, notamment pour les personnes ne se reconnaissant dans aucune de ces deux civilités, et aussi pour les ressortissants d'États admettant un genre neutre. La CNIL a conclu au rejet du recours en soutenant que le traitement pouvait être fondé sur l'intérêt légitime de SNCF Connect et que les personnes concernées disposaient d'un droit d'opposition. Le Conseil d'État par décision du 21 juin 2023 a sursis à statuer et a saisi la CJUE par renvoi préjudiciel afin de poser deux questions portant d'une part sur la possibilité de tenir compte des usages en matière de communications civiles, commerciales et administratives pour apprécier la nécessité de la collecte de la civilité au regard de l'article 5 paragraphe 1 c), et de l'article 6 paragraphe 1 b) et f) RGPD, et d'autre part sur la prise en compte du droit d'opposition de l'article 21 pour compenser le caractère obligatoire de cette collecte.

- Extraits -

« 64. Eu égard à l'ensemble des considérations qui précèdent, il y a lieu de répondre à la première question que l'article 6, paragraphe 1, premier alinéa, sous b) et f), du RGPD, lu en combinaison avec l'article 5, paragraphe 1, sous c), de ce règlement, doit être interprété en ce sens que :

- le traitement de données à caractère personnel relatives à la civilité des clients d'une entreprise de transport, ayant pour finalité une personnalisation de la communication commerciale fondée sur leur identité de genre, ne paraît ni objectivement indispensable ni essentiel afin de permettre l'exécution correcte d'un contrat et, partant, ne peut pas être considéré comme étant nécessaire à l'exécution de ce contrat ;
- le traitement de données à caractère personnel relatives à la civilité des clients d'une entreprise de transport, ayant pour finalité une personnalisation de la communication commerciale fondée sur leur identité de genre, ne peut pas être considéré comme étant nécessaire aux fins des intérêts légitimes poursuivis par le responsable de ce traitement ou par un tiers, lorsque :
- l'intérêt légitime poursuivi n'a pas été indiqué à ces clients lors de la collecte de ces données ; ou

– ledit traitement n’est pas opéré dans les limites du strict nécessaire pour la réalisation de cet intérêt légitime ; ou

– au regard de l’ensemble des circonstances pertinentes, les libertés et droits fondamentaux desdits clients sont susceptibles de prévaloir sur ledit intérêt légitime, notamment en raison d’un risque de discrimination fondée sur l’identité de genre. »

70. Eu égard à l’ensemble des considérations qui précèdent, il y a lieu de répondre à la seconde question que l’article 6, paragraphe 1, premier alinéa, sous f), du RGPD doit être interprété en ce sens que, afin d’apprécier la nécessité d’un traitement de données à caractère personnel au titre de cette disposition, il n’y a pas lieu de prendre en considération l’existence éventuelle d’un droit d’opposition de la personne concernée, au titre de l’article 21 du RGPD. »

INTERNET ET PROTECTION ET DROIT DE LA PROPRIETE INTELLECTUELLE

Par Sandrine Roose-Grenier, Maître de conférences à l'Université de Montpellier

CJUE, 1re ch., 17 oct. 2024, aff. C-159/23

Dans cet arrêt, la Cour de justice de l'Union Européenne répond à une demande de décision préjudicielle introduite par le Bundesgerichtshof (Cour fédérale de justice, Allemagne) portant sur l'interprétation de l'article 1er, paragraphes 1 à 3, et de l'article 4, paragraphe 1, sous b), de la directive 2009/24/CE du 23 avril 2009 concernant la protection juridique des programmes d'ordinateur. La Cour dit pour droit que le contenu des données variables insérées par un programme d'ordinateur protégé dans la mémoire vive d'un ordinateur et utilisées par ce programme au cours de son exécution ne relève pas de la protection conférée à cette directive, dans la mesure où ce contenu ne permet pas la reproduction ou la réalisation ultérieure dudit programme.

Faits - Le litige opposait Sony Computer Entertainment Europe Ltd, licencié exclusif pour l'Europe de la console PlayStation Portable (PSP) et de jeux associés, dont *MotorStorm : Arctic Edge*, à la société Dattel Design and Development Ltd ainsi qu'à Dattel Direct Ltd, développeurs et distributeurs de logiciels tiers complémentaires aux produits Sony. Dattel commercialisait deux produits interagissant avec les jeux originaux Sony : le logiciel *Action Replay PSP*, chargé via une clé USB connectée à la console après redémarrage de celle-ci, qui modifiait le contenu de variables stockées en mémoire vive durant l'exécution du jeu afin d'offrir à l'utilisateur des options non prévues par Sony - telles que la suppression des restrictions d'utilisation du turbo ou le déblocage anticipé de conducteurs normalement conditionnés à l'obtention d'un certain score - et le dispositif *Tilt FX*, capteur de mouvement raccordé à la PSP accompagné d'un logiciel chargé par le même procédé, permettant la commande de la console par gestes et supprimant certaines restrictions en cours d'exécution du jeu, dont l'usage illimité du turbo.

Dans les deux cas, ni le code source ni le code objet du jeu Sony n'étaient altérés ; seules les variables dynamiques en mémoire vive étaient modifiées à la volée, en cours d'exécution. Sony assigna Dattel en cessation de commercialisation et en réparation du préjudice, soutenant que ces logiciels permettaient une transformation illicite de ses programmes protégés par le droit d'auteur. Le Landgericht Hamburg (Tribunal régional de Hambourg) fit partiellement droit aux demandes de Sony par jugement du 24 janvier 2012, avant que l'Oberlandesgericht Hamburg (Tribunal régional supérieur de Hambourg) ne réforme ce jugement en appel en rejetant intégralement le recours de Sony. Saisi d'un pourvoi en *Revision* (comparable à un pourvoi en cassation), le Bundesgerichtshof décida de surseoir à statuer et de renvoyer l'affaire à la CJUE par décision du 23 février 2023, parvenue à la Cour le 15 mars 2023.

- Extraits -

« 33. Il ressort ainsi des termes de l'article 1er de la directive 2009/24, en particulier de ses paragraphes 2 et 3, que sont protégées toutes les "formes d'expression" d'un programme

d'ordinateur, à l'exception des idées et principes à la base des éléments qui le composent, à la condition qu'un tel programme soit original, en ce sens qu'il est la création intellectuelle propre à son auteur.

34. [...] la Cour a déjà jugé [...] que les "formes d'expression" d'un programme d'ordinateur sont celles qui permettent de le reproduire dans différents langages informatiques, tels le code source et le code objet.

35. En revanche, la Cour a jugé que l'interface utilisateur graphique d'un programme d'ordinateur, laquelle ne permet pas de reproduire ce programme, mais constitue simplement un élément dudit programme au moyen duquel les utilisateurs exploitent les fonctionnalités dudit programme, ne constitue pas une forme d'expression d'un programme d'ordinateur au sens de cette disposition.

36. [...] ni la fonctionnalité d'un programme d'ordinateur ni le langage de programmation et le format de fichiers de données utilisés dans le cadre d'un programme d'ordinateur pour exploiter certaines de ses fonctions ne constituent une forme d'expression de ce programme [...].

En effet, admettre que la fonctionnalité d'un programme d'ordinateur puisse être protégée par le droit d'auteur reviendrait à offrir la possibilité de monopoliser les idées, au détriment du progrès technique et du développement industriel.

37. [...] le code source et le code objet relèvent de la notion de "forme d'expression" d'un programme d'ordinateur, au sens de cette disposition, en tant qu'ils permettent la reproduction ou la réalisation de ce programme à un stade ultérieur, tandis que d'autres éléments de celui-ci, tels que notamment ses fonctionnalités, ne sont pas protégés par cette directive. Ladite directive ne protège pas non plus les éléments au moyen desquels les utilisateurs exploitent de telles fonctionnalités, sans toutefois permettre une telle reproduction ou réalisation ultérieure dudit programme.

38. [...] la protection garantie par la directive 2009/24 se limite à la création intellectuelle telle qu'elle se reflète dans le texte du code source et du code objet et, partant, à l'expression littérale du programme d'ordinateur dans ces codes, qui constituent respectivement un ensemble d'instructions selon lesquelles l'ordinateur doit effectuer les tâches prévues par l'auteur du programme.

51. [...] le logiciel de Datel, en ce qu'il modifie uniquement le contenu des variables insérées par un programme d'ordinateur protégé dans la mémoire vive d'un ordinateur et utilisées par ce programme au cours de son exécution, ne permet pas, en tant que tel, de reproduire ce programme ni une partie de celui-ci [...]. Le contenu des variables constitue donc un élément dudit programme, au moyen duquel les utilisateurs exploitent les fonctionnalités d'un tel programme, qui n'est pas protégé en tant que "forme d'expression" d'un programme d'ordinateur au sens de l'article 1er, paragraphe 2, de la directive 2009/24.

52. [...] l'article 1er, paragraphes 1 à 3, de la directive 2009/24 doit être interprété en ce sens que ne relève pas de la protection conférée par cette directive le contenu des données variables insérées par un programme d'ordinateur protégé dans la mémoire vive d'un ordinateur et utilisées par ce programme au cours de son exécution, dans la mesure où ce contenu ne permet pas la reproduction ou la réalisation ultérieure d'un tel programme. »

Cass. com., 15 janv. 2025, n° 23-14.625, FS-B
--

Dans cet arrêt, la Cour de cassation rejette le pourvoi formé par la société Dstorage en rappelant tout d'abord que l'article 6, I, de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN), dans sa rédaction antérieure à celle issue de la loi du 4 août 2014, n'a ni pour objet ni pour effet de priver les signataires d'un contrat

monétique auquel est partie un hébergeur de la faculté de stipuler que celui-ci est tenu à une obligation de surveillance des informations qu'il stocke ou publie, et de sanctionner la méconnaissance de cette obligation par une résiliation du contrat. La Cour écarte ensuite le moyen tiré d'une violation de la LCEN, en considérant que la cour d'appel a pu valablement retenir que la Société générale avait justement résilié le contrat, dès lors qu'il résultait de ses constatations que la société Dstorage n'avait pas respecté son engagement contractuel de ne publier ou stocker aucun contenu illicite.

Faits - Le litige opposait la société Dstorage, exploitant un service de stockage de contenus en ligne accessible depuis le site "1fichier.com", à la Société générale, avec laquelle elle avait conclu le 4 janvier 2013 un contrat monétique lui permettant de proposer à ses utilisateurs un service de paiement à distance sécurisé par carte bancaire. Ce contrat stipulait en son article 3.1.4 que la société Dstorage s'engageait à s'abstenir de toute activité illicite, notamment de tout acte de contrefaçon d'oeuvres protégées par un droit de propriété intellectuelle, et en son article 1.4 que la Société générale pouvait suspendre ou résilier le service dès lors qu'elle était informée de l'illicéité du contenu du site. Le 15 juin 2015, à la suite de la mise en oeuvre d'un système de détection d'activités illicites, le groupe Mastercard informa la Société générale de la présence sur le site 1fichier.com de contenus violant les droits de propriété intellectuelle de la société indienne Zee Entertainment Entreprises, permettant le téléchargement illégal de séries et de films. La Société générale notifia cette situation à la société Dstorage le 19 juin 2015, puis la mit en demeure le 25 juin 2015 de supprimer les 740 fichiers identifiés dans un délai de vingt-quatre heures, sous peine de résiliation du contrat. De nouveaux fichiers illicites ayant été rendus accessibles sur la plateforme, la Société générale résilia le contrat le 6 juillet 2015 sur le fondement de l'article 1.4.

La société Dstorage assigna alors la Société générale en invoquant une résiliation abusive du contrat, afin d'obtenir le rétablissement du service de paiement sécurisé en ligne et sa condamnation à des dommages et intérêts. La cour d'appel de Paris, par arrêt du 3 mars 2023, rejeta ses demandes, décision contre laquelle la société Dstorage forma un pourvoi en cassation.

- Extraits -

« 7. L'article 6, I, de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, dans sa rédaction antérieure à celle issue de la loi n° 2014-873 du 4 août 2014, n'a ni pour objet ni pour effet de priver les signataires d'un contrat monétique auquel est partie un hébergeur de la faculté de stipuler que celui-ci est tenu à une obligation de surveillance des informations qu'il stocke ou publie, et de sanctionner la méconnaissance de cette obligation par une résiliation du contrat. »

« 9. En l'état de ses constatations et énonciations, dont il résulte que la société Dstorage n'avait pas respecté son engagement contractuel de ne publier ou stocker aucun contenu illicite, la cour d'appel a pu retenir que la Société générale avait justement résilié le contrat. »

« 11. Il n'y a, en conséquence, pas lieu de saisir la Cour de justice de l'Union européenne des questions préjudicielles suggérées par la société Dstorage sur l'interprétation de l'article 14 de la directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, qui n'est pas applicable au litige. »

Dans ce jugement, le tribunal judiciaire de Marseille retient l'existence d'actes de contrefaçon de droits d'auteur portant sur des créations vestimentaires, après avoir reconnu l'originalité des modèles « Hearts from X » et « Love from X » et la titularité des droits de la société AZ FACTORY. Il juge que la reprise des caractéristiques originales de ces créations par la société défenderesse caractérise une atteinte aux droits patrimoniaux de l'auteur, indépendamment de la nullité du procès-verbal de saisie-contrefaçon, laquelle ne fait pas obstacle à l'examen des autres éléments de preuve produits.

Le tribunal en déduit que la société mise en cause engage sa responsabilité civile délictuelle au titre de la contrefaçon et la condamne en conséquence à réparer le préjudice subi, à cesser toute exploitation des vêtements litigieux, ainsi qu'à procéder à la destruction des produits contrefaisants, assortie de mesures de publication judiciaire.

