COLLOQUE
Journée d'actualisation du droit de l'internet

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

Vendredi 7 mars 2025

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.

SOMMAIRE

- Décret n° 2023-497 du 22 juin 2023 relatif aux modalités de communication au public du prix des offres de livres neufs et d'occasion : *Comm. com. électr.*, n°4, avr. 2024, chron. 5, obs. E. Emile-Zola-Place.
- Cass. Com., 6 mars 2024, n°22-23.657, n°22-22.651 et n°22-18.818, B+L : *RLDI*, n°214, mai 2026, 4916.
- CJUE, 5e ch., 21 mars 2024, aff. C-10/22, *Liberi editori e autori (LEA) c/ Jamendo SA* : *Comm. com. électr.*, n° 5, mai 2024, comm. 43, ob. P. Kamina
- Cass. 1re civ., 15 nov. 2023, n° 22-23.266 : *JurisData* n° 2023-020293 ; Comm. com. électr. 2024, comm. 3, P. Kamina ; C. Masson, *Prescription et action en contrefaçon et droit d'auteur : plaidoyer pour un dualisme tempéré*, *Comm. com. électr.*, n° 4, avr. 2024, étude 6.
- Cass. com., 6 mars 2024, n° 22-23.657, n° 22-22.651 et n° 22-18.818, FS-B : *RLDI*, n° 216, juill. 2024, note J. Groffe-Charrier.

Internet et droit de la consommation

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

- **Pratiques commerciales**

- L. n° 2023-451, 9 juin 2023, visant à encadrer l'influence commerciale et à lutter contre les dérives des influenceurs sur les réseaux sociaux : *JO* 10 juin 2023, texte n° 1.
- CJUE, 30 mai 2024, aff. C-662/22 et C-667/22, *Airbnb Ireland* : *JurisData* n° 2024-008148. – CJUE, 30 mai 2024, aff. C-663/22, *Expedia* : *JurisData* n° 2024-008149. – CJUE, 30 mai 2024, aff. C-664/22 et C-666/22, *Google Ireland* : *JurisData* n° 2024-008150 et *JurisData* n° 2024-008148.
- Comm. UE, communiqué, 8 nov. 2024 (*Temu*) pratiques commerciales.
- Comm. UE, communiqué, 12 nov. 2024 (*Apple*).
- CJUE, 26 sept. 2024, aff. C-330/23, *Aldi Süd* : *JurisData* n° 2024-022294.
- Cass. com., 4 sept. 2024, n° 22-12.321.
- Décret n° 2023-497 du 22 juin 2023 relatif aux modalités de communication au public du prix des offres de livres neufs et d'occasion : *Comm. com. électr.*, n° 4, avril 2024, chron. 5, obs. E. Emile-Zola-Place.
- Conseil d'État, juge des référés, 23 mai 2024, n° 494320, 494328, 494342, et 494356, *La Quadrature du Net* : *JurisData* n° 2024-008051.
- CEDH, 20 février 2024, n° 48340/20, *aff. Dede c. Türkiye.*

- **Pratiques restrictives et protection des consommateurs**

- Cass. com., 4 sept. 2024, n° 22-12.321, FS-B, *Sté Up to Motion c/ Google France et Google Ireland*: *JurisData* n° 2024-014907 ; *Comm. com. électr*. 2024, comm. 97, G. Loiseau ; *Contrats, conc. consom.* 2024, comm. 172, S. Bernheim-Desvaux ; *Contrats, conc. consom.* 2024, comm. 149, N. Mathey.

Internet et droit du travail

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

- Cass. soc., 27 septembre 2023, n° 20-22.465 FS-B : *Comm. com. électr*. 2023, comm. 79, Gr. Loiseau.
- Cass. soc., ass. plén., 22 décembre 2023, n° 20-20.648 B+R : *JurisData* n° 2023-023012.
- Cass. soc., 14 février 2024, n° 22-23.073 F-B : *JurisData* n° 2024-001483 ; *JCP* S 2024, 1123, S. Brissy.
- Cass. soc., 25 septembre 2024, n° 23-13.992 FS-B : *JurisData* n° 2024-016440 ; *JCP* E 2024, 1359, B. Bossu.
- CA Paris, pôle 6, ch. 6, 27 sept. 2023, n° 21/02239 : *JurisData* n° 2023-021844 ; *Comm. com. électr*. 2024, comm. 12, E.-A. Caprioli.
- Cass. soc., 14 février 2024, RG n° 21-19.802 F-D : *JurisData* n° 2024-001709 ; *Comm. com. électr*. 2024, alerte 131, Cabinet Racine.
- Cass. soc., 14 février 2024, n° 22-18.014 F-D : *JurisData* n° 2024-001741 ; *Comm. com. électr*. 2024, comm. 36, A. Lepage.

INTERNET ET RESPONSABILITÉ DES PRESTATAIRES TECHNIQUES

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

Cass. com., 27 mars 2024, n° 22-21.586, F-B, *Sté LBC France c/ Sté Olivo* : *JurisData* n° 2024-004004 ; *Comm. com. électr.* 2024, comm. 45, G. Loiseau

Par un arrêt en date du 27 mars 2024, la chambre commerciale de la Cour de cassation réaffirme le principe selon lequel les hébergeurs en ligne ne peuvent être soumis à une obligation générale de surveillance des contenus qu'ils hébergent. Dans cet arrêt, la Cour de cassation rappelle le fait que si les hébergeurs sont tenus de retirer promptement les contenus illicites dès lors qu'ils en ont connaissance, ils ne peuvent toutefois être contraints de surveiller de manière attentive et illimitée dans le temps, les informations qu'ils stockent. Cette décision met en avant l'importance qui existe de préserver un équilibre entre la protection de la liberté d'expression et de communication sur internet et la lutte contre les contenus illicites en ligne.