Faits - La société AZ FACTORY, créatrice et détentrice de créations vestimentaires originales commercialisées sous les marques « Hearts from X » et « Love from X », a constaté la vente de vêtements présentant les mêmes caractéristiques et commercialisés sous des étiquettes différentes. Estimant que ces articles reproduisent illicitement ses créations, elle a engagé une action en contrefaçon contre la société VALERIA MODA, supposé fournisseur des vêtements litigieux, et obtenu une autorisation judiciaire de saisie-contrefaçon au siège de cette dernière. La société VALERIA MODA a contesté notamment la validité du procès-verbal de saisie-contrefaçon. Le tribunal devait se prononcer à la fois sur la nullité formelle de ce procès-verbal et sur l'existence d'actes de contrefaçon justifiant réparation.

- Extraits -

« Il est donc établi que la société AZ FACTORY est bien investie des droits d'auteur sur les créations originales Hearts from X et Love from X, l'originalité de la combinaison des caractéristiques de ces créations résultant de choix arbitraires et esthétiques provenant de nombreux croquis et dessins réalisés par X Y, reproduits sur des encarts de tissus de vêtements, à la façon de bandes dessinées concernant les créations Love from X, l'originalité des créations Hearts from X résidant quant à elle dans la reproduction de cœurs multiples en différents coloris et tailles, dessinés par X Y. »

« Dès lors, la société VALERIA MODA a commercialisé des vêtements reprenant la combinaison originale des créations Hearts from X et Love from X qui constituent des copies serviles des vêtements commercialisés par la société AZ FACTORY. »

« Ces agissements constituent ainsi des actes de contrefaçon des droits d'auteur de la société AZ FACTORY qui ont nécessairement dévalorisé les créations Hearts from X et Love from X en affectant leur attractivité. »

« En conséquence, la société VALERIA MODA sera condamnée à payer à la société AZ FACTORY la somme totale de 11 900€ à titre de dommages et intérêts en réparation de ses préjudices nés du chef des actes de contrefaçon de ses droits d'auteur sur les œuvres Hearts from X et Love from X.

De plus, il y a lieu d'ordonner l'arrêt immédiat de toute fabrication, reproduction, exposition ou vente des vêtements litigieux qui reprendrait la combinaison de caractéristiques originales des créations Love from X et Hearts from X sous astreinte de 500€ par jour de retard à compter

du prononcé du jugement à venir ; d'ordonner la destruction, justifiée par Commissaire de justice, aux frais de la société VALERIA MODA des exemplaires de vêtements contrefaisants qui seraient en sa possession ou dans ses stocks, sous astreinte de 500€ par jour de retard, dans les quinze jours à compter de la date à laquelle le jugement deviendra définitif. »

CA Paris, pôle 1, ch. 2, 25 sept. 2025, n° 24/17261
--

Cet arrêt rendu le 25 septembre 2025 par la Cour d'appel de Paris s'inscrit dans le contentieux relatif aux droits voisins des éditeurs de presse à l'égard des services de communication en ligne, prévus par l'article 15 de la directive (UE) 2019/790 du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique. L'arrêt fait suite à l'ordonnance de référé du Tribunal judiciaire de Paris du 23 mai 2024, qui avait ordonné à la société X Internet Unlimited Company de communiquer aux éditeurs de presse requérants un ensemble de données relatives à l'utilisation de leurs publications sur la plateforme X. La décision d'appel confirme intégralement l'ordonnance de première instance, et condamne ainsi la société X aux dépens.

Faits - La directive (UE) 2019/790 du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique a créé, en son article 15, un droit voisin au profit des éditeurs de presse. Ce droit leur permet de percevoir une rémunération en contrepartie de l'utilisation de leurs publications par les services de communication en ligne. Ce texte a été transposé en droit français par la loi n° 2019-775 du 24 juillet 2019, dont les dispositions sont codifiées aux articles L. 218-1 à L. 218-5 du Code de la propriété intellectuelle.

L'article L. 218-4 du CPI prévoit notamment que la rémunération due au titre des droits voisins repose sur les recettes de l'exploitation, et impose aux services de communication en ligne de fournir aux éditeurs « tous les éléments d'information relatifs aux utilisations des publications de presse » nécessaires à une évaluation transparente de cette rémunération.

Les sociétés éditrices de presse ont sollicité auprès de la société X International Unlimited Company la communication des éléments d'information nécessaires au calcul de leur rémunération, sans parvenir à un accord amiable. Par actes du 11 juillet 2023, les éditeurs ont assigné X devant le juge des référés du Tribunal judiciaire de Paris, afin d'obtenir une mesure d'instruction portant sur de nombreuses catégories de données, dont les impressions, clics, revenus publicitaires, notamment. L'essentiel des demandes a été accueilli et il a été ordonné à X de communiquer sept catégories d'informations, sous astreinte de 3 000 euros par jour de retard pendant six mois. La société X Internet Unlimited Company a interjeté appel le 9 octobre 2024.

La Cour confirme intégralement l'ordonnance de référé du 23 mai 2024 et rejette l'ensemble des moyens soulevés par X Internet Unlimited Company. Elle écarte le cadre normatif invoqué par X en rappelant que la directive 2004/48/CE régit la lutte contre la contrefaçon et non le droit voisin des éditeurs de presse, lequel relève de la directive 2019/790 ; c'est donc à la lumière de ce second texte que s'apprécient les conditions de légalité des mesures sollicitées. Elle distingue par ailleurs la surveillance de contenus illicites, prohibée par le Règlement sur les Services Numériques, de la communication de données économiques d'exploitation imposée par l'article L. 218-4 du CPI, rendant inopérant l'argument de X qui tentait d'invoquer le statut d'hébergeur.

Les injonctions sont jugées suffisamment circonscrites : elles visent tout post reproduisant, même partiellement, un article de presse et renvoyant vers le site de l'éditeur, sans imposer à X aucune analyse éditoriale.

La Cour relève que le partage d'articles génère automatiquement un affichage standardisé transportant l'URL d'origine, permettant à la plateforme d'identifier les données via ses propres

interfaces de programmation, ce qui écarte l'impossibilité technique invoquée. Sur la conservation des données depuis 2019, la Cour oppose à X sa propre politique de confidentialité et affirme qu'étant légalement tenue de communiquer ces informations depuis cette date, il lui appartenait d'adapter ses outils sans attendre d'y être contrainte judiciairement. La Cour valide les sept injonctions en les alignant sur les engagements pris par Google devant l'Autorité de la concurrence, jugés nécessaires à une évaluation transparente des droits voisins, et refuse que X puisse invoquer un moindre outillage technique pour échapper à une obligation légale qui lui incombe au même titre. Elle écarte également la demande d'annulation des injonctions n° 4 et 5, précisant que la première vise les revenus publicitaires de l'ensemble des éditeurs certifiés CPPAP et non les seuls requérants, et que la seconde, calquée sur le modèle Google, est compatible avec la politique de confidentialité de X qui reconnaît collecter les termes de recherche de ses utilisateurs.

Enfin, la Cour maintient l'astreinte de 3 000 euros par jour, les injonctions demeurant inexécutées, et condamne X aux dépens d'appel.

- Extraits -

« Il ne s'agit pas ici de contraindre le fournisseur à rechercher des faits ou des circonstances révélant des activités illégales, mais seulement à collecter et extraire de sa plateforme des données d'audience et de revenus ayant pour objet de définir l'assiette du droit à rémunération des éditeurs et agences de presse, sans avoir à porter une quelconque appréciation sur les contenus téléversés par les utilisateurs de la plateforme ».

« En visant dans ses injonctions "les publications définies à l'article L. 218-1 du code de la propriété intellectuelle leur appartenant", l'ordonnance vise l'intégralité des articles de presse publiés sur les sites de presse en ligne des éditeurs requérants, de sorte que tout post publié par un utilisateur quelconque sur la plateforme X qui reproduirait, même partiellement, un élément quelconque d'une publication de presse appartenant à un éditeur requérant et renverrait vers le site internet dudit éditeur est nécessairement visé par l'ordonnance ».

« Sur la durée de conservation des données, la société X indique dans sa politique de confidentialité qu'elle conserve les informations de ses utilisateurs pendant toute la durée de vie de leur compte. Elle ne conteste pas disposer, comme l'indiquent les intimées, d'une API (interface de programmation d'application) lui permettant de conserver des archives depuis 2006. En outre, étant légalement tenue depuis le 24 juillet 2019, date d'entrée en vigueur de la loi sur le droit voisin, de communiquer aux éditeurs de presse tous les éléments nécessaires au calcul de l'assiette de leur rémunération, il lui appartenait de conserver ces informations depuis le 24 juillet 2019 ».

Cass. com., 26 mars 2025, n° 23-13.589, FS-B

Par un arrêt en date du 26 mars 2025, la chambre commerciale de la Cour de cassation se prononce sur deux questions distinctes soulevées par le litige opposant la société Meta à la société Cargo Media AG. D'une part, elle confirme que l'identification du public de référence pour caractériser l'atteinte à une marque renommée relève de l'appréciation souveraine des juges du fond, lesquels peuvent valablement retenir que le public d'un service de niche est compris dans le public plus large de la marque renommée. D'autre part, et surtout, elle précise les conditions du cumul de l'action en contrefaçon de marque et de l'action en concurrence déloyale : un même acte matériel peut fonder ces deux actions dès lors qu'il porte

atteinte à des droits de nature différente. Elle pose toutefois une limite essentielle tirée du principe de réparation intégrale : la victime ne saurait obtenir une double indemnisation pour un préjudice déjà réparé au titre de la contrefaçon.

Faits - La société Meta Platforms Inc., anciennement Facebook Inc., est titulaire de plusieurs marques verbales et figuratives de l'Union européenne portant le signe « Facebook », enregistrées à partir de 2005 pour désigner notamment des services de réseaux sociaux et de mise en relation. La société suisse Cargo Media AG exploite quant à elle un site de rencontres pour adultes à caractère sexuel dénommé “Fuckbook”, pour lequel elle a acquis en 2012 les noms de domaine “fuckbook.com” et “fuckbook.xxx”. Estimant que l'usage du signe “fuckbook” portait atteinte à ses droits, la société Meta a assigné la société Cargo Media en invoquant l'atteinte à ses marques renommées au titre de la contrefaçon ainsi que des actes de concurrence déloyale. La cour d'appel de Paris, dans un arrêt du 28 octobre 2022, a fait droit à ces demandes, retenant à la fois l'atteinte aux marques renommées de Meta, la contrefaçon, et des actes distincts de concurrence déloyale résultant de l'usage du nom commercial “Fuckbook” et des noms de domaine litigieux, créant un risque de confusion avec le nom commercial “Facebook” et le nom de domaine “facebook.com”.

La société Cargo Media a alors formé un pourvoi en cassation, contestant notamment que les faits retenus au soutien de la concurrence déloyale soient distincts de ceux fondant la condamnation pour contrefaçon de marque. La question posée à la Cour de cassation était donc de savoir si un même acte matériel peut simultanément fonder une action en contrefaçon de marque et une action en concurrence déloyale, et, dans l'affirmative, dans quelles limites la victime peut obtenir réparation à ces deux titres. La Cour de cassation a rejeté le pourvoi, confirmant que l'usage du signe “fuckbook” constituait à la fois une contrefaçon des marques “Facebook” et des actes distincts de concurrence déloyale, dans la mesure où ces derniers sanctionnaient une atteinte à des droits de nature différente tout en précisant que la victime ne peut obtenir d'indemnisation au titre de la concurrence déloyale que pour un préjudice distinct de celui déjà réparé au titre de la contrefaçon.

- Extraits -

« [L]e public du site “Fuckbook”, majoritairement composé d'adultes de sexe masculin recherchant des partenaires, était compris dans le public plus large des services du réseau social “Facebook”. »

« Un même acte matériel peut caractériser des faits distincts s'il porte atteinte à des droits de nature différente. »

« Il en résulte que la victime peut obtenir, au titre de la concurrence déloyale, la réparation du préjudice distinct né de l'atteinte à la distinctivité de ses signes d'identification, tels le nom commercial ou le nom de domaine, seulement si le préjudice n'est pas déjà réparé au titre de la contrefaçon. »

United States Court of Appeals for the District of Columbia Circuit, 18 mars 2025, n° 23-5233, <i>S. Thaler v. S. Perlmutter</i>

Par un arrêt en date du 18 mars 2025, la Cour d'appel du District de Columbia confirme que le droit d'auteur américain exige, en vertu du Copyright Act de 1976, que toute œuvre protégeable soit créée en premier lieu par un être humain. La Cour réaffirme ainsi que l'intelligence artificielle ne peut être reconnue comme auteur d'une œuvre aux fins de

l'enregistrement du copyright, quand bien même elle en serait l'unique créatrice. Cette décision s'inscrit dans un contexte d'essor rapide de l'IA générative et invite le législateur à se saisir de la question de l'adaptation du droit d'auteur aux nouvelles réalités technologiques.

Faits – Le Dr Stephen Thaler, informaticien, a développé un système d'intelligence artificielle générative qu'il a dénommé la “Creativity Machine”. Ce système a produit de manière autonome une œuvre visuelle intitulée “A Recent Entrance to Paradise”. En mai 2019, le Dr Thaler a déposé une demande d'enregistrement du copyright auprès du United States Copyright Office, en désignant la Creativity Machine comme seul auteur de l'œuvre et lui-même comme simple propriétaire. Le Copyright Office a rejeté cette demande au motif qu'aucun être humain n'avait créé l'œuvre, conformément à sa politique constante d'exigence d'une paternité humaine. Le Dr Thaler a sollicité successivement le réexamen de cette décision par le Registration Program, puis par le Review Board, en soutenant que cette exigence était inconstitutionnelle et contraire au texte de la loi. Ces deux instances ont maintenu le refus d'enregistrement. Le Dr Thaler a alors saisi le tribunal fédéral du District de Columbia, qui a confirmé la décision du Copyright Office en jugeant que l'exigence d'une paternité humaine constitue un fondement essentiel du droit d'auteur américain. Le Dr Thaler a interjeté appel, en faisant valoir notamment que le terme « auteur » ne se limiterait pas aux êtres humains au sens du Copyright Act, que la disposition relative aux œuvres créées dans le cadre d'un contrat de travail lui permettrait d'être considéré comme auteur en tant que propriétaire de la Creativity Machine, et qu'il devrait en tout état de cause être reconnu comme auteur pour avoir conçu et utilisé ce système. La Cour d'appel a confirmé le rejet de la demande d'enregistrement, en retenant que le Copyright Act de 1976, interprété à la lumière de son texte, de sa structure et de l'histoire législative, impose que toute œuvre protégeable soit créée en premier lieu par un être humain. Elle a en outre écarté l'argument tiré de la disposition sur les œuvres de commande, jugeant que celle-ci présuppose l'existence préalable d'une œuvre éligible au copyright, laquelle ne peut naître que d'une création humaine. Enfin, la Cour a refusé d'examiner l'argument selon lequel le Dr Thaler serait l'auteur pour avoir conçu et utilisé la Creativity Machine, ce moyen ayant été jugé abandonné faute d'avoir été soulevé en temps utile devant l'agence.

- Extraits -

« The Copyright Act does not define the word “author.” But traditional tools of statutory interpretation show that, within the meaning of the Copyright Act, “author” refers only to human beings. »

« All of these statutory provisions collectively identify an "author" as a human being. Machines do not have property, traditional human lifespans, family members, domiciles, nationalities, mentes reae, or signatures. By contrast, reading the Copyright Act to require human authorship comports with the statute's text, structure, and design because humans have all the attributes the Copyright Act treats authors as possessing. »

« The human authorship requirement does not prohibit copyrighting work that was made by or with the assistance of artificial intelligence. The rule requires only that the author of that work be a human being—the person who created, operated, or used artificial intelligence—and not the machine itself. »

« The Supreme Court has long held that copyright law is intended to benefit the public, not authors. Copyright law “makes reward to the owner a secondary consideration. * * * “[T]he primary object in conferring the monopoly lie[s] in the general benefits derived by the public from the labors of authors. »

« Importantly, that evolution in copyright protection has been at Congress's direction, not through courts giving new meaning to settled statutory terms. »

INTERNET ET PROTECTION ET DROIT DE LA CONSOMMATION

Par Malo Depincé, Professeur en Droit privé à l'Université de Montpellier

TJ Paris, 22 oct. 2024, n° 17/06842

Le jugement rendu le 22 octobre 2024 par le Tribunal judiciaire de Paris oppose l'association de consommateurs CLCV à la société anglaise Opodo Limited, exploitant d'un site de comparaison et de vente en ligne de voyages. La décision rappelle les exigences probatoires en matière de transparence qui pèsent sur les sites de comparaison en ligne et précise l'appréciation du caractère trompeur des informations relatives au classement et à la présentation des offres.

Faits - L'association agréée de défense des intérêts collectifs des consommateurs dénommée CLCV (Consommation, Logement et Cadre de Vie), a mis en demeure la société Opodo Limited de mettre en conformité son site avec la réglementation applicable aux comparateurs en ligne. Faute de réponse, elle a assigné la société devant le Tribunal judiciaire de Paris le 12 avril 2017. Dans son assignation initiale, la CLCV a fondé son action sur les articles L. 111-7 et D. 111-10 du Code de la consommation, reprochant à Opodo l'absence d'une rubrique spécifique accessible sur toutes les pages du site, l'absence de mention claire des critères de classement, un défaut de lisibilité des caractéristiques essentielles des offres comparées, ainsi qu'un manque de transparence sur le prix total à payer. En cours de procédure, et à la suite d'un arrêt de la Cour de cassation du 6 mars 2022 affirmant qu'une association de consommateurs n'est pas recevable à agir sur le fondement des articles L. 621-1 et L. 621-2 du Code de la consommation, "dès lors qu'elle n'invoque ni infraction pénale ni méconnaissance d'une disposition issue de la transposition du droit de l'Union", la CLCV a modifié ses fondements juridiques dans des conclusions du 23 mai 2023. Elle a requalifié les mêmes agissements en pratiques commerciales trompeuses au sens de l'article L. 121-1 du Code de la consommation. Elle a également étendu ses demandes à la suppression et à la déclaration de non-écriture de quatre clauses des conditions générales de vente (CGV), qu'elle estimait abusives au sens de l'article R. 212-1, 6° du Code de la consommation en ce qu'elles supprimaient ou réduisaient le droit à réparation des consommateurs.

Opodo contestait tant la recevabilité de ces demandes additionnelles, faute de lien suffisant avec les prétentions initiales, que leur bien-fondé, faisant valoir la conformité de son site à la réglementation applicable et la mise à jour de ses conditions générales en cours de procédure. Le tribunal déclare recevables les demandes additionnelles de la CLCV en relevant que la demande de suppression des CGV poursuit une finalité identique à la demande de cessation des pratiques illicites, le seul changement de fondement juridique étant insuffisant à caractériser un défaut de lien suffisant.

Sur le fond, le Tribunal précise que la qualification de pratique commerciale trompeuse est autonome et ne suppose pas de démontrer préalablement une contrariété à la diligence professionnelle. Il déboute ensuite la CLCV sur chacun des griefs soulevés : les critères de classement par défaut sont jugés suffisamment listés et accessibles sur le site, et la CLCV n'apporte aucun exemple d'offre qui aurait été omise des résultats de recherche.

Sur les clauses litigieuses présentes au sein des CGV, en ce qu'elles prévoyaient la possibilité d'une variation de prix entre la réservation sur le site et le moment du paiement effectif par le consommateur, et excluaient toute responsabilité d'Opodo pour les dommages résultant de

l'achat d'un produit ou service proposé sur son site, elles ont fait l'objet d'une modification en cours de procédure, sans que la CLCV ne formule d'observation sur ces changements. S'agissant du prix, le Tribunal constate enfin que le prix détaillé est communiqué avant la confirmation de l'achat et que la CLCV ne verse aucun élément établissant un écart significatif entre le prix initialement affiché et le prix final, excluant ainsi toute pratique trompeuse par omission.

- Extraits -

« La demande relative à la suppression des clauses des CGV a une finalité identique à celle tendant à la cessation des pratiques considérées comme illicites, la situation de fait dénoncée est la même et le seul changement de fondement juridique est insuffisant à justifier d'une irrecevabilité pour faute de lien suffisant de la demande additionnelle avec la demande initiale. »

« La clause 8.2 des Conditions de vente stipule désormais que "La limitation de la responsabilité de Opodo sera conforme à la législation en vigueur à tout moment", de sorte que plus aucune limitation spécifique de responsabilité n'est prévue aux termes des conditions de vente. Or, la CLCV ne formule aucune observation sur ce changement. »

« Le prix détaillé étant connu avant la confirmation de l'achat du produit ou service, ce qui n'est pas contesté par la CLCV, et cette dernière n'apportant au demeurant aux débats aucun élément établissant une différence significative entre le prix indiqué lors du premier affichage de l'offre et le prix final à l'issue du processus de réservation, il n'y a pas lieu de retenir l'existence d'une pratique commerciale trompeuse. »

CAA Paris, 9e ch., 7 févr. 2025, n° 23PA03283
--

Par cette décision, la Cour a rappelé la légalité d'une sanction administrative prononcée par une autorité administrative investie de prérogatives de puissance publique à l'encontre d'un professionnel ne respectant pas ses obligations légales ayant trait à l'information claire et loyale du consommateur. Cette décision confirme l'utilisation de la publication des sanctions comme outil d'information et de protection du consommateur, et renforce les pouvoirs de sanction de l'administration dans l'environnement numérique, notamment par le contrôle des pratiques commerciales numériques trompeuses et par le biais de la pratique du name and shame.

Faits - L'enseigne Darty est spécialisée dans la vente d'appareils électroménagers et propose à ses clients différentes garanties lors de la vente de ses produits. En 2017, elle est sujette à une opération de contrôle menée par la DGCCRF visant plusieurs de ses établissements ainsi que les sites internet sur lesquels elle les commercialise. Ces contrôles ont mis en lumière des manquements au droit à l'information des consommateurs relatifs aux garanties légales et commerciales dont ils peuvent bénéficier. En effet, les informations fournies par la société créaient une confusion sur l'existence et les modalités d'exercices des garanties légales et présentaient de plus les droits légaux conférés aux consommateurs pour leur protection comme une caractéristique propre à l'offre commerciale de l'enseigne. La Direction générale de la concurrence, de la consommation et de la répression des fraudes adresse à la société une injonction de faire cesser ces manquements et de rétablir une information lisible et non trompeuse pour les consommateurs. Toutefois, à la suite de nouveaux contrôles, il a été relevé

que peu d'améliorations avaient été mises en œuvre et que l'information du consommateur demeurait incomplète ou trompeuse, notamment autour de la formule ambiguë de la « garantie 2 ans », induisant le consommateur en erreur sur le caractère commercial de cette garantie. En conséquence, par une décision du 26 mars 2021, la directrice départementale de la protection des populations a prononcé une amende administrative de 25 000 euros à la société et ordonné la publication de cette décision sur la page d'accueil du site Internet de l'entreprise, à des fins d'information, conformément à l'article L. 522-6 du code de la consommation. La société conteste cette décision devant le tribunal administratif de Montreuil, qui rejette sa demande par un jugement du 23 mai 2023. Elle interjette alors appel devant la cour administrative d'appel de Paris, soutenant notamment que la décision de sanction était insuffisamment motivée, que les manquements n'étaient pas établis et arguait du caractère disproportionné de la sanction prononcée. Dans son arrêt du 7 février 2025, la cour administrative d'appel de Paris rejette la requête de la société en écartant les moyens soulevés. Elle a considéré que la décision était suffisamment détaillée et la sanction ainsi justifiée, considérant la persistance des pratiques commerciales trompeuses liées à une présentation confuse des garanties légales et commerciales. Par ailleurs, elle retient que l'amende de 25 000 euros n'était pas disproportionnée au regard de la gravité et de la persistance des manquements et en particulier que la mesure de publication poursuivait des fins d'information du consommateur.

- Extraits -

« Les plaquettes publicitaires disponibles en libre-service ou remises au client lors de la réalisation de l'achat, ne précisaient pas l'existence de garanties légales et l'information délivrée oralement par les vendeurs sur les garanties légales n'était ni spontanée, ni suffisante, voire même erronée. Sur le site internet de l'enseigne " darty.com ", si la présentation de la garantie commerciale a été réduite et les mentions portant à confusion entre les garanties légales et les garanties commerciales ont été reformulées et clarifiées, la garantie légale n'apparaît pas en page d'accueil contrairement à la garantie contractuelle " SAV A... " et la page dédiée au service après-vente ne fait pas mention de la garantie légale ».

« Il résulte de l'instruction que la décision attaquée du 26 mars 2021, qui mentionne les dispositions du code de la consommation dont il est fait application, rappelle l'ensemble des étapes de la procédure. Elle précise le périmètre du contrôle et ses modalités, les manquements relevés au cours de contrôles réalisés en 2017 ayant conduit à une mesure d'injonction de mise en conformité en matière d'information des consommateurs sur les garanties légales et commerciales adressée à la société A... le 4 octobre 2018 ».

« Il résulte de ce qui a été exposé aux points 10 et 12 du présent arrêt qu'en dépit des améliorations constatées, la sanction financière prononcée, limitée à 25 000 euros, n'apparaît pas disproportionnée compte tenu de la nature et de la persistance des manquements relevés à l'occasion des derniers contrôles réalisés un an après les injonctions de mise en conformité adressées à la société A. (...) ».

D. n° 2024-753, 7 juill. 2024 modifiant le Code de la consommation en ce qui concerne les obligations d'information des fournisseurs de comparateurs en ligne, de places de marché en ligne et d'agrégateurs de contenus d'actualité en ligne
--

Dans ce décret, le pouvoir réglementaire redéfinit les modalités d'information applicables aux fournisseurs de comparateurs en ligne et de places de marché en ligne, tout en les

articulant avec celles qui concernent désormais certains agrégateurs de contenus d'actualité en ligne. Le texte réécrit les articles D. 111-6 à D. 111-8 du Code de la consommation, précise la présentation des informations relatives au référencement, au déréférencement, au classement et à l'influence éventuelle d'intérêts économiques sur les résultats affichés, puis réorganise les dispositions réglementaires du même chapitre. Sa portée est essentiellement pratique : il encadre, au plus près de l'interface, les conditions dans lesquelles les offres et contenus sont présentés, hiérarchisés et, le cas échéant, signalés comme publicitaires. Son intérêt, en droit de la consommation comme en droit de l'internet, tient à ce qu'il déplace l'exigence de transparence vers les mécanismes mêmes de visibilité et d'orientation du choix en ligne.

Contexte - Le décret intervient dans le sillage de la loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, qui a modifié l'article L. 111-7 du Code de la consommation. Dans sa rédaction issue de cette loi, ce texte impose aux fournisseurs de places de marché en ligne et de comparateurs en ligne une information « *loyale, claire et transparente* » sur les conditions générales d'utilisation du service d'intermédiation, sur les modalités de classement et, pour les comparateurs, sur les modalités de référencement et de déréférencement. Il vise également l'existence d'une relation contractuelle, d'un lien capitalistique ou d'une rémunération influençant le classement ou le référencement. Le décret du 7 juillet 2024 a ainsi pour objet de donner à ces prescriptions législatives une portée opératoire. Il s'inscrit aussi dans l'extension de cette logique de transparence à certains services de diffusion groupée de contenus de presse : l'article 15, II, de la loi du 2 avril 1947 vise les personnes proposant un service de communication au public en ligne reposant sur le classement ou le référencement algorithmique de contenus extraits de publications de presse ou de services de presse en ligne d'information politique et générale, au-delà d'un seuil de connexions fixé par décret. À ces opérateurs, le législateur impose, outre l'information prévue à l'article L. 111-7, une information sur l'utilisation des données personnelles dans le classement ou le référencement des contenus, ainsi que la publication annuelle d'éléments statistiques relatifs à leur consultation. Le texte réglementaire répond donc à un besoin de mise en cohérence et d'application, dans un domaine où la compréhension des logiques de présentation des résultats participe directement de la protection du consommateur.