Faits – La société Olivo spécialisée dans la fabrication et la commercialisation de conteneurs à usage maritime, a constaté l'existence d'annonces frauduleuses usurpant son identité, diffusées sur le site leboncoin.fr. Les annonces litigieuses usurpaient son identité en faisant apparaître sa dénomination sociale, son RCS ainsi que son IBAN dans le but de proposer des faux devis et fausses commandes pour des containers maritimes. La société Olivo a alors demandé à la société LBC France, hébergeur du site leboncoin.fr de retirer ces annonces frauduleuses estimant que ces dernières portaient atteinte à son image et induisaient en erreur les consommateurs. Face à la persistance de la diffusion des annonces frauduleuses, la société Olivo a assigné en justice la société LBC France pour demander la cessation de la diffusion de ces annonces. La cour d'appel ayant confirmé le jugement du tribunal faisant droit à la demande de la société Olivo, la société LBC France, hébergeur du site leboncoin.fr, a alors formé un pourvoi en cassation estimant que l'injonction qui lui été faite de supprimer les annonces frauduleuses était de nature à la contraindre à procéder à une appréciation autonome de la licéité des contenus en cause. La question qui se posait alors à la Cour de cassation était de savoir si un hébergeur en ligne pouvait être contraint à une obligation générale et illimitée de surveillance des contenus qu'il héberge dans le but de prévenir la diffusion de contenus illicites. Les juges de la Cour de cassation ont cassé et annulé l'arrêt rendu par la cour d'appel de Lyon. Les juges ont notamment eu l'occasion de rappeler qu'au regard de l'article 6 de la loi pour la confiance dans l'économie du numérique du 21 juin 2004, il est possible de prescrire à tout hébergeur toutes mesures propres à prévenir ou faire cesser un dommage. Néanmoins cet hébergeur ne peut être soumis à une obligation générale de surveillance des informations qu'il transmet et stocke, qui l'obligerait à procéder à une appréciation autonome.

- Extraits –

« Vu l'article 6 de la loi n° 2004-575 du 21 juin 2004 en ses dispositions I.2, I.5 et I.7, dans sa rédaction issue de la loi n° 2020-766 du 24 juin 2020 :

8. Il résulte de ces textes que si l'autorité judiciaire peut prescrire, en référé ou sur requête, à

tout hébergeur ou tout fournisseur d'accès à des services de communication au public en ligne, toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un tel service, elle ne peut soumettre cet hébergeur ou ce fournisseur d'accès à une obligation générale de surveillance des informations qu'il transmet et stocke ou de recherche des faits ou des circonstances révélant des activités illicites, qui l'obligerait à procéder à une appréciation autonome.

9. Pour interdire à la société LBC la diffusion d'annonces utilisant la dénomination sociale et/ou le numéro RCS et/ou l'IBAN de la société Olivo aux fins d'établir de faux devis, de fausses commandes portant sur la commercialisation de containers à usage maritime, l'arrêt retient, par motifs propres, que les éléments produits suffisent à retenir l'existence d'un dommage en terme d'image et de communication subi par la société Olivo et occasionné par le service en ligne géré par la société LBC, et, par motifs adoptés, que des annonces frauduleuses ont continué d'être diffusées sur le site leboncoin.fr en juillet 2021, la publication de ces annonces constituant un trouble manifestement illicite qu'il convient de faire cesser.

10. En mettant ainsi à la charge de la société LBC un dispositif non seulement non limité dans le temps mais aussi qui, portant sur d'éventuelles annonces à venir, aboutit à la soumettre à une obligation générale de surveillance des informations stockées, l'obligeant à une appréciation autonome du contenu de ces annonces, la cour d'appel a violé le texte susvisé.

PAR CES MOTIFS, la Cour :
CASSE ET ANNULE, en toutes ses dispositions, l'arrêt rendu le 6 juillet 2022, entre les parties, par la cour d'appel de Lyon ; ».

Cass. com., 4 sept. 2024, n° 22-12.321, FS-B, *Sté Up to Motion c/ Google France et Google Ireland* : *JurisData* n° 2024-014907 ; *Comm. com. électr.* 2024, comm. 97, G. Loiseau ; *Contrats, conc. consom.* 2024, comm. 172, S. Bernheim-Desvaux ; *Contrats, conc. consom.* 2024, comm. 149, N. Mathey

La chambre commerciale de la Cour de cassation, par une décision rendue le 4 septembre 2024, confirme le raisonnement des juges du fond en rappelant que pèse sur les hébergeurs l'obligation légale d'agir promptement pour retirer des données dont ils connaissent le caractère illicite ou pour en rendre l'accès impossible (art. 6, §2, loi n° 2004-575, 21 juin 2004 pour la confiance dans l'économie numérique). Ainsi, en prévoyant une clause contractuelle lui permettant de suspendre promptement l'usage de ses services de référencement pour des raisons légales, puis en l'appliquant lorsqu'il est informé du caractère trompeur d'un site auquel il donne accès, Google ne crée pas un déséquilibre significatif au sens de l'article L. 442-6, I, 2° (devenu l'article L. 442-1, 2° du code de commerce). À l'occasion de cette décision, la Cour de cassation rappelle également que seules certaines entreprises sont autorisées à collecter les données de leurs clients nécessaires à l'établissement de certificats d'immatriculation. Il s'agit des entreprises qui jouissent de l'habilitation prévue à l'article R. 322-1, I, du code de la route. En l'espèce, la société ne disposait pas de l'habilitation obligatoire et n'a pas cherché à l'obtenir même après la suspension de son compte. Son activité était donc illicite, il est jugé que Google n'a pas commis d'abus en suspendant son compte.