Le nouvel article D. 111-6 établit un socle commun. Il impose aux comparateurs en ligne, aux places de marché en ligne et aux personnes mentionnées à l'article 15, II, de la loi du 2 avril 1947 de faire figurer, dans une rubrique spécifique, les modalités de référencement, de déréférencement et de classement. Cette rubrique doit exposer les critères de classement par défaut et leurs principaux paramètres, ainsi que, le cas échéant, l'existence d'un lien capitalistique ou d'une rémunération influençant le référencement ou le classement. Le texte ajoute une obligation d'information à proximité de chaque résultat classé lorsque son rang a été influencé par une relation contractuelle, un lien capitalistique ou une rémunération, y compris pour ce qui relève de la publicité au sens de l'article 20 de la LCEN. L'article D. 111-7 précise ensuite les exigences propres aux comparateurs en ligne : information sur les critères de classement et leur définition, sur l'existence de liens contractuels ou capitalistiques avec les professionnels référencés, sur l'éventuelle rémunération et son incidence, sur les éléments constitutifs du prix, sur le caractère exhaustif ou non des offres comparées, sur le nombre de sites ou d'entreprises référencés et sur la périodicité d'actualisation. Il impose aussi, en tête de chaque page de résultats, l'indication du critère de classement utilisé par défaut, du caractère exhaustif ou non du périmètre comparé et du caractère payant ou non du référencement. À proximité de chaque offre comparée doivent encore apparaître les caractéristiques essentielles du bien ou du service, le prix total à payer et, lorsqu'elles existent, les garanties commerciales comprises dans le prix. Enfin, seules les offres référencées à titre

payant dont le rang dépend de cette rémunération doivent faire apparaître leur caractère publicitaire par la mention « *Annonces* ». L'article D. 111-8 organise, pour les places de marché en ligne, une transparence accessible sans identification préalable, portant notamment sur les principaux paramètres de classement, la qualité des personnes autorisées à déposer une offre, le descriptif du service de mise en relation, les modalités de paiement, les assurances et garanties proposées ainsi que les modalités de règlement des litiges. Lorsqu'une telle plateforme met en relation des consommateurs ou non-professionnels entre eux, elle doit également indiquer le statut déclaré de l'offreur, avertir celui-ci des sanctions encourues s'il agit en professionnel tout en se présentant comme non-professionnel, et préciser, pour chaque offre, le prix total, l'existence ou l'absence d'un droit de rétractation ainsi que l'absence de garantie légale de conformité et l'application de la garantie des vices cachés. Le décret ne modifie donc pas les régimes substantiels de la vente ou de la publicité ; il renforce l'effectivité des exigences de transparence par une normalisation plus fine de la présentation des résultats et des offres dans les interfaces numériques.

Sur le plan de la technique normative, le décret réorganise et renumérote les dispositions réglementaires du même chapitre, sans que cette opération formelle altère sa logique principale, qui demeure celle d'un encadrement plus serré des modalités de classement et de mise en relation.

- Extraits -

« ... les modalités de référencement, déréférencement et de classement. » (C. consom., art. D. 111-6, I).

« ... sans que l'utilisateur ait besoin de s'identifier ... » (C. consom., art. D. 111-8, I).

« ... leur caractère publicitaire par la mention du mot "Annonces" ... » (C. consom., art. D. 111-7, IV).

« ... sur l'utilisation de ses données personnelles dans le cadre du classement ou du référencement de ces contenus. » (L. n° 47-585 du 2 avr. 1947, art. 15, II).

D. n° 2025-9, 3 janv. 2025, désignant l'autorité administrative chargée de la concurrence et de la consommation compétente en matière de saisine de la juridiction civile en application de l'article L. 133-2 du Code de la consommation et compétente en application de l'article 7 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique

Par ce décret, le pouvoir réglementaire désigne l'autorité administrative compétente pour deux séries d'actes distinctes : d'une part, la saisine de la juridiction civile prévue à l'article L. 133-2 du Code de la consommation ; d'autre part, l'exercice des compétences mentionnées à l'article 7 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique. Le texte modifie l'article R. 524-1 du Code de la consommation en y intégrant l'article L. 133-2 et précise, séparément, que l'autorité administrative chargée de la concurrence et de la consommation mentionnée à l'article 7 de la LCEN est le directeur général de la concurrence, de la consommation et de la répression des fraudes.

Sa portée est essentiellement procédurale et institutionnelle : il ne crée aucune obligation matérielle nouvelle pour les opérateurs, mais rend pleinement opératoires des mécanismes de mise en oeuvre prévus par les textes supérieurs. Son intérêt tient ainsi moins à l'innovation normative qu'à la clarification organique et procédurale qu'il apporte dans l'architecture nationale de régulation des services numériques.

Contexte - Le décret trouve son origine dans les dispositions issues de la loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique. Celle-ci a inséré dans le Code de la consommation un chapitre consacré aux obligations des fournisseurs de plateformes en ligne. L'article L. 133-2 permet à l'autorité administrative chargée de la concurrence et de la consommation, après avis au procureur de la République, de demander à la juridiction civile d'enjoindre à l'auteur des pratiques de se mettre en conformité, l'injonction pouvant être assortie d'une astreinte journalière plafonnée à 5 % du chiffre d'affaires mondial hors taxes journalier moyen du fournisseur concerné. Parallèlement, l'article 7 de la LCEN, dans sa rédaction issue de la même loi, désigne trois autorités compétentes pour l'application de l'article 49 du règlement (UE) 2022/2065 : l'Autorité de régulation de la communication audiovisuelle et numérique, l'autorité administrative chargée de la concurrence et de la consommation, et la Commission nationale de l'informatique et des libertés ; l'ARCOM est en outre désignée coordinateur pour les services numériques. Le décret du 3 janvier 2025 répond ainsi à un besoin classique de mise en œuvre : il transforme une désignation fonctionnelle opérée par la loi en une désignation organique précise, et il étend à la nouvelle action prévue à l'article L. 133-2 le cadre réglementaire de compétence et de représentation devant les juridictions.

L'article 1^{er} du décret complète l'article R. 524-1 du Code de la consommation en y insérant la référence à l'article L. 133-2. Il en résulte que l'autorité administrative mentionnée à cet article est, selon le texte réglementaire, le directeur général de la concurrence, de la consommation et de la répression des fraudes, le chef du service national des enquêtes de cette direction, le directeur régional de l'économie, de l'emploi, du travail et des solidarités ou le directeur de la direction départementale chargée de la protection des populations. L'article R. 524-1 organise également les modalités de représentation devant les juridictions civiles et administratives de première instance et d'appel. Le décret assure donc l'effectivité procédurale du mécanisme institué par l'article L. 133-2, sans modifier ni la définition des manquements visés, ni le régime de l'injonction ou de l'astreinte. L'article 2 poursuit une fonction distincte : il désigne, pour l'application de l'article 7 de la LCEN, le seul directeur général de la concurrence, de la consommation et de la répression des fraudes comme autorité administrative chargée de la concurrence et de la consommation.

Ce point est simple dans sa rédaction, mais décisif dans son effet : il individualise, pour le versant « *consommation* » de la mise en œuvre nationale du règlement sur les services numériques, l'organe administratif compétent, tout en laissant intacte la pluralité des autorités compétentes prévue par l'article 7 de la LCEN et le rôle de coordination attribué à l'ARCOM. Le texte a ainsi une portée avant tout institutionnelle : il complète l'architecture nationale de police économique du numérique en déterminant l'autorité habilitée à agir et, pour la saisine civile prévue à l'article L. 133-2, en stabilisant le régime de compétence et de représentation devant le juge. Dans ce cadre, son apport est moins substantiel que structurel, mais cette fonction de clarification n'en est pas moins importante pour l'effectivité du droit applicable aux services numériques.

- Extraits -

« ... demander à la juridiction civile d'enjoindre à l'auteur des pratiques de se mettre en conformité. » (C. consom., art. L. 133-2).

« L'autorité administrative mentionnée à l'article L. 133-2 ... est le directeur général ..., le chef du service national des enquêtes ... » (C. consom., art. R. 524-1).

« Les autorités compétentes désignées en application de l'article 49 du règlement (UE) 2022/2065 ... sont : » (L. n° 2004-575 du 21 juin 2004, art. 7).

« L'autorité administrative chargée de la concurrence et de la consommation mentionnée à l'article 7 de la loi du 21 juin 2004 susvisée est le directeur général de la concurrence, de la consommation et de la répression des fraudes. » (D. n° 2025-9, 3 janv. 2025, art. 2).

Directive (UE) 2024/2853, 23 oct. 2024, relative à la responsabilité du fait des produits défectueux et abrogeant la directive 85/374/CEE du Conseil

La directive (UE) 2024/2853 relative à la responsabilité du fait des produits défectueux, adoptée le 23 octobre 2024 par le Parlement européen et le Conseil de l'Union européenne, modernise en profondeur le régime européen de responsabilité du fait des produits défectueux. Elle abroge la Directive 85/374/CEE relative à la responsabilité du fait des produits défectueux et doit être transposée par les États membres au plus tard en décembre 2026. Le texte procède à une révision substantielle du dispositif existant, en élargissant notamment l'étendue des préjudices réparables, en adaptant les règles relatives à la preuve du lien de causalité et en actualisant le champ d'application du régime afin de tenir compte de l'intégration croissante des logiciels et technologies numériques dans les produits.

Contexte - Cette réforme intervient dans un contexte de transformation numérique des biens de consommation, caractérisé par l'intégration croissante de composants logiciels, de services numériques et de systèmes interconnectés dans les produits commercialisés sur le marché européen. Face à ces évolutions technologiques, l'Union européenne a engagé une modernisation du cadre juridique applicable afin de garantir un niveau élevé de protection des consommateurs tout en assurant l'adaptation du droit aux nouveaux modèles technologiques. Le régime instauré par la directive 85/374/CEE relative à la responsabilité du fait des produits défectueux repose sur un principe de responsabilité sans faute du producteur : la victime peut obtenir réparation en démontrant l'existence d'un défaut du produit, la réalité du dommage et le lien de causalité entre les deux, sans avoir à établir une faute du fabricant. Dans ce système particulièrement protecteur, la détermination du champ d'application du régime revêt une importance déterminante, puisqu'elle conditionne l'accès à ce mécanisme de responsabilité. La réforme opérée par la directive (UE) 2024/2853 relative à la responsabilité du fait des produits défectueux s'inscrit également dans la continuité des travaux législatifs européens consacrés aux biens comportant des éléments numériques, en particulier la directive (UE) 2019/771 relative à certains aspects concernant les contrats de vente de biens, qui a introduit des exigences spécifiques de conformité pour les biens intégrant des services numériques, notamment en matière de mises à jour nécessaires au maintien du bon fonctionnement du produit. Dans cette logique d'adaptation du droit aux réalités technologiques contemporaines, la directive de 2024 étend explicitement le champ du régime de responsabilité sans faute aux logiciels ainsi qu'aux services numériques indispensables à l'utilisation d'un produit. Le législateur européen entend ainsi éviter qu'un dommage causé par un composant logiciel, un système d'intelligence artificielle ou un service numérique interconnecté échappe au régime de responsabilité applicable aux produits défectueux, alors même que ces éléments peuvent désormais être à l'origine d'un défaut affectant la sécurité du produit.

- Extraits -

« Considérant 13 : À l'ère numérique, les produits peuvent être corporels ou incorporels. Les logiciels, tels que les systèmes d'exploitation, les micrologiciels, les programmes informatiques, les applications ou les systèmes d'IA, sont de plus en plus répandus sur le marché et jouent un rôle de plus en plus important pour la sécurité des produits. Les logiciels

peuvent être mis sur le marché en tant que produits autonomes ou être intégrés par la suite dans d'autres produits en tant que composants, et ils sont susceptibles de causer des dommages lors de leur exécution. Dans l'intérêt de la sécurité juridique, il convient de préciser dans la présente directive que le logiciel est un produit aux fins de l'application de la responsabilité sans faute, quel que soit son mode de fourniture ou d'utilisation, et donc indépendamment du fait qu'il soit installé sur un appareil, accessible via un réseau de communication ou des technologies en nuage, ou fourni dans le cadre d'un modèle de logiciel en tant que service. Toutefois, les informations ne doivent pas être considérées comme un produit, et les règles en matière de responsabilité du fait des produits ne devraient donc pas s'appliquer au contenu des fichiers numériques, tels que les fichiers médias, les livres électroniques ou le simple code source des logiciels. Un développeur ou un producteur de logiciels, y compris les fournisseurs de systèmes d'IA au sens du règlement (UE) 2024/1689 du Parlement européen et du Conseil (5), devraient être considérés comme des fabricants.

Considérant 17 de la directive (UE) 2024/2853 : « Il est de plus en plus fréquent que des services numériques soient intégrés à un produit ou interconnectés avec celui-ci de telle sorte que l'absence du service empêcherait le produit d'exécuter une de ses fonctions. Bien que la présente directive n'ait pas vocation à s'appliquer aux services en tant que tels, il est nécessaire d'étendre la responsabilité sans faute auxdits services numériques intégrés ou interconnectés, étant donné que ceux-ci déterminent la sécurité du produit au même titre que les composants physiques ou numériques. Il convient que ces services connexes soient considérés comme des composants du produit auquel ils sont intégrés ou avec lequel ils sont interconnectés, lorsqu'ils sont sous le contrôle du fabricant de ce produit. Parmi les exemples de services connexes figurent la fourniture continue de données relatives au trafic au sein d'un système de navigation, un service de surveillance de la santé qui s'appuie sur des capteurs d'un produit physique pour suivre l'activité physique ou les mesures de santé de l'utilisateur, un service de contrôle de la température qui surveille et régule la température d'un réfrigérateur intelligent, ou un service d'assistant vocal qui permet de contrôler un ou plusieurs produits au moyen de commandes vocales. Les services d'accès à l'internet ne devraient pas être traités comme des services connexes, étant donné qu'ils ne peuvent pas être considérés comme faisant partie d'un produit sous le contrôle d'un fabricant et qu'il serait déraisonnable d'engager la responsabilité des fabricants pour les dommages causés par des lacunes dans les services d'accès à l'internet. Néanmoins, un produit qui repose sur des services d'accès à l'internet et qui ne garantit pas la sécurité en cas de perte de connectivité pourrait être considéré comme défectueux en vertu de la présente directive ».

L'article 4 de la directive étend la notion de produit à tout meuble, qu'il soit incorporé ou interconnecté à un autre meuble ou à un immeuble, et inclut explicitement l'électricité, les fichiers de fabrication numériques, les logiciels et les services numériques intégrés nécessaires au fonctionnement du produit. Cette définition couvre les logiciels autonomes comme ceux intégrés dans d'autres produits, y compris les systèmes d'intelligence artificielle, dès lors qu'ils sont mis sur le marché dans un cadre commercial. Les logiciels libres non commerciaux sont exclus, sauf lorsqu'ils sont intégrés dans un produit commercial, auquel cas ils entrent dans le champ de responsabilité du fabricant.

La notion de défectuosité, définie à l'article 7, est redéfinie pour tenir compte des spécificités numériques. Un produit est défectueux s'il n'offre pas la sécurité à laquelle une personne peut légitimement s'attendre.

Pour les produits numériques et systèmes d'IA, cette appréciation inclut la capacité du produit à apprendre ou acquérir de nouvelles caractéristiques après sa mise sur le marché ou sa mise en service, l'effet raisonnablement prévisible de son interconnexion avec d'autres produits, ainsi que le respect des exigences de cybersécurité.

L'article 6 précise le champ des dommages indemnifiables, limité aux personnes physiques. La directive étend la réparation aux atteintes psychologiques médicalement reconnues et à la destruction ou corruption de données personnelles. Les dommages purement économiques, les atteintes aux droits fondamentaux et les biens utilisés exclusivement à des fins professionnelles demeurent exclus, mais la directive reconnaît de nouvelles formes de préjudices propres à l'ère numérique.

L'article 8 de la directive organise la responsabilité des opérateurs économiques, couvrant le fabricant du produit défectueux, le fabricant du composant ou logiciel intégré ou interconnecté sous son contrôle, l'importateur, le mandataire, le distributeur et le prestataire de services numériques intervenant dans la chaîne.

L'article 12 précise la solidarité possible entre ces opérateurs. La directive assure ainsi qu'un acteur basé dans l'Union européenne puisse toujours répondre des dommages et encadre la responsabilité liée aux mises à jour, mises à niveau ou services numériques sous le contrôle du fabricant.

L'article 9 adapte le régime probatoire aux produits numériques et à l'IA. La charge de la preuve reste à la victime mais elle est allégée par des présomptions réfragables de défectuosité et de causalité. La victime peut demander la divulgation judiciaire d'éléments de preuve détenus par le défendeur, ce qui répond à l'asymétrie d'information caractéristique des systèmes complexes et facilite l'accès à la réparation.

L'article 11 prévoit des causes limitées, adaptées aux produits numériques ainsi qu'à l'IA. La défectuosité provenant d'un service ou logiciel sous le contrôle du fabricant n'exonère pas ce dernier, même après la mise sur le marché. Le risque de développement reste une cause possible d'exonération mais adaptée aux évolutions autonomes des produits numériques.

Ainsi, la directive (UE) 2024/2853 renforce la protection des victimes de produits défectueux et clarifie la responsabilité des opérateurs. Elle modernise le régime en incluant les logiciels, produits connectés et éléments numériques dont l'IA. Cette nouvelle directive permet donc d'assurer un cadre juridique harmonisé et opérationnel au sein de l'Union européenne.

Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024, concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règles (UE) n° 168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828

Le Cyber Resilience Act marque une évolution majeure du droit de l'internet en Europe en instaurant une responsabilité accrue des fabricants de technologies numériques et en consacrant un principe de cybersécurité intégrée dès la conception des produits. Il contribue ainsi à structurer un véritable droit européen de la sécurité des technologies numériques.

Contexte - Le règlement a été publié le 20 novembre 2024. L'application est progressive, avec une mise en œuvre complète prévue le 11 décembre 2027. Il vise à renforcer la cybersécurité des produits comportant des éléments numériques (logiciels, objets connectés, systèmes informatiques) mis sur le marché de l'Union européenne. Il établit un cadre juridique harmonisé imposant des exigences de cybersécurité tout au long du cycle de vie des produits, afin de garantir un niveau élevé de sécurité pour les consommateurs et les entreprises.

Le règlement s'applique aux « produits comportant des éléments numériques », c'est-à-dire : logiciels, matériels connectés, objets connectés (IoT), systèmes d'exploitation, applications, dispositifs numériques intégrés. Le règlement impose que la cybersécurité soit intégrée : lors de la conception, du développement, de la production, de la mise sur le marché, et pendant toute la durée d'utilisation du produit. Les fabricants doivent notamment réaliser une évaluation des risques de cybersécurité, mettre en place des processus de gestion des vulnérabilités, fournir des mises à jour de sécurité pendant la durée de support du produit.

Trois types d'opérateurs économiques ont des obligations. Les fabricants ont la responsabilité principale et doivent notamment constituer une documentation technique démontrant la conformité du produit. De plus, avant la mise sur le marché, les importateurs doivent vérifier que la procédure d'évaluation de conformité a été réalisée et que la documentation technique existe. Enfin, les distributeurs doivent vérifier la conformité du produit avant sa commercialisation et coopérer avec les autorités de surveillance du marché.

Le règlement distingue plusieurs catégories de produits selon le niveau de risque. Les produits standards sont soumis aux exigences générales de cybersécurité. De même, les produits importants qui présentent un risque élevé pour la cybersécurité sont soumis à des procédures de conformité plus strictes.

Enfin, il prévoit également des procédures d'évaluation de conformité, un marquage CE pour les produits conformes et une surveillance du marché par les autorités nationales qui peuvent exiger un retrait du produit, une correction des vulnérabilités ou une sanction. En cas de non-respect, les entreprises peuvent faire face à des amendes administratives importantes, des interdictions de mise sur le marché ou des obligations de retrait ou rappel de produits.

- Extraits -

« 1. Lorsqu'ils mettent sur le marché un produit comportant des éléments numériques, les fabricants s'assurent que ce produit a été conçu, développé et fabriqué conformément aux exigences essentielles de cybersécurité énoncées à l'annexe I, partie I.

2. Aux fins du respect du paragraphe 1, les fabricants procèdent à une évaluation des risques de cybersécurité associés à un produit comportant des éléments numériques et tiennent compte des résultats de cette évaluation au cours des phases de planification, de conception, de développement, de production, de livraison et de maintenance du produit comportant des éléments numériques, en vue de réduire au minimum les risques de cybersécurité, de prévenir les incidents et d'en réduire au minimum leurs répercussions, y compris en ce qui concerne la santé et la sécurité des utilisateurs. »

TA Lyon, 6^e ch., 19 mars 2024, n° 2204832

Dans cet arrêt, le tribunal administratif de Lyon rejette la requête de la société Babyroi et confirme la sanction administrative prononcée par la directrice départementale de la protection des populations du Rhône. Le tribunal rappelle d'abord que les agents de la DGCCRF peuvent adresser une injonction à un professionnel afin qu'il se conforme à ses obligations en matière de protection des consommateurs, puis prononcer une amende

administrative en cas de non-respect de cette injonction. Il considère ensuite que l'administration n'a pas commis d'erreur d'appréciation en constatant la persistance de plusieurs manquements aux obligations d'information du consommateur sur le site internet de la société, notamment concernant le droit de rétractation, les garanties légales et les coordonnées du médiateur de la consommation.

La juridiction juge enfin que la régularisation ultérieure des manquements ne fait pas obstacle à ce qu'ils soient sanctionnés dès lors qu'ils étaient encore constatés lors des contrôles effectués par l'administration. Elle estime également que l'amende administrative de 10 000 euros n'est pas disproportionnée au regard de la gravité des manquements et de la situation financière de la société.

Faits - Le litige oppose la société Babyroi, spécialisée dans la vente à distance d'articles de puériculture, à l'administration chargée de la protection des consommateurs. À la suite d'un contrôle effectué en 2020 par un inspecteur de la concurrence, de la consommation et de la répression des fraudes sur le site internet et au siège de la société, plusieurs manquements aux obligations prévues par le code de la consommation ont été constatés. L'administration a alors adressé à la société une injonction de mise en conformité le 6 janvier 2021, lui imposant notamment d'adhérer à un service de médiation de la consommation, de modifier les informations relatives au droit de rétractation et aux garanties légales, et de rendre ces informations accessibles sur son site internet. À la suite de nouveaux contrôles effectués en avril et juillet 2021, certains manquements ont été constatés comme persistants. La directrice départementale de la protection des populations du Rhône a alors infligé à la société, par une décision du 14 février 2022, une amende administrative d'un montant total de 10 000 euros. Après le rejet de son recours gracieux, la société Babyroi a saisi le tribunal administratif afin d'obtenir l'annulation ou la réduction de cette sanction.

- Extraits -

« Lorsque les agents habilités constatent un manquement ou une infraction avec les pouvoirs prévus au présent livre, ils peuvent, après une procédure contradictoire, enjoindre à un professionnel, en lui impartissant un délai raisonnable qu'ils fixent, de se conformer à ses obligations, de cesser tout agissement illicite ou de supprimer toute clause illicite ou interdite ».

« Le fait de ne pas déférer dans le délai imparti à une injonction relative aux infractions ou aux manquements constatés avec les pouvoirs mentionnés aux articles L. 511-5, L. 511-6 et L. 511-7, est passible d'une amende administrative ».

« La circonstance qu'elle se soit mise en conformité dans le délai imparti de 30 jours concernant les autres manquements relevés dans la mesure d'injonction du 6 janvier 2021 ne faisait pas obstacle à ce que l'administration constate et sanctionne la persistance des trois manquements précités à la date des deux contrôles des 12 avril et 26 juillet 2021, ainsi que par voie de conséquence le non-respect de la mesure d'injonction pour ce qui concerne ces manquements en application de l'article L. 532-1 du code de la consommation, sans qu'y fasse obstacle la circonstance postérieure à ces constats de la régularisation de ces manquements intervenue le 6 août 2021 ».

« Dans ces conditions, eu égard à la nature des manquements reprochés à la SASU Babyroi et au montant maximal des amendes encourues pour chacun d'eux, il ne résulte pas de l'instruction en l'espèce, alors même qu'elle a régularisé sa situation, dès le 7 août 2021, que

le montant de l'amende d'un montant total de 10 000 euros qui lui a été infligée présente un caractère disproportionné ».

CAA Paris, 9e ch., 7 févr. 2025, n° 23PA03283

Par cette décision, la Cour a rappelé la légalité d'une sanction administrative prononcée par une autorité administrative investie de prérogatives de puissance publique à l'encontre d'un professionnel ne respectant pas ses obligations légales ayant trait à l'information claire et loyale du consommateur. Cette décision confirme l'utilisation de la publication des sanctions comme outil d'information et de protection du consommateur, et renforce les pouvoirs de sanction de l'administration dans l'environnement numérique, notamment par le contrôle des pratiques commerciales numériques trompeuses et par le biais de la pratique du name and shame.

Faits - L'enseigne Darty est spécialisée dans la vente d'appareils électroménagers et propose à ses clients différentes garanties lors de la vente de ses produits. En 2017, elle est sujette à une opération de contrôle menée par la DGCCRF visant plusieurs de ses établissements ainsi que les sites internet sur lesquels elle les commercialise.

Ces contrôles ont mis en lumière des manquements au droit à l'information des consommateurs relatifs aux garanties légales et commerciales dont ils peuvent bénéficier. En effet, les informations fournies par la société créaient une confusion sur l'existence et les modalités d'exercices des garanties légales et présentaient de plus les droits légaux conférés aux consommateurs pour leur protection comme une caractéristique propre à l'offre commerciale de l'enseigne.

La Direction générale de la concurrence, de la consommation et de la répression des fraudes adresse à la société une injonction de faire cesser ces manquements et de rétablir une information lisible et non trompeuse pour les consommateurs. Toutefois, à la suite de nouveaux contrôles, il a été relevé que peu d'améliorations avaient été mises en œuvre et que l'information du consommateur demeurerait incomplète ou trompeuse, notamment autour de la formule ambiguë de la « garantie 2 ans », induisant le consommateur en erreur sur le caractère commercial de cette garantie. En conséquence, par une décision du 26 mars 2021, la directrice départementale de la protection des populations a prononcé une amende administrative de 25 000 euros à la société et ordonné la publication de cette décision sur la page d'accueil du site Internet de l'entreprise, à des fins d'information, conformément à l'article L. 522-6 du code de la consommation.

La société conteste cette décision devant le tribunal administratif de Montreuil, qui rejette sa demande par un jugement du 23 mai 2023. Elle interjette alors appel devant la cour administrative d'appel de Paris, soutenant notamment que la décision de sanction était insuffisamment motivée, que les manquements n'étaient pas établis et arguait du caractère disproportionné de la sanction prononcée.

Dans son arrêt du 7 février 2025, la cour administrative d'appel de Paris rejette la requête de la société en écartant les moyens soulevés. Elle a considéré que la décision était suffisamment détaillée et la sanction ainsi justifiée, considérant la persistance des pratiques commerciales trompeuses liées à une présentation confuse des garanties légales et commerciales. Par ailleurs, elle retient que l'amende de 25 000 euros n'était pas disproportionnée au regard de la gravité et de la persistance des manquements et en particulier que la mesure de publication poursuivait des fins d'information du consommateur.

- Extraits -

« Les plaquettes publicitaires disponibles en libre-service ou remises au client lors de la réalisation de l'achat, ne précisait pas l'existence de garanties légales et l'information délivrée oralement par les vendeurs sur les garanties légales n'était ni spontanée, ni suffisante, voire erronée. Sur le site internet de l'enseigne " darty.com ", si la présentation de la garantie commerciale a été réduite et les mentions portant à confusion entre les garanties légales et les garanties commerciales ont été reformulées et clarifiées, la garantie légale n'apparaît pas en page d'accueil contrairement à la garantie contractuelle " SAV A... " et la page dédiée au service après-vente ne fait pas mention de la garantie légale. »

« Il résulte de l'instruction que la décision attaquée du 26 mars 2021, qui mentionne les dispositions du code de la consommation dont il est fait application, rappelle l'ensemble des étapes de la procédure. Elle précise le périmètre du contrôle et ses modalités, les manquements relevés au cours de contrôles réalisés en 2017 ayant conduit à une mesure d'injonction de mise en conformité en matière d'information des consommateurs sur les garanties légales et commerciales adressée à la société A... le 4 octobre 2018 ».