Faits - En 2013, une société titulaire des droits sur une plateforme a conclu avec la société Google Ireland un contrat de référencement de son site web, au moyen du service « Google Adwords ». La plateforme en question permettait l'obtention de certificats d'immatriculation

de véhicules automobiles auprès des services de l'État français. Après avoir reçu un courrier du secrétariat d'Etat chargé du numérique en 2017, Google suspend le compte de la société. Cette suspension intervient sur le fondement de l'une des clauses du contrat qui stipule que Google possède un droit de résiliation du contrat et de suspension de la participation du client au programme « Adwords » à tout moment, si cela est justifié. À la suite de la suspension de son compte, la société assigne Google France et Google Ireland. La demanderesse requiert l'annulation de la clause ayant servi de fondement à la suspension de son compte.
La Cour d'appel de Paris, par un arrêt du 17 septembre 2021, déboute la société de sa demande. La Cour relève également que la société proposait sur sa plateforme l'obtention de certificats d'immatriculation de véhicules automobiles auprès des services de l'État français alors même qu'elle ne disposait pas de l'habilitation permettant de délivrer de tels certificats. La société se pourvoit en cassation. Elle argue, notamment, le déséquilibre significatif qu'il résulterait de la clause ayant servi de fondement à Google pour la suspension du compte. Elle allègue également que, bien qu'elle ne possède pas la certification requise pour collecter les données de ses clients, cela serait justifié par le fait que son activité ne requiert pas une telle habilitation. La Cour de cassation, par cet arrêt rendu le 4 septembre 2024, confirme le raisonnement des juges du fond en rappelant que pèse sur les hébergeurs l'obligation légale d'agir promptement pour retirer des données dont ils connaissent le caractère illicite ou pour en rendre l'accès impossible. « 6. La société Up to Motion fait grief à l'arrêt de rejeter sa demande d'annulation de l'article 13 des conditions générales du contrat, alors « que, pour rejeter la demande de nullité de l'article 13 des conditions générales du contrat conclu entre la société Fathi et la société Google, la cour d'appel a retenu que la faculté que s'était ainsi réservée cette dernière "d'interrompre immédiatement (…) le référencement" était "justifiée" par "l'accès universel, instantané et continu des services numériques sur internet et la téléphonie mobile (…) si leur contenu est susceptible de porter atteinte à l'ordre public en particulier en cas de publicité trompeuse" ; qu'il résultait cependant de ces constatations que la société Google, dont la cour d'appel a fait un gardien de l'ordre public, avait, par la clause litigieuse et au gré des faits dont elle était exclusivement le juge, fût-ce sur un simple soupçon, la faculté de décider unilatéralement et sans préavis la fin du contrat ; qu'en jugeant pourtant, pour exclure la demande d'annulation de cette clause, qu'elle n'avait créé aucun déséquilibre significatif entre les parties, la cour d'appel n'a pas tiré les conséquences légales de ses constatations, en violation de l'article L. 442-6 du code de commerce, dans sa rédaction applicable au litige.

- Extraits -

« 7. Il résulte de l'article 6, paragraphe 2, de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, dans sa rédaction issue de la loi n° 2016-444 du 13 avril 2016, que pèse sur les hébergeurs l'obligation légale d'agir promptement pour retirer des données dont ils connaissent le caractère illicite ou pour en rendre l'accès impossible et qu'ils engagent leur responsabilité en cas de manquement à cette obligation.

8. Il s'en déduit qu'en prévoyant une clause contractuelle lui permettant de suspendre promptement l'usage de ses services de référencement pour des raisons légales, puis en l'appliquant lorsqu'il est informé du caractère trompeur d'un site auquel il donne accès, un hébergeur ne crée pas un déséquilibre significatif au sens de l'article L. 442-6, I, 2°, devenu l'article L. 442-1, 2° du code de commerce.

Réponse de la Cour

13. Après avoir énoncé à bon droit que seules les entreprises qui jouissent de l'habilitation prévues à l'article R. 322-1, I, du code de la route ont le droit de collecter les données de leurs clients nécessaires à l'établissement de certificats d'immatriculation et le droit de prélever les taxes prévues par le code général des impôts au titre de la délivrance des certificats d'immatriculation, l'arrêt relève que la société Fathi ne disposait pas de l'habilitation requise et n'a pas cherché à l'obtenir après la suspension de son compte "Google Ads ".

14. En l'état de ces énonciations et constatations, la cour d'appel a exactement retenu que l'activité de la société Fathi était illicite, de sorte que la société Google Ireland n'avait pas commis d'abus en suspendant puis en refusant de réactiver ledit compte. »

Cass. 1re civ., 13 mars 2024, n° 22-12.345, *Sté SFR c/ Assoc. ADAPEI-ARIA de Vendée* : *JurisData* n° 2024-003031 ; *Comm. com. électr.* 2024, alerte 160, Cabinet Racine ; *Comm. com. électr.* 2024, comm. 46, Gr. Loiseau ; *Resp. civ. et assur.* 2024, comm. 109, C. Signat

Dans cet arrêt, la Cour de cassation rejette le pourvoi de SFR en rappelant tout d'abord que les articles 14 alinéa 1 et 2 et 15, I, de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) obligent le fournisseur d'accès à une bonne exécution des obligations résultant du contrat et le soumettent à une responsabilité de plein droit à l'égard de son client. De sorte que l'opérateur ne pouvait s'exonérer de tout ou partie de sa responsabilité qu'en apportant la preuve que l'inexécution est imputable soit au client, soit au fait d'un tiers étranger au contrat, soit à un cas de force majeure. La cour ajoute que l'article 15, I de la LCEN est bien d'ordre public, contrairement à ce que faisait valoir le demandeur dans ses prétentions. La cour écarte ensuite l'argument selon lequel l'article 7-4 prévu dans le contrat n'institue pas un délai de forclusion fixant un terme au droit d'agir du créancier, mais a plutôt pour objet de réduire conventionnellement le délai de la prescription auquel sont soumises les actions en justice engagées par un client à l'encontre de la société SFR. Dès lors, c'est à bon droit que la cour d'appel a conclu que la clause devait être réputée non écrite en ce qu'elle réduit l'action à moins d'un an à compter du jour où le titulaire du droit a connu ou aurait dû connaître les faits lui permettant de l'exercer. En effet, dans le contrat l'action était soumise à un an à compter du fait générateur, violant ainsi l'article 2254 du code civil. Enfin, la cour considère que le fournisseur d'accès à un service de communication électronique a gravement manqué à ses obligations contractuelles notamment en raison de la nécessité d'un réseau téléphonique et internet opérationnel dans le cadre de l'action de l'association en faveur des personnes handicapées, justifiant ainsi la résiliation des contrats.

Faits - Le litige opposait l'association ADAPEI-ARIA de Vendée à la Société française du radiotéléphone (SFR) ayant conclu un contrat afin que la dernière assure l'ensemble des prestations téléphoniques et internet des établissements de la première. Le contrat stipulait en son article 7-1 que SFR n'était soumis qu'à une obligation de moyen et que sa responsabilité ne pourrait être engagée qu'en cas de faute prouvée. Il était également prévu à l'article 7-4 qu'aucune action judiciaire ou réclamation du client ne pourrait être engagée ou formulée contre la société SFR plus d'un an après la survenance du fait générateur. L'association a finalement assigné l'opérateur téléphonique le 13 décembre 2018 afin d'obtenir la communication des contrats, leur résolution et la réparation des préjudices causés par des dysfonctionnement ayant perturbé son activité entre 2017 et 2018. La cour d'appel a finalement prononcé la résiliation des contrats aux torts de l'opérateur.

- Extraits -

« […] 7. Les dispositions prévues à l'article 15, I, précité, étant d'ordre public en ce qu'elles concernent les contrats conclus entre les fournisseurs d'accès à un service de communications électroniques et leurs clients, la liberté contractuelle ne permet pas d'y déroger.

[…] 14. Aux termes de l'article 2224 du code civil, les actions personnelles ou mobilières se prescrivent par cinq ans à compter du jour où le titulaire d'un droit a connu ou aurait dû connaître les faits lui permettant de l'exercer.

15. Selon l'article 2254, alinéa 1er, du code civil, la durée de la prescription peut être abrégée ou allongée par accord des parties. Elle ne peut toutefois être réduite à moins d'un an ni étendue à plus de dix ans.

16. Il s'en déduit que la prescription d'une action ne peut être réduite conventionnellement à moins d'un an à compter du jour où le titulaire du droit a connu ou aurait dû connaître les faits lui permettant de l'exercer.

17. L'arrêt constate que la clause prévue à l'article 7.4 soumettait l'action du client à une prescription d'un an après la survenance du fait générateur.
18. Il en résulte qu'en raison de la fixation du point de départ du délai d'un an à un tel événement, cette clause réduisait la prescription applicable en deçà de la limite fixée par l'article 2254 du code civil, de sorte qu'elle devait être réputée non écrite.

[…] 21. D'autre part, ayant retenu que l'association avait subi des dysfonctionnements récurrents pendant plusieurs mois entre 2017 et 2018 et que l'association avait dû faire face à des coupures à répétition et supporter un service dégradé alors que, pour l'accomplissement de ses missions en faveur des personnes handicapées et la communication avec les organismes sociaux, il était nécessaire qu'elle dispose d'un réseau téléphonique et internet opérationnel dans l'ensemble de ses établissements, la cour d'appel, qui a fait ressortir la gravité du manquement de la société SFR à ses obligations contractuelles et n'était pas tenue de suivre les parties dans le détail de leur argumentation, a légalement justifié sa décision. »

CJUE, 9 nov. 2023, aff. C-376/22, *Google Ireland Limited, Meta Platforms Ireland Limited, Tik Tok Technology Limited c/ Kommunikationsbehörde Austria* : *Comm. com. électr.* 2024, alerte 16, Cabinet Racine ; *JCP* G 2023, act. 1344, D. Berlin

La question préjudicielle émane d'un litige entre Google Ireland Limited, Meta Platforms Ireland Limited et Tik Tok Technology Limited, des sociétés basées en Irlande, et la Kommunikationsbehörde Austria (KommAustria), autorité autrichienne de régulation en matière de communication, concernant des décisions de cette dernière déclarant que ces sociétés sont soumises à la loi fédérale autrichienne sur les mesures de protection des utilisateurs de plateformes de communication. La KommAustria, en posant une question préjudicielle à la Cour de justice de l'Union européenne a cherché à savoir si les États membres peuvent prendre des mesures générales et abstraites visant une catégorie de services de la société de l'information. La Cour de justice de l'Union européenne a jugé que de telles mesures générales et abstraites entraveraient la libre circulation des services de la société de l'information et violeraient le principe du contrôle dans l'État membre d'origine, ainsi que les objectifs de la directive sur les services de l'information. En conséquence, la Cour a conclu que

la réglementation autrichienne est contraire au droit de l'Union européenne et représente un obstacle à la libre prestation des services de la société de l'information.

Faits – Le litige opposait le parquet général de la République de Lituanie (Lietuvos Respublikos generalinė prokuratūra) et A.G, procureur. Ce dernier a été démis de ses fonctions par le bureau du procureur général de Lituanie au motif qu'il aurait fourni illégalement, au cours d'enquêtes préliminaires, des informations à un suspect et à son avocat. Cette faute professionnelle reprochée au procureur et à l'origine de la sanction disciplinaire avait été établie aux moyens de données collectées et conservées par des fournisseurs de services de communications électroniques. Ce dernier a dès lors engagé une procédure devant les tribunaux lituaniens concernant la légalité de cette décision prise par le parquet général le révoquant de ses fonctions. Le Lietuvos vyriausiasis administracinis teismas (Cour administrative suprême de Lituanie) a décidé de surseoir et de saisir la CJUE de la question préjudicielle susvisée.

- Extraits -

« [...] La Cour a déjà jugé que l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, s'oppose à des mesures législatives prévoyant, à titre préventif, aux fins de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation (arrêt du 20 septembre 2022, SpaceNet et Telekom Deutschland, C-793/19 et C-794/19, EU:C:2022:702, points 74 et 131 ainsi que jurisprudence citée). En revanche, elle a précisé que cet article 15, paragraphe 1, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, ne s'oppose pas à des mesures législatives prévoyant, aux fins de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique [...]