« Il résulte de ce qui a été exposé aux points 10 et 12 du présent arrêt qu'en dépit des améliorations constatées, la sanction financière prononcée, limitée à 25 000 euros, n'apparaît pas disproportionnée compte tenu de la nature et de la persistance des manquements relevés à l'occasion des derniers contrôles réalisés un an après les injonctions de mise en conformité adressées à la société A. (...) ».

DGCCRF, « *Fast fashion : SHEIN sanctionné d'une amende de 40 millions d'euros* », communiqué de presse, 3 juillet 2025

Par un communiqué de presse du 3 juillet 2025, la DGCCRF a infligé une amende de 40 millions d'euros à la société ISEL pour pratiques commerciales trompeuses. L'autorité a considéré que la société avait trompé le consommateur sur la réalité des réductions dont ils pouvaient bénéficier et les avait également induits en erreur quant à la portée et la véracité de ses engagements environnementaux, faute de justification suffisante.

Faits - Le groupe SHEIN exerce une activité de vente en ligne de vêtements, chaussures et accessoires. La société ISEL, établie en Irlande, est responsable des ventes des produits de la marque SHEIN sur le territoire européen. A la suite de faits constatés entre le 1er octobre 2022 et le 31 août 2023 sur le site internet fr.shein.com, une enquête a été ouverte par la DGCCRF. L'enquête a mis en évidence des pratiques commerciales trompeuses à l'égard des consommateurs, à deux niveaux. D'une part, concernant les prix pratiqués : 57% des annonces contrôlées ne correspondaient à aucune réduction réelle ; 19% affichaient une réduction moins importante que celle annoncée et 11% des réductions étaient précédées d'une augmentation de prix, neutralisant ainsi l'avantage promotionnel annoncé. D'autre part, concernant les allégations environnementales : le site présentait l'entreprise comme engagée dans une démarche responsable affirmant notamment avoir réduit de 25% ses émissions de gaz à effet de serre. Toutefois, elle n'a pas été en mesure d'apporter des éléments justificatifs suffisants à l'appui de ces affirmations.

La DGCCRF devait se demander si la présentation de réduction de prix ne correspondant pas à une baisse réelle, ainsi que la mise en avant d'allégations environnementales non justifiées, constituent-elles des pratiques commerciales trompeuses au sens du code de la consommation. Cette procédure a abouti, avec l'accord de la procureure de la République de Paris, à la proposition d'une amende transactionnelle que l'entreprise a acceptée, mettant ainsi fin aux poursuites.

- Extraits -

« Une enquête de la Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes (DGCCRF) a révélé la mise en œuvre par la société Infinite Style E-commerce LTD (ISEL), responsable des ventes des produits de la marque SHEIN, de pratiques commerciales trompeuses à l'égard des consommateurs sur la réalité des réductions de prix accordées et sur la portée des engagements concernant les allégations environnementales. Une amende de 40 millions d'euros a été adressée à la société pour sanctionner ces agissements. »

DGCCRF, « Amende transactionnelle de 600 000 euros à l'encontre de la société SHOWROOMPRIVE.COM », communiqué de presse, 11 juillet 2025

Par un communiqué de presse du 11 juillet 2023, la DGCCRF a sanctionné la société SHOWROOMPRIVE.COM à une amende de 600 000 euros. L'autorité a considéré que les fausses promotions pratiquées étaient constitutives de pratiques commerciales trompeuses, en ce qu'elles ont pu altérer le jugement du consommateur lors de son achat.

Faits - La société SHOWROOMPRIVE.COM exploite un site de ventes privées en ligne. A la suite de faits constatés entre 2015 et 2020, une enquête de la DGCCRF a relevé que le site d'e-commerce pratiquait, par le biais de ses annonces commerciales, des réductions de prix fondées sur la mise en avant d'un prix de référence trompeur.

La DGCCRF devait se demander si les annonces de réduction du prix fondées sur la mise en avant d'un prix de référence trompeur constituaient une pratique commerciale trompeuse au sens des articles L.121-2 et L.121-3 du code de la consommation.

Cette investigation a conduit à la proposition d'une amende transactionnelle, validée par le parquet compétent, que la société a acceptée afin de clore la procédure contentieuse.

- Extraits -

« Ces fausses promotions sont constitutives du délit de pratiques commerciales trompeuses, tel que défini aux articles L.121-2 et L.121-3 du code de la consommation, dans la mesure où elles altèrent le jugement du consommateur dans son acte d'achat.

Avec l'accord du Parquet de Bobigny, une amende transactionnelle d'un montant de 600 000 euros a été proposée à la société SHOWROOMPRIVE.COM qui l'a acceptée. »

<i>DGCCRF, injonction faite à Booking le 10 juillet 2025 de mettre en conformité ses CGU avant fin décembre 2025</i>

À l'issue d'une enquête nationale sur les relations commerciales entre plateformes de réservation en ligne et hôteliers, la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) a fait usage de son pouvoir d'injonction à l'encontre de la plateforme Booking.com. L'autorité a relevé l'existence de clauses contractuelles susceptibles de porter atteinte à l'équilibre des relations commerciales entre la plateforme et les professionnels de l'hôtellerie. Par une injonction adressée le 10 juillet 2025, elle a exigé la mise en conformité des conditions générales d'utilisation avant la fin de l'année 2025. La plateforme s'est engagée à modifier les clauses litigieuses, les nouvelles dispositions étant entrées en vigueur le 29 janvier 2026, sous la vigilance continue de l'autorité administrative.

Faits - L'intervention de la Direction générale de la concurrence, de la consommation et de la répression des fraudes s'inscrit dans le cadre de sa mission de surveillance de l'équilibre des relations commerciales entre les plateformes d'intermédiation en ligne et les entreprises qui utilisent leurs services. Dans le secteur hôtelier, ces plateformes occupent une position structurelle centrale dans l'accès à la clientèle, ce qui confère à leurs conditions contractuelles une influence déterminante sur les modalités de commercialisation des hébergements.

Les professionnels de l'hôtellerie ont développé une stratégie de distribution multicanale : ils commercialisent leurs offres à la fois sur leurs propres sites internet et via des plateformes telles que Booking.com, qui leur assurent une visibilité importante auprès des consommateurs. Cette situation peut toutefois inciter les plateformes à instaurer des cadres contractuels particulièrement favorables à leurs intérêts économiques, notamment au moyen de clauses de parité tarifaire ou de restrictions affectant la commercialisation directe des chambres. La DGCCRF a estimé que certaines de ces stipulations pouvaient constituer des clauses restrictives de concurrence, en raison du déséquilibre qu'elles sont susceptibles d'introduire dans les relations contractuelles avec les hôteliers. De telles pratiques peuvent également avoir des effets directs sur les consommateurs : en empêchant les établissements de proposer sur leurs propres canaux de distribution des tarifs plus avantageux, elles limitent la possibilité pour les clients de bénéficier de prix plus compétitifs en réservant directement, réduisant ainsi l'intensité de la concurrence tarifaire et, in fine, le pouvoir d'achat. C'est dans ce contexte que l'injonction adressée le 10 juillet 2025 à Booking.com a imposé une mise en conformité de ses conditions générales d'utilisation avant la fin du mois de décembre 2025. La plateforme s'est engagée à modifier les clauses jugées problématiques afin de rééquilibrer ses relations commerciales avec les hôteliers, les nouvelles clauses étant entrées en vigueur le 29 janvier 2026. L'autorité a néanmoins indiqué qu'elle resterait attentive à la conformité de ces modifications et à leur application effective.

- Extraits -

« A la suite d'une enquête nationale, la DGCCRF avait enjoint plusieurs plateformes à corriger certaines clauses restrictives de concurrence. Afin de maximiser leur niveau d'activité et de rentabilité, les professionnels de l'hôtellerie diversifient leurs canaux de distribution en commercialisant leurs hébergements sur leurs propres sites internet, et en profitant aussi de la visibilité offerte par les plateformes. Dans ce dernier cas, la plateforme peut être tentée de créer un cadre contractuel avec les hôteliers qui lui est plus favorable, afin de capter la clientèle et les commissions associées à l'intermédiation ainsi réalisée. La DGCCRF veille à l'équilibre des relations commerciales entre professionnels, et en particulier entre les plateformes

d'intermédiation en ligne et les entreprises utilisatrices de leurs services. C'est pourquoi dans le cadre d'une enquête sur les relations commerciales entre les plateformes internet de réservation de nuitées et les hôteliers, la DGCCRF avait enjoint plusieurs plateformes à corriger certaines clauses restrictives de concurrence. Parmi ces plateformes, Booking.com s'est engagé à faire évoluer ses clauses pour rééquilibrer les relations commerciales avec les hôteliers. Les modifications des clauses élaborées par Booking.com sont entrées en vigueur le 29 janvier 2026. La DGCCRF restera vigilante sur la conformité des clauses et sur leur application effective. »

Ord. n° 2024-978, 6 nov. 2024, modifiant la loi n° 2023-451 du 9 juin 2023 visant à encadrer l'influence commerciale et à lutter contre les dérives des influenceurs sur les réseaux sociaux

L'ordonnance n° 2024-978 du 6 novembre 2024 modifie la loi n° 2023-451 du 9 juin 2023 afin d'en assurer la conformité avec le droit de l'Union européenne, notamment avec la directive 2005/29/CE relative aux pratiques commerciales déloyales. Elle assouplit les modalités d'identification du caractère commercial des contenus diffusés par les influenceurs, en admettant que l'intention promotionnelle puisse ressortir du contexte et non plus uniquement de mentions explicites telles que « publicité » ou « collaboration commerciale ». L'ordonnance introduit également une obligation nouvelle de transparence concernant l'utilisation d'images retouchées ou générées par intelligence artificielle, afin de prévenir les pratiques susceptibles d'induire le consommateur en erreur.

Contexte - L'activité des influenceurs sur les réseaux sociaux s'est fortement développée ces dernières années, avec une multiplication des formes de promotion commerciale (posts sponsorisés, stories, vidéos ou contenus générés par intelligence artificielle). Cette évolution s'est accompagnée d'un risque accru de pratiques trompeuses pour les consommateurs. Afin d'y répondre, le législateur français a adopté la loi n° 2023-451 du 9 juin 2023 visant à encadrer l'influence commerciale, premier texte spécifiquement consacré à la régulation de l'influence commerciale. Ce dispositif instaurait notamment des obligations de transparence destinées à garantir que les contenus promotionnels soient clairement identifiés comme tels. Toutefois, certaines dispositions de cette loi ont rapidement suscité des interrogations quant à leur compatibilité avec le droit de l'Union européenne. En particulier, la Commission européenne a relevé que la réglementation nationale devait être ajustée pour respecter le cadre posé par la directive 2005/29/CE relative aux pratiques commerciales déloyales, qui opère une harmonisation exhaustive des règles relatives à la qualification et à la sanction des pratiques commerciales déloyales dans le marché intérieur. C'est dans ce contexte que l'ordonnance du 6 novembre 2024 est intervenue afin d'adapter le dispositif français tout en maintenant un niveau élevé de protection des consommateurs face aux nouvelles formes de communication commerciale en ligne.

- Extraits -

« Art. 5-2.- Constitue une pratique commerciale trompeuse au sens de l'article L. 121-3 du code de la consommation et dans les conditions prévues à ce même article, l'absence d'indication par une mention claire, lisible et compréhensible, sur tout support utilisé, de l'intention commerciale poursuivie par une personne physique ou morale exerçant une activité d'influence au sens de l'article 1er de la présente loi, dès lors que cette intention ne ressort pas déjà du contexte. L'intention commerciale peut être explicitement indiquée par le recours aux mentions “ publicité ” ou “ collaboration commerciale ” ou par une mention équivalente

adaptée aux caractéristiques de l'activité d'influence et au format du support de communication utilisé. »

INTERNET ET DROIT DU TRAVAIL

Par Axel Saint-Martin, Avocat, cabinet ASM, Montpellier

Cass. soc., 26 nov. 2025, n° 23-22.415

La Chambre sociale de la Cour de cassation casse et annule l'arrêt rendu par la Cour d'appel mais seulement en ce qu'il déboute le salarié de sa demande tendant à dire que la prise d'acte produit les effets d'un licenciement sans cause réelle et sérieuse. La Cour justifie cette décision par le fait que la Cour d'appel s'est fondée sur le seul motif que les faits remontent à une date trop ancienne à savoir au mois d'août 2013 et pour la Cour d'appel, ce manquement était trop ancien pour constituer un motif de prise d'acte en 2020 et 2021. La Cour de cassation estime qu'en se fondant seulement sur l'ancienneté du manquement sans pour autant apprécier la gravité et la réalité de ce manquement reproché à l'employeur, la Cour d'appel n'a pas donné de base légale à sa décision.

Faits – Le litige oppose ici un salarié engagé en qualité de technicien micro et serveur à la société Mas Informatique ci-après nommée « l'employeur ». En l'espèce, le salarié a été en arrêt de travail pour maladie à compter du 5 novembre 2018. Le 14 janvier 2020, il a saisi la juridiction prud'homale en résiliation de son contrat de travail et a pris acte de la rupture de ce contrat le 15 mai 2021. Les juges de première instance ont jugé que l'emplacement d'une caméra de surveillance en salle de pause était intrusif. La Cour d'appel a infirmé le jugement de première instance. Le salarié fait grief à l'arrêt de le débouter de sa demande tendant à juger que la prise d'acte de la rupture du contrat de travail produit les effets d'un licenciement sans cause réelle et sérieuse. Il estime qu'un système de vidéosurveillance mis en place dans une salle de pause constituait à lui seul une atteinte disproportionnée aux droits des salariés et justifie de ce fait la rupture du contrat de travail aux torts de l'employeur.