L'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne,

Doit être interprété en ce sens que :

il s'oppose à ce que des données à caractère personnel relatives à des communications électroniques qui ont été conservées, en application d'une mesure législative prise au titre de cette disposition, par les fournisseurs de services de communications électroniques et qui ont par la suite été mises à la disposition, en application de cette mesure, des autorités compétentes à des fins de la lutte contre la criminalité grave, puissent être utilisées dans le cadre d'enquêtes relatives à des fautes de service apparentées à la corruption. »

CE, 6 mars 2024, n° 461193 et 461195, *Sté WebGroup Czech Republic et a.* : *Comm. com. électr.* 2024, comm. 57, E. Raschel

Le Conseil d'État examine la conformité du décret n° 2021-1306 du 7 octobre 2021, qui impose des mesures aux sites diffusant des contenus pornographiques pour empêcher l'accès des mineurs. L'arrêt s'inscrit dans un cadre plus large de protection des mineurs contre ces

contenus, conformément à la loi du 30 juillet 2020. Toutefois, le Conseil d'État soulève des questions sur la compatibilité du décret avec la directive 2000/31/CE sur le commerce électronique, en particulier sur la compétence des États membres pour réglementer les services de la société de l'information établis dans un autre État membre. Il décide de surseoir à statuer et saisit la Cour de justice de l'Union européenne (CJUE) pour trancher ces points.

Faits - La loi du 30 juillet 2020 vise à protéger les mineurs contre l'accès à la pornographie en rendant plus effective l'application de l'article 227-24 du Code pénal, qui interdit la diffusion de contenus pornographiques accessibles aux mineurs. Le décret du 7 octobre 2021 précise les modalités de mise en œuvre de cette loi, notamment en permettant à l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom) de mettre en demeure les éditeurs de sites pornographiques de bloquer l'accès aux mineurs. Les sociétés Webgroup Czech Republic et NKL Associates sro, éditrices de sites pornographiques, demandent l'annulation du décret, arguant qu'il viole le droit de l'Union européenne, notamment en ne respectant pas le principe de reconnaissance mutuelle et la directive 2000/31/CE.

- Extraits -

« 1. Afin de lutter contre l'exposition croissante des jeunes mineurs à des contenus pornographiques et contre les effets préjudiciables qu'une telle exposition produit sur leur construction psychologique et sur les violences faites aux femmes, la loi du 30 juillet 2020 a entendu renforcer [...] l'effectivité des dispositions de l'article 227-24 du code pénal. »

13. « La directive 2000/31 repose (…) sur l'application des principes de contrôle dans l'État membre d'origine et de la reconnaissance mutuelle, de telle sorte que, dans le cadre du domaine coordonné défini à l'article 2, sous h), de cette directive, les services de la société de l'information sont réglementés dans le seul État membre sur le territoire duquel les prestataires de ces services sont établis. »

17. Ces questions sont déterminantes pour la solution du litige que doit trancher le Conseil d'Etat. Elles présentent une difficulté sérieuse. Il y a lieu, par suite, d'en saisir la Cour de justice de l'Union européenne en application de l'article 267 du traité sur le fonctionnement de l'Union européenne et, jusqu'à ce que celle-ci se soit prononcée, de surseoir à statuer sur les requêtes ».

CA Paris, pôle 1, ch. 2, 21 déc. 2023, n° 23/06581, *Meta Platforms Ireland Limited c/ ANPAA* : *Comm. com. électr.* 2024, alerte 95, Cabinet Racine

La Cour d'appel de Paris, le 21 décembre 2023, rend une décision précisant dans quelles conditions les juges peuvent ordonner une levée d'anonymat de titulaires de comptes de réseaux sociaux faisant de la publicité pour des marques d'alcool. La Cour confirme la décision rendue par les juges de première instance ayant enjoint la société Meta de communiquer les données d'identification des titulaires des comptes à l'origine de publicités litigieuses. Cependant, les juges du fond précisent que cette infraction étant réprimée d'une peine inférieure à un an de prison, elle n'agit pas pour « les besoins de la lutte contre la criminalité et la délinquance grave » (article L. 34-1, 3°, du code des postes et des communications électroniques). Sur ce fondement, la société Meta n'a l'obligation de communiquer à l'ANPAA (L'Association nationale de prévention en alcoologie et addictologie) que les données d'identité civile des personnes derrière ces comptes Instagram.

Faits - L'Association nationale de prévention en alcoologie et addictologie (l'ANPAA) saisit la justice après avoir identifié plusieurs comptes ayant posté des publicités illicites pour des boissons alcoolisées sur le réseau social Instagram, hébergé par la société Meta. En effet, ces publications litigieuses, pour beaucoup, ne comportaient pas la mention légale imposée par la loi « Evin » (loi n° 91-32 du 10 janvier 1991) : « l'abus d'alcool est dangereux pour la santé ». Ces publicités associaient l'image de personnalités avec la consommation d'alcool dans des environnements festifs, joyeux et conviviaux. En première instance, le tribunal judiciaire de Paris rend une décision le 5 janvier 2023, selon la procédure accélérée au fond. Le tribunal enjoint Meta de communiquer les données d'identification des titulaires des comptes à l'origine des publicités litigieuses, sur le fondement de l'article L. 3351-7 du code de la santé publique. Le tribunal a également précisé que le retrait des publications n'était pas suffisant pour prévenir le dommage qui résultait des publications. La société Meta Platforms Ireland interjette appel de cette décision. La société demande aux juges du fond d'infirmer le jugement du tribunal judiciaire de Paris. Elle argue notamment que le tribunal aurait été dépourvu de pouvoir juridictionnel pour statuer sur la demande de l'ANPAA tendant à la communication des données de nature à identifier les titulaires des comptes. La Cour d'appel de Paris confirme la décision des juges de 1ère instance. Pour ordonner à Meta de communiquer les données d'identification des titulaires desdits compte, auteurs des publicités illicites pour des boissons alcoolisées, les juges du fond s'appuient, notamment, sur l'article 6 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN), qui dispose que « *Le président du tribunal judiciaire, statuant selon la procédure accélérée au fond, peut prescrire à toute personne susceptible d'y contribuer toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne* ».

- Extraits –

« Il en résulte que seul le président du tribunal judiciaire, statuant selon la procédure accélérée au fond, est compétent pour prescrire les mesures propres à prévenir ou faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne - ce qui peut inclure, le cas échéant, la communication de données d'identification lorsque celle-ci s'avère nécessaire à la prévention ou à l'arrêt du dommage. Contrairement à ce qu'indique donc l'appelante, le premier juge disposait bien du pouvoir juridictionnel pour statuer. »

« Au cas présent, l'ANPAA a sollicité la communication de données d'identification des auteurs de publications sur Instagram pour les besoins d'une procédure pénale, celle-ci souhaitant poursuivre les intéressés pour des faits d'infraction aux dispositions des articles L. 3323-2, L. 3323-4 à L. 3323-6, relatifs à la publicité des boissons alcooliques, prévues et réprimées par l'article L 3351-7 du code de la santé publique et hospitalière.

Elle n'agit donc pas 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 » visés au 3° de l'article L. 34-1 précité du code des postes et communications électroniques.
En application de ces dispositions, la société Meta n'est donc tenue de communiquer à l'ANPAA que les informations suivantes :
- les noms et prénoms ou la raison sociale du titulaire du compte,
- les pseudonymes utilisés,
- les adresses de courrier électronique ou de comptes associés.

Il y a lieu toutefois de constater que la société Meta ne s'oppose pas à communiquer en outre, si elle les a conservées, les données relatives à l'identifiant de connexion au moment de la création du compte, à l'adresse IP de connexion du compte et à la date de création des comptes. Les astreintes prononcées sont par ailleurs proportionnées et adaptées au litige, en ce compris celle dont est assortie l'injonction de retirer les publications litigieuses. Le jugement sera infirmé sur l'étendue de la communication. »

CJUE, ass. plén., 30 avr. 2024, aff. C-470/21 : *La Quadrature du Net e.a. contre Premier ministre et ministère de la Culture*

La Cour a jugé qu'une réglementation nationale peut permettre à une autorité publique de protection des droits d'auteur d'accéder aux données d'identité civile associées à des adresses IP collectées par les ayants droit. Toutefois, cet accès est soumis à des conditions strictes pour garantir la protection de la vie privée des utilisateurs. Ainsi, les données doivent être conservées de manière distincte, sans possibilité de recoupement, et pour une durée limitée au strict nécessaire. L'accès doit être restreint à l'identification des titulaires d'adresses IP suspectées d'infractions, sans permettre la reconstitution de leur navigation. En cas de réitération d'infractions, un contrôle préalable par une juridiction ou une autorité administrative indépendante est requis. Enfin, un audit régulier du système de traitement des données doit être assuré par un organisme tiers pour prévenir tout risque d'abus.

Faits - Des organisations de défense des droits et libertés numériques dont La Quadrature du Net ont contesté devant le Conseil d'État français le rejet implicite de leur demande d'abrogation du décret n° 2010-236 au motif qu'il porterait atteinte au droit au respect de la vie privée protégé par la Constitution et le droit de l'Union européenne. Elles estimaient que ce décret permettait à la Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet d'accéder aux données d'identité civile associées à des adresses IP sans contrôle judiciaire préalable. Cela constituant une violation de l'article 15 de la directive 2002/58 et des articles 7, 8, 11 et 52 de la Charte des droits fondamentaux de l'UE. Le Conseil d'État a saisi le Conseil constitutionnel d'une question prioritaire de constitutionnalité. Le Conseil constitutionnel a déclaré contraires à la Constitution les troisième et quatrième alinéa de l'article L331-21 du CPI, mais a déclaré conforme à celle-ci le cinquième alinéa dudit article à l'exception du mot « notamment » y figurant. Les requérantes soutenaient que le décret permettait un accès disproportionné aux données de connexion pour des infractions mineures au droit d'auteur, sans contrôle judiciaire préalable. Le Conseil d'État a rappelé la jurisprudence de la CJUE, selon laquelle l'accès aux données d'identité civile est autorisé sans délai pour la poursuite des infractions pénales, mais doit en principe être soumis à un contrôle préalable indépendant. Le Conseil d'État a relevé que la Hadopi collecte chaque année un grand nombre de données et qu'un contrôle préalable pourrait entraver sa mission. Le Conseil d'État a donc saisi la CJUE de trois questions préjudicielles portant sur l'obligation de contrôle préalable pour les données d'identité civile associées à une adresse IP ainsi que sur la possibilité d'un contrôle adapté, automatisé ou interne à une autorité indépendante.

- Extraits –

« 95. Il découle de la jurisprudence de la Cour que, dans le domaine de la lutte contre les infractions pénales, seuls les objectifs de lutte contre la criminalité grave ou de prévention de menaces graves pour la sécurité publique sont de nature à justifier l'ingérence grave dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte que comporte l'accès des autorités

publiques à un ensemble de données relatives au trafic ou de données de localisation, susceptibles de fournir des informations sur les communications effectuées par un utilisateur d'un moyen de communication électronique ou sur la localisation des équipements terminaux qu'il utilise et permettant de tirer des conclusions précises sur la vie privée des personnes concernées, sans que d'autres facteurs tenant à la proportionnalité d'une demande d'accès, tels que la durée de la période pour laquelle l'accès est sollicité à de telles données, puissent avoir pour effet que l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales en général soit susceptible de justifier un tel accès [arrêt du 2 mars 2021, *Prokuratuur* (Conditions d'accès aux données relatives aux communications électroniques), C-746/18, EU:C:2021:152, point 35].

96. En revanche, lorsque l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte que comporte l'accès des autorités publiques aux données relatives à l'identité civile conservées par les fournisseurs de services de communications électroniques, sans que ces données puissent être associées à des informations relatives aux communications effectuées, n'est pas grave dès lors que, prises dans leur ensemble, ces données ne permettent pas de tirer des conclusions précises concernant la vie privée des personnes dont les données sont concernées, ledit accès est susceptible d'être justifié par un objectif de prévention, de recherche, de détection et de poursuite des infractions pénales en général (voir, en ce sens, arrêt du 2 octobre 2018, *Ministerio Fiscal,* C-207/16, EU:C:2018:788, points 54, 57 et 60). »

Conseil d'État, juge des référés, 23 mai 2024, n° 494320, n° 494328, n° 494342, n° 494356, *La Quadrature du Net* : *JurisData* n° 2024-008051

La haute juridiction administrative, statuant en référé-liberté, a été appelée à se prononcer sur la légalité d'un arrêté ministériel autorisant la mise en œuvre d'un dispositif de surveillance et de collecte de données personnelles à des fins de lutte contre la criminalité organisée et le terrorisme. L'ordonnance de référé rendue par le Conseil d'État affirme la nécessité de concilier, d'une part, la garantie des droits et libertés fondamentaux, en particulier le droit au respect de la vie privée et le droit à la protection des données personnelles (articles 8 de la Convention européenne des droits de l'homme et 9 du Code civil), et d'autre part, la préservation de l'ordre public. Cette décision insiste sur la proportionnalité de la mesure et rappelle que les limitations aux libertés individuelles doivent être strictement encadrées, tant dans leurs modalités que dans leur durée, pour demeurer conformes au bloc de constitutionnalité et aux engagements internationaux de la France.