- Extraits -

« Vu les articles L. 1231-1 du code du travail et 1184 du code civil dans sa rédaction antérieure à celle issue de l'ordonnance n°2021-6-131 du 10 février 2026

6. Il résulte de ces textes que lorsque le salarié prend acte de la rupture de son contrat de travail en raison de faits qu'il reproche à son employeur, cette rupture produit les effets, soit d'un licenciement sans cause réelle et sérieuse si les faits invoqués la justifiaient, soit, dans le cas contraire, d'une démission. La prise d'acte permet au salarié de rompre le contrat de travail en cas de manquement suffisamment grave de l'employeur empêchant la poursuite du contrat de travail.

7. Pour rejeter les demandes du salarié, l'arrêt relève que si celui-ci avait invoqué, au titre des manquements imputés à l'employeur, une atteinte à la santé constituée par le contrôle permanent des salariés via un système de vidéo-surveillance directement dirigé vers leurs bureaux, il avait été avisé de l'installation de ces caméras au mois d'août 2013.

8. L'arrêt en déduit que cet élément est trop ancien pour constituer un motif de prise d'acte en 2020 et 2021.

9. En se déterminant ainsi, en se référant uniquement à l'ancienneté du manquement, la cour d'appel, à laquelle il appartenait d'apprécier la réalité et la gravité de ce manquement et de dire

s'il était de nature à empêcher la poursuite du contrat de travail, n'a pas donné de base légale à sa décision. »

Cass. soc., 5 novembre 2025, n° 24-16.208

L'arrêt rendu par la chambre sociale de la Cour de cassation porte sur la question de l'admissibilité d'un moyen de preuve obtenu de manière déloyale dans le cadre d'un litige prud'homal. La Cour de cassation approuve la décision de la Cour d'appel ayant écarté des débats la retranscription d'un enregistrement réalisé à l'insu de l'employeur. Elle rappelle que si l'illicéité ou la déloyauté dans l'obtention d'un moyen de preuve ne conduit pas nécessairement à son exclusion, il appartient au juge d'apprécier, lorsqu'il en est saisi, si la production de cette preuve porte atteinte au caractère équitable du procès en mettant en balance le droit à la preuve et les droits opposés en présence. En l'espèce, la cour d'appel ayant retenu que l'enregistrement litigieux n'était pas indispensable à l'exercice du droit à la preuve, la Cour de cassation considère que la décision est légalement justifiée et le pourvoi est rejeté. La décision confirme la méthode désormais classique de mise en balance entre le droit à la preuve et les droits concurrents dans le procès civil. Elle rappelle que la production d'une preuve obtenue de manière déloyale ne peut être admise que de façon exceptionnelle, lorsque celle-ci apparaît indispensable à l'exercice du droit à la preuve. En l'espèce, les juges du fond ayant estimé que d'autres éléments permettaient déjà de laisser supposer l'existence d'une discrimination, l'exclusion de l'enregistrement litigieux ne portait pas atteinte au caractère équitable de la procédure. La solution s'inscrit ainsi dans la jurisprudence récente visant à concilier l'effectivité du droit à la preuve avec le respect du principe de loyauté dans l'administration de la preuve.

Faits – Dans cette affaire, M. [Z] avait été engagé par la société Hostellerie du royal lieu par un contrat à durée déterminée du 7 au 30 septembre 2020. Soutenant avoir été victime d'une discrimination liée à son handicap, au motif que son employeur était informé de son statut de travailleur handicapé avant la rupture de la relation de travail, le salarié a saisi la juridiction prud'homale le 20 avril 2021. Il sollicitait notamment la requalification de la relation de travail en contrat à durée indéterminée, la nullité de son licenciement ou subsidiairement, la reconnaissance d'un licenciement sans cause réelle et sérieuse, ainsi que l'allocation de diverses sommes à titre de dommages-intérêts. Au soutien de ses prétentions, il produisait notamment la retranscription, réalisée par huissier, d'un enregistrement de propos qu'il attribuait à son employeur et qui avait été effectué à l'insu de ce dernier. La cour d'appel d'Amiens, par un arrêt du 28 septembre 2023, a toutefois écarté cette pièce des débats, ordonné la suppression de son contenu et débouté le salarié de ses demandes. Celui-ci a alors formé un pourvoi en cassation.

- Extraits -

« Au regard de l'article 6 § 1 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales et de l'article 9 du code de procédure civile :

5. Dans un procès civil, l'illicéité ou la déloyauté dans l'obtention ou la production d'un moyen de preuve ne conduit pas nécessairement à l'écarter des débats. Le juge doit, lorsque cela lui est demandé, apprécier si une telle preuve porte une atteinte au caractère équitable de la procédure dans son ensemble, en mettant en balance le droit à la preuve et les droits antinomiques en présence,

6. le droit à la preuve pouvant justifier la production d'éléments portant atteinte à d'autres droits à condition que cette production soit indispensable à son exercice et que l'atteinte soit strictement proportionnée au but poursuivi.

7. En l'espèce, ayant constaté que le salarié produisait la retranscription d'un enregistrement, en date du 1er octobre 2020, de propos que le salarié prêtait à son employeur, effectué à l'insu de ce dernier, et retenu, après avoir analysé les autres éléments de preuve produits par le salarié, que ces éléments laissaient supposer l'existence d'une discrimination en raison du handicap,

8. la cour d'appel, qui a retenu que la production de l'enregistrement litigieux n'était pas indispensable au soutien des demandes du salarié fondées sur la discrimination, a légalement justifié sa décision

PAR CES MOTIFS, la Cour :

REJETTE le pourvoi ; ».

Cass. soc., 26 février 2025, n° 22-18.179.

Dans cet arrêt, la Cour de cassation rappelle que le droit à la preuve, garanti par les articles 6 et 8 de la Convention européenne des droits de l'homme peut justifier la production d'éléments portant atteinte à la vie privée du salarié, à condition que cette production soit indispensable à l'exercice du droit à la preuve et strictement proportionnée au but poursuivi. Elle admet ainsi la production en justice de courriels provenant de la messagerie personnelle du salarié lorsque ceux-ci sont nécessaires pour établir un manquement à l'obligation de loyauté. Toutefois, la Cour rappelle également que la responsabilité pécuniaire du salarié envers son employeur ne peut être engagée qu'en présence d'une faute lourde, caractérisée par l'intention de nuire, de sorte qu'une condamnation à des dommages-intérêts ne peut être prononcée si seule une faute grave est retenue.

Faits – L'arrêt de la chambre sociale du 26 février 2025 concerne un litige opposant M.[Z] à la société Automobiles générales martiniquaises (Autos GM). Engagé le 19 juillet 2010 en qualité de directeur de site, le salarié a présenté sa démission le 22 décembre 2017, avec une fin de contrat prévue au 22 mars 2018. Toutefois, le 12 janvier 2018, il a été mis à pied à titre conservatoire et convoqué à un entretien préalable, à l'issue duquel l'employeur a décidé de rompre son préavis pour faute lourde par lettre du 1^{er} février 2018.

Estimant que le salarié avait manqué à son obligation de loyauté en participant activement à un projet de création d'une société concurrente et en transmettant des informations confidentielles à des partenaires extérieurs, l'employeur a saisi la juridiction prud'homale afin d'obtenir sa condamnation au paiement de dommages-intérêts pour exécution déloyale du contrat de travail ainsi qu'une indemnité correspondant au préavis non exécuté. De son côté, le salarié a formé une demande reconventionnelle, sollicitant des dommages-intérêts pour rupture anticipée du préavis sans cause réelle et sérieuse ainsi qu'un rappel de rémunération variable.

La cour d'appel de Fort-de-France a considéré que les agissements du salarié caractérisaient une faute grave, justifiant la rupture du préavis. Elle a également condamné ce dernier à verser à l'employeur des dommages-intérêts pour exécution déloyale du contrat de travail. Le salarié a alors formé un pourvoi en cassation, soutenant notamment que les preuves produites par l'employeur provenaient de sa messagerie personnelle et portaient ainsi atteinte au secret des correspondances. L'employeur a formé un pourvoi incident, reprochant à la cour d'appel de ne pas avoir retenu la faute lourde.

La Cour de cassation rejette le moyen du salarié en considérant que la production des courriels issus de sa messagerie personnelle, bien qu'elle constitue une atteinte à sa vie privée, était indispensable à l'exercice du droit à la preuve et proportionnée au but poursuivi, à savoir la défense des intérêts légitimes de l'entreprise et la préservation de la confidentialité de ses affaires.

En revanche, elle relève d'office que la cour d'appel ne pouvait condamner le salarié à des dommages-intérêts au profit de l'employeur alors qu'elle n'avait retenu qu'une faute grave et non une faute lourde. Or, la responsabilité pécuniaire du salarié à l'égard de son employeur ne peut résulter que d'une faute lourde caractérisée par l'intention de nuire.

La Cour de cassation casse donc partiellement l'arrêt d'appel en ce qu'il condamne le salarié à payer des dommages-intérêts pour exécution déloyale du contrat de travail, tout en rejetant les autres moyens et en maintenant le reste de la décision.

- Extraits -

« Il résulte des articles 6 et 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, 9 du code civil et 9 du code de procédure civile, que le droit à la preuve peut justifier la production d'éléments portant atteinte à la vie privée à la condition que cette production soit indispensable à l'exercice de ce droit et que l'atteinte soit proportionnée au but poursuivi.

8. La production en justice par l'employeur de courriels, dont il n'était pas contesté qu'ils provenaient de la messagerie personnelle du salarié, constituait une atteinte à la vie privée du salarié.

9. Cependant, la cour d'appel a constaté que, pour établir le grief de déloyauté à raison de pourparlers en vue de la création d'une société concurrente et de la divulgation d'informations confidentielles de l'entreprise auprès de professionnels susceptibles de travailler pour des entreprises concurrentes, l'employeur s'était borné à produire les messages échangés par l'intéressé avec ses partenaires pour préparer et négocier le rachat d'une société de ventes de véhicules de même standing que ceux vendus par son employeur et leur faire parvenir des informations confidentielles.

10. En l'état de ces constatations, la cour d'appel a fait ressortir que cette production d'éléments portant atteinte à la vie privée du salarié était indispensable à l'exercice du droit à la preuve et proportionnée au but poursuivi, soit la défense de l'intérêt légitime de l'employeur à la préservation de ses intérêts et la confidentialité de ses affaires.

Vu le principe selon lequel la responsabilité pécuniaire d'un salarié à l'égard de son employeur ne peut résulter que de sa faute lourde :

17. Pour condamner le salarié à payer à la société une somme à titre de dommages-intérêts, l'arrêt retient qu'il est démontré que le salarié a, par son comportement, nui à la confiance nécessaire existant entre son employeur et son salarié, au surplus cadre dirigeant. Ce dernier se doit d'agir de manière exemplaire et en toute transparence dans le souci de la bonne marche de l'entreprise qui l'emploie.

18. En statuant ainsi, alors qu'elle décidait, par un chef de dispositif que le rejet du premier moyen du pourvoi incident rend définitif, que la rupture du préavis était fondée sur une faute grave, la cour d'appel, qui n'a pas retenu l'existence de faits, distincts de ceux visés par la lettre de rupture, du 1^{er} février 2018, susceptibles de caractériser une faute lourde, a violé le principe susvisé.

PAR CES MOTIFS, la Cour :

REJETTE les pourvois tant principaux qu'incidents ;

CASSE ET ANNULE, mais seulement en ce qu'il condamne M. [Z] à verser à la société Autos GM la somme de 200 000 euros à titre de dommages-intérêts en réparation de l'exécution

déloyale du contrat de travail, l'arrêt rendu le 20 mai 2022, entre les parties, par la cour d'appel de Fort-de-France ».

Cass. soc., 19 mars 2025, n° 23-19.154

La Chambre sociale de la Cour de cassation casse et annule partiellement l'arrêt rendu par la Cour d'appel et déclare recevable l'employeur en son appel. Elle fonde sa décision sur le principe fondamental du droit à la preuve et les articles L4121-1 et L4121-2 du Code du travail relatifs à l'obligation de sécurité de l'employeur envers ses salariés. La Cour faisant application des principes édictés par la CEDH en matière pénale déclare au visa de l'article 6 § 1 et 3 que « le juge ne peut fonder sa décision uniquement ou de manière déterminante sur des témoignages anonymes, il peut néanmoins prendre en considération des témoignages anonymisés, c'est-à-dire rendus anonymes à posteriori afin de protéger leurs auteurs mais dont l'identité est néanmoins connue par la partie qui les produit, lorsque sont versés aux débats d'autres éléments aux fins de corroborer ces témoignages et de permettre au juge d'en analyser la crédibilité et la pertinence. » La Cour en déduit donc que la Cour d'appel ne pouvait pas écarter ces témoignages au seul motif qu'ils étaient anonymisés. Selon la Cour de cassation, la production de ces témoignages anonymisés était indispensable à l'exercice du droit à la preuve de l'employeur tenu d'assurer la sécurité et de protéger la santé des travailleurs et que l'atteinte portée au principe d'égalité des armes était strictement proportionnée au but poursuivi.

Faits – Le litige oppose ici un salarié à la société Savoie rectification ci-après nommée « l'employeur ». En l'espèce, un salarié est licencié pour faute grave. L'employeur lui reproche de faire régner un climat de peur au sein de l'entreprise par un comportement agressif et violent tant verbalement que physiquement à l'égard de certains salariés. Ces derniers craignant des représailles acceptent de témoigner en faveur de l'employeur mais sous réserve que leur identité ne soit jamais révélée. L'employeur fait alors appel à un huissier de justice qui dresse des constats d'audition des salariés tout en prenant soin de ne mentionner ni leurs noms ni les éléments qui permettraient à l'auteur des faits de les reconnaître. La Cour d'appel juge le licenciement sans cause réelle et sérieuse aux motifs que l'employeur ne rapporte pas la preuve d'une faute grave. Elle considère en effet dépourvus de valeur probante les constats d'audition car il s'agit de témoignages anonymes et qu'aucun autre élément de preuve n'est apporté.