Faits - L'association *La Quadrature du Net*, spécialisée dans la défense des libertés numériques, a saisi le juge des référés du Conseil d'État afin de suspendre en urgence l'application d'un arrêté qui, selon elle, autoriserait une collecte de données de masse sans garanties suffisantes pour les droits fondamentaux des personnes surveillées. Le texte ministériel contesté avait pour ambition de doter les services de renseignement et les forces de l'ordre d'outils technologiques destinés à analyser en temps réel de grands volumes de données (métadonnées de connexion, informations de géolocalisation, historique de navigation, etc.). Le gouvernement soutenait que cette mesure était justifiée par l'impératif de sécurité publique, faisant valoir la menace terroriste persistante et la nécessité de détecter en amont les comportements criminels. Face à ces arguments, l'association requérante estimait que le dispositif portait une atteinte disproportionnée au respect de la vie privée et craignait un usage abusif de ces données, en raison notamment du caractère étendu et peu encadré de la surveillance autorisée.

- Extraits -

« (…) la mise en balance des intérêts en présence implique de vérifier que la mesure contestée, si elle poursuit un but légitime de sécurité publique, est strictement nécessaire et proportionnée, et comporte des garanties procédurales aptes à limiter toute dérive (…) »

« (…) le droit au respect de la vie privée est un principe à valeur constitutionnelle et conventionnelle dont la restriction ne peut être admise qu'en cas de menace caractérisée pour l'ordre public, sous réserve d'un encadrement légal rigoureux (…) »

« (…) en l'absence d'éléments attestant d'un usage abusif avéré ou d'une insuffisance manifeste de garanties dans la mise en œuvre du dispositif, l'urgence justifiant la suspension de l'arrêté ne saurait être retenue (…) ».

INTERNET ET PROTECTION DES DONNÉES PERSONELLES

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

CJUE, 3e ch., 25 janvier 2024, aff. C-687/21 : *Europe* 2024, comm. 127, D. Bouvier

La Cour a jugé que la simple transmission erronée d'un document contenant des données personnelles à un tiers non autorisé ne suffit pas, à elle seule, à établir l'insuffisance des mesures techniques et organisationnelles mises en place par le responsable du traitement en vertu du RGPD. Elle précise que le droit à réparation prévu à l'article 82 du RGPD a une fonction strictement compensatoire et non punitive, visant à indemniser intégralement le préjudice subi. La gravité de la violation n'est pas un critère requis pour accorder une réparation. Toutefois, la personne demandant réparation doit prouver à la fois la violation du RGPD et l'existence d'un dommage matériel ou moral. Enfin, une crainte subjective d'un usage abusif futur des données, en l'absence de preuve que le tiers non autorisé en a pris connaissance, ne constitue pas un dommage moral indemnisable.

Faits - Le requérant au principal a acheté un appareil électroménager dans un magasin Saturn, où un employé a enregistré ses données personnelles (nom, adresse, employeur, revenus, coordonnées bancaires) pour établir un contrat de vente et de crédit. Par erreur, ces documents ont été remis à un autre client, qui est parti avec l'appareil et les documents avant que l'erreur ne soit corrigée en moins de 30 minutes. Estimant l'indemnisation proposée par la société insuffisante, le requérant a saisi la justice, invoquant un préjudice moral lié aux risques causés par la perte de contrôle sur ses données personnelles. La juridiction de renvoi a posé plusieurs questions préjudicielles à la CJUE concernant l'interprétation de l'article 82 du RGPD. La juridiction de renvoi interroge la CJUE sur la nécessité de prouver un dommage moral en plus d'une violation du règlement pour obtenir réparation. Elle demande si la transmission erronée de données personnelles à un tiers constitue en soi une violation, et si la simple crainte d'un usage abusif des données peut suffire à caractériser un préjudice moral en vertu des articles 2, 5, 6 et 24 du règlement. Enfin, elle s'interroge sur le rôle de la gravité de la violation et souhaite connaître la finalité de la réparation d'un préjudice moral due au titre du RGPD.

- Extraits –

« 37. L'article 32 du RGPD précise, quant à lui, les obligations du responsable du traitement et d'un éventuel sous-traitant quant à la sécurité de ce traitement. Ainsi, le paragraphe 1 de cet article dispose que ces derniers doivent mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté aux risques liés audit traitement, en prenant en compte l'état des connaissances, les coûts de mise œuvre ainsi que la nature, la portée, le contexte et les finalités du traitement concerné. De même, le paragraphe 2 dudit article énonce que, lors de l'évaluation du niveau de sécurité approprié, il doit être tenu compte, en particulier, des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée des données à caractère personnel, ou de l'accès non autorisé à de telles données de manière accidentelle ou illicite (voir, en ce sens, arrêt du 14 décembre 2023, *Natsionalna agentsia za prihodite*, C-340/21, EU:C:2023:986, points 26 et 27).

38. Il ressort ainsi des libellés des articles 24 et 32 du RGPD que le caractère approprié des mesures mises en œuvre par le responsable du traitement doit être évalué de manière concrète, compte tenu des différents critères visés à ces articles et des besoins de protection des données spécifiquement inhérents au traitement concerné ainsi qu'aux risques induits par ce dernier, et cela d'autant plus que ledit responsable doit être en mesure de démontrer la conformité avec ce règlement desdites mesures, possibilité dont il serait privé si une présomption irréfragable était admise (voir, en ce sens, arrêt du 14 décembre 2023, *Natsionalna agentsia za prihodite*, C-340/21, EU:C:2023:986, points 30 à 32) ».