- Extraits -

« Vu les articles 6 de la CEDH et L.4121-1 et L.4121-2 du Code du travail

4. La Cour européenne des droits de l'homme juge que le principe du contradictoire et celui de l'égalité des armes, étroitement liés entre eux, sont des éléments fondamentaux de la notion de « procès équitable » au sens de l'article 6, § 1, de la Convention (...).

7. Pour dire le licenciement du salarié sans cause réelle et sérieuse et condamner l'employeur à lui payer diverses sommes, l'arrêt, après avoir constaté que la lettre de licenciement reprochait au salarié de faire régner un climat de peur au sein de l'entreprise et d'avoir repris ses horaires d'équipe de l'après-midi, sans l'accord de son employeur qui l'avait affecté en équipe de nuit avec horaires aménagés à sa demande, afin de « neutraliser, sans heurts, (ses) capacités de nuisance et limiter au maximum (ses) contacts avec les salariés s'étant ouverts de leurs peurs à (son) encontre » relève, d'abord, que la société, pour caractériser la faute du salarié, produit uniquement deux constats d'audition aux fins de preuve établis par huissier de

justice, les 11 février et 26 mars 2020, reprenant les contenus des auditions effectuées par cet huissier de cinq témoins dont l'identité n'est jamais mentionnée, à la demande de ces personnes, et que ces témoignages évoquent son attitude irrespectueuse voire agressive tant verbalement que physiquement envers ses collègues.

8. Il retient, ensuite, que ces deux constats d'audition aux fins de preuve établis par huissier consistent dans le recueil de témoignages anonymes ne comportant ni l'identité des témoins, ni la période durant laquelle ces personnes auraient travaillé avec le salarié, ni leur qualité au sein de l'entreprise. Il ajoute que la proposition de l'employeur de produire aux seuls membres de la cour d'appel les originaux, non anonymisés, des constats d'huissier doit être rejetée, de telles pièces ne pouvant être déclarées recevables, et que les constats anonymisés, en application de l'article 16 du code de procédure civile et de l'article 6, § 1 et 3, de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, doivent être déclarés "non probants", de sorte que l'existence d'une faute grave n'est pas démontrée.

9. En statuant ainsi, alors, d'une part, que relève de l'admissibilité des preuves et non de l'examen au fond le fait de déclarer non probante une pièce au motif de son défaut de contradiction et, d'autre part, qu'il résultait de ses constatations que la teneur des témoignages anonymisés, c'est-à-dire rendus anonymes a posteriori afin de protéger leurs auteurs, mais dont l'identité était connue de l'employeur et de l'huissier de justice qui avait recueilli ces témoignages, avait été portée à la connaissance du salarié, que ces témoignages avaient été recueillis par un huissier de justice responsable de la rédaction de ses actes pour les indications matérielles qu'il a pu lui-même vérifier en application des articles 1er et 2 de l'ordonnance n° 45-2592 du 2 novembre 1945 alors applicable, et qu'il n'était pas contesté que le salarié avait déjà été affecté à une équipe de nuit pour un comportement similaire à celui reproché dans la lettre de licenciement, de sorte que la production de ces témoignages anonymisés était indispensable à l'exercice du droit à la preuve de l'employeur tenu d'assurer la sécurité et de protéger la santé des travailleurs et que l'atteinte portée au principe d'égalité des armes était strictement proportionnée au but poursuivi, la cour d'appel, qui n'a pas tiré les conséquences légales de ses constatations, a violé les textes susvisés. »

Cass. soc., 22 janv. 2025, n° 22-15.793, F-D

La chambre sociale de la Cour de cassation a rendu une décision en date du 22 janvier 2025 confirmant que, dans un procès civil, l'illicéité dans l'obtention ou la production d'un moyen de preuve ne conduit pas nécessairement à son exclusion des débats. Cet arrêt souligne l'importance, pour les juges confrontés à une preuve illicite, de procéder à une mise en balance entre le droit au respect de la vie privée et le droit à la preuve, tout en tenant compte du caractère indispensable de la preuve litigieuse et du caractère proportionné de l'atteinte portée aux droits invoqués. Dans cette affaire, était en cause l'utilisation par un employeur de données issues d'un logiciel de gestion informatisée d'un centre d'appels, collectées afin de contrôler l'activité des salariées sans qu'elles en aient été préalablement informées.

Faits – Le litige oppose ici la société Gestionappels.com, exploitant un centre d'appels proposant aux professionnels de santé un service de télésecrétariat, à quatre de ses anciennes salariées. En l'espèce, Mmes Y., Z., H. et K. occupaient respectivement des postes de télésecrétaires au sein de cette société depuis 2011, 2013 et 2016. À la suite du constat que les salariées ne prenaient pas de nombreux appels alors qu'elles étaient disponibles, et réduisaient ainsi délibérément leur cadence de travail, l'employeur a décidé d'exploiter les données issues du logiciel de gestion informatisée du centre d'appels afin de contrôler l'activité de chacune d'elles. Il a également fait dresser un constat d'huissier à partir de ces mêmes données, permettant de déterminer le relevé des appels entrants et sortants, les temps de traitement et

d'attente ainsi que le nombre d'appels pris ou perdus, par collaboratrice identifiée par son prénom. Ces opérations avaient été réalisées sans que les salariées en eussent été informées préalablement. Par lettres du 9 février 2018, Mmes Y., Z., H. et K. ont été licenciées pour faute grave. Estimant avoir été victimes d'un licenciement sans cause réelle et sérieuse, elles ont saisi la juridiction prud'homale pour contester cette rupture. La cour d'appel de Dijon ayant confirmé le bien-fondé des licenciements, les salariées ont formé un pourvoi en cassation. Selon elles, les preuves issues du logiciel de gestion utilisées par l'employeur étaient totalement illicites en raison du défaut d'information préalable, et la cour d'appel avait failli à son obligation de caractériser l'indispensabilité de ces preuves et le but légitime justifiant une surveillance aussi stricte. En l'occurrence, la question qui se posait aux juges de la Cour de cassation était de savoir si la production de preuves obtenues de manière illicite, par l'exploitation de données personnelles issues d'un logiciel de gestion à l'insu des salariées pouvait être recevable pour justifier un licenciement pour faute grave. La Cour de cassation a rejeté le pourvoi et confirmé la décision de la cour d'appel en fondant sa décision sur une mise en balance entre le droit de l'employeur au bon fonctionnement de son entreprise et le droit des salariées au respect de leur vie privée, en tenant compte du caractère proportionné de l'atteinte portée au regard du but poursuivi. Elle a ainsi conclu que la production des données personnelles issues du logiciel de gestion était indispensable à l'exercice du droit à la preuve de l'employeur et proportionnée au but poursuivi, à savoir la défense de l'intérêt légitime de l'employeur au bon fonctionnement de l'entreprise.

- Extraits -

« 5. Il résulte des articles 6 et 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, 9 du code civil et 9 du code de procédure civile, que le droit à la preuve peut justifier la production d'éléments portant atteinte à la vie privée à la condition que cette production soit indispensable à l'exercice de ce droit et que l'atteinte soit proportionnée au but poursuivi.

6. L'obtention et la production en justice par l'employeur d'une preuve tirée de l'exploitation de données personnelles issues du logiciel de gestion du centre d'appels pour contrôler et surveiller l'activité des salariées, sans qu'elles en eussent été informées préalablement, constituait une atteinte à leur vie privée. »

« 8. En l'état de ces constatations, la cour d'appel a fait ressortir que cette production d'éléments portant atteinte à la vie privée des salariées était indispensable à l'exercice du droit à la preuve et proportionnée au but poursuivi, soit la défense de l'intérêt légitime de l'employeur au bon fonctionnement de l'entreprise. »

Cass. soc., 25 sept. 2024, n° 23-11.860, FS-B
--

La chambre sociale de la Cour de cassation rejette le pourvoi formé par l'employeur. Elle confirme la Cour d'appel dans ses propos en déclarant qu' « une conversation de nature privée d'un salarié n'a pas vocation à être rendue publique et ne constituant pas un manquement du salarié aux obligations découlant du contrat de travail, le licenciement prononcé pour motif disciplinaire était insusceptible d'être justifié et était atteint de nullité comme portant atteinte au droit au respect de l'intimité de la vie privée du salarié. » La Cour poursuit en affirmant au visa des articles 9 du Code civil et L1121-1 du Code du travail que « le salarié a droit même au temps et au lieu de travail au respect de l'intimité de sa privée. »

Faits – Le litige oppose un dirigeant à la Société SPB. En l'espèce, un cadre dirigeant est licencié pour faute grave en raison de l'envoi de mails à caractère sexuel depuis son ordinateur professionnel. Les propos étaient tenus dans le cadre d'une conversation privée avec trois personnes.

L'employeur pour justifier le licenciement argue qu'au regard de son obligation générale de prévention au harcèlement sexuel et agissement sexiste, sa décision de licencier le dirigeant était justifiée.

La Cour d'appel quant à elle déclare que ces courriels relevaient de la sphère privée, qu'ils ne visaient personne en particulier et que les agissements du dirigeant en l'espèce n'établissaient aucun fait pénalement répréhensible. Elle déclare le licenciement nul en se fondant partiellement sur l'exercice non abusif de la liberté d'expression.

- Extraits -

« 4. D'abord, il résulte des articles 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, 9 du code civil et L. 1121-1 du code du travail que le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée. Celle-ci implique en particulier le secret des correspondances.

L'employeur ne peut dès lors, sans violation de cette liberté fondamentale, utiliser le contenu des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail, pour le sanctionner.

5. Ensuite, il résulte des articles L. 1234-1, L. 1234-5 et L. 1234-9 du code du travail, qu'un motif tiré de la vie personnelle du salarié ne peut justifier, en principe, un licenciement disciplinaire, sauf s'il constitue un manquement de l'intéressé à une obligation découlant de son contrat de travail.

6. Le caractère illicite du motif du licenciement fondé, même en partie, sur le contenu de messages personnels émis par le salarié grâce à un outil informatique mis à sa disposition pour son travail, en violation du droit au respect de l'intimité de sa vie privée, liberté fondamentale, entraîne à lui seul la nullité du licenciement. »

Cass. soc., 25 sept. 2024, n° 23-13.992, FS-B
--

La solution retenue par la Cour dans cette décision illustre la mise en balance entre respect de la vie privée et droit à la preuve, et spécifiquement la preuve numérique dans la sphère professionnelle. Elle retient un principe crucial de protection des supports numériques personnels du salarié, protection particulièrement importante dans l'environnement numérique actuel où une grande partie des informations professionnelles circule sous forme de fichiers informatiques ou données stockés sur des supports électroniques.

Faits – Une salariée employée en tant qu'assistante commerciale par la société VS technologie est licenciée pour faute grave en 2017 après que son employeur découvre dans son bureau des clés USB sur lesquelles elle avait copié de nombreux fichiers comportant des informations confidentielles et notamment sur le processus de fabrication des produits commercialisés. L'expert mandaté par l'employeur a constaté, en présence d'un huissier, que ces fichiers avaient été copiés sans justification professionnelle par l'employée et qu'elle envisageait de les emporter.

Elle saisit alors le conseil des prud'hommes puis la cour d'appel de Lyon afin de contester son licenciement et obtenir notamment des indemnités pour licenciement sans cause réelle et sérieuse. Dans son arrêt du 25 janvier 2023, la cour d'appel de Lyon considère que les

éléments de preuve issus de l'exploitation des clés USB sont recevables et que les faits reprochés caractérisent une faute grave justifiant le licenciement. La salariée forme alors un pourvoi en cassation, soutenant le caractère illicite de la preuve constituée par les clés USB au motif que le caractère professionnel de celles-ci, autorisant l'employeur à consulter leur contenu, ne pouvait être présumé qu'à la condition où elles étaient connectées à un outil informatique mis à sa disposition dans le cadre de ses missions. Elle avance par ailleurs que le fait que ces clés aient été connectées au matériel informatique de l'entreprise par le passé ne constituait pas une condition suffisante pour légitimer leur consultation par l'employeur. Ainsi, ces conditions seraient suffisantes à caractériser une atteinte à la vie privée et à faire écarter les informations tirées des clés USB des éléments de preuve.

La chambre sociale de la Cour de cassation rejette le pourvoi en rappelant tout d'abord que l'accès par l'employeur, hors la présence du salarié, au contenu de clés USB personnelles non connectées à un ordinateur professionnel constitue en principe une atteinte à la vie privée du salarié. Pour autant, elle affirme que l'illicéité ou la déloyauté dans l'obtention d'une preuve ne conduit pas nécessairement à l'écarter des débats, et le juge doit apprécier si la production de cette preuve porte atteinte au caractère équitable du procès en mettant en balance le droit à la preuve de l'employeur et les droits fondamentaux, relatifs au respect de la vie privée, du salarié.

En l'espèce, les juges du fond avaient retenu que l'employeur disposait d'indices sérieux justifiant le contrôle, que l'exploitation des clés USB avait été réalisée de manière encadrée par un expert et un huissier, et que seuls les fichiers strictement professionnels avaient été utilisés. La production de ces éléments étant indispensable à l'exercice du droit à la preuve et proportionnée au but poursuivi, à savoir préserver la confidentialité de ses affaires, la Cour de cassation déclare les clés recevables les clés et confirme que les faits reprochés caractérisaient une faute grave rendant impossible le maintien de la salariée dans l'entreprise.

- Extraits -

« Il résulte de l'article L. 1121-1 du code du travail que l'accès par l'employeur, hors la présence du salarié, aux fichiers contenus dans des clés USB personnelles, qui ne sont pas connectées à l'ordinateur professionnel, constitue une atteinte à la vie privée du salarié. »

« Le juge doit, lorsque cela lui est demandé, apprécier si une telle preuve porte une atteinte au caractère équitable de la procédure dans son ensemble, en mettant en balance le droit à la preuve et les droits antinomiques en présence, le droit à la preuve pouvant justifier la production d'éléments portant atteinte à d'autres droits à condition que cette production soit indispensable à son exercice et que l'atteinte soit strictement proportionnée au but poursuivi. »