CJUE, gde ch., 5 déc. 2023, aff. C-683/21

La Cour a jugé qu'une entité peut être considérée comme responsable du traitement lorsqu'elle a chargé une entreprise de développer une application mobile et a participé à la détermination des finalités et des moyens du traitement des données à caractère personnel. La Cour a jugé qu'une entité peut être considérée comme responsable du traitement lorsqu'elle a chargé une entreprise de développer une application mobile et a participé à la détermination des finalités et des moyens du traitement des données à caractère personnel. Cela même si elle n'a pas réalisé elle-même d'opérations de traitement ni donné son accord explicite à pour l'exécution de l'application, à moins qu'elle se soit expressément opposée à sa mise en service avant sa mise à disposition du public. La Cour précise que la responsabilité conjointe ne nécessite pas d'accord formel entre les entités sur la finalité et les moyens du traitement ni sur leurs obligations respectives.

Faits - Dans le contexte de la pandémie de COVID-19, le ministre de la Santé de Lituanie a chargé le Centre national de santé publique (ci-après "CNSP") d'acquérir un système informatique pour enregistrer et suivre les données des personnes exposées au virus. La société ITSS a développé une application mobile destinée à cette fin avec la collaboration du CNSP. Elle a été mise en ligne et utilisée par 3 802 personnes, collectant des données sensibles. Cependant, aucun contrat de marché public n'a été conclu entre le CNSP et ITSS. L'Inspection nationale de protection des données (ci-après INPD) a infligé des amendes au CNSP et à ITSS, considérant qu'ils étaient responsables conjoints du traitement des données personnelles. Le tribunal administratif de Vilnius interroge la CJUE sur l'interprétation de la notion de « responsable du traitement » au sens de l'article 4 du RGPD, notamment pour savoir si une entité publique ayant initié l'acquisition d'un outil de collecte de données, mais sans conclure de contrat de marché public ni gérer l'outil, peut être qualifiée de responsable du traitement. Il demande également si cette qualification peut découler du simple fait que l'entité est mentionnée dans la politique de protection des données ou dans l'application elle-même. La Cour est aussi invitée à préciser si une entité peut être responsable du traitement sans avoir réalisé d'opérations de traitement ni donné d'instructions explicites, ainsi que si l'utilisation de copies de données personnelles à des fins de test constitue un traitement au sens du RGPD. Enfin, la juridiction de renvoi s'interroge sur le champ d'application des amendes administratives prévues à l'article 83 du RGPD, en particulier si les actions de traitement des données à caractère personnel inappropriées réalisées par le sous-traitant engagent la responsabilité juridique du responsable du traitement.

- Extraits –

« 30. La Cour a déjà jugé que toute personne physique ou morale qui influe, à des fins qui lui sont propres, sur le traitement de telles données et participe de ce fait à la détermination des

finalités et des moyens de ce traitement peut être considérée comme étant responsable dudit traitement. À cet égard, il n'est pas nécessaire que les finalités et les moyens du traitement soient déterminés au moyen de lignes directrices écrites ou de consignes de la part du responsable du traitement (voir, en ce sens, arrêt du 10 juillet 2018, *Jehovan todistajat*, C-25/17, EU : C:2018:551, points 67 et 68), ni que celui-ci ait été formellement désigné comme tel.

31. Dès lors, pour établir si une entité, telle que le CNSP, peut être considérée comme étant responsable du traitement au sens de l'article 4, point 7, du RGPD, il convient d'examiner si cette entité a effectivement influé, à des fins qui lui sont propres, sur la détermination des finalités et des moyens de ce traitement.

32. En l'occurrence, sous réserve des vérifications qu'il appartient à la juridiction de renvoi d'effectuer, il ressort du dossier dont dispose la Cour que la création de l'application mobile en cause a été commandée par le CNSP et visait à mettre en œuvre l'objectif assigné par celui-ci, à savoir la gestion de la pandémie de COVID-19 par le biais d'un outil informatique aux fins de l'enregistrement et du suivi des données des personnes exposées au virus de la COVID-19. Le CNSP avait prévu à cette fin que les données à caractère personnel des utilisateurs de l'application mobile en cause soient traitées. Il ressort en outre de la décision de renvoi que les paramètres de cette application, tels que les questions posées et leur formulation, ont été adaptés aux besoins du CNSP et que celui-ci a joué un rôle actif dans leur détermination. »

CJUE, ass. plén., 30 avr. 2024, aff. C-470/21 : *La Quadrature du Net e.a. contre Premier ministre et ministère de la Culture*

La Cour a jugé qu'une réglementation nationale peut permettre à une autorité publique de protection des droits d'auteur d'accéder aux données d'identité civile associées à des adresses IP collectées par les ayants droit. Toutefois, cet accès est soumis à des conditions strictes pour garantir la protection de la vie privée des utilisateurs. Ainsi, les données doivent être conservées de manière distincte, sans possibilité de recoupement, et pour une durée limitée au strict nécessaire. L'accès doit être restreint à l'identification des titulaires d'adresses IP suspectées d'infractions, sans permettre la reconstitution de leur navigation. En cas de réitération d'infractions, un contrôle préalable par une juridiction ou une autorité administrative indépendante est requis. Enfin, un audit régulier du système de traitement des données doit être assuré par un organisme tiers pour prévenir tout risque d'abus.

Faits - Des organisations de défense des droits et libertés numériques dont La Quadrature du Net ont contesté devant le Conseil d'État français le rejet implicite de leur demande d'abrogation du décret n° 2010-236 au motif qu'il porterait atteinte au droit au respect de la vie privée protégé par la Constitution et le droit de l'Union européenne. Elles estimaient que ce décret permettait à la Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet d'accéder aux données d'identité civile associées à des adresses IP sans contrôle judiciaire préalable. Cela constituant une violation de l'article 15 de la directive 2002/58 et des articles 7, 8, 11 et 52 de la Charte des droits fondamentaux de l'UE. Le Conseil d'État a saisi le Conseil constitutionnel d'une question prioritaire de constitutionnalité. Le Conseil constitutionnel a déclaré contraires à la Constitution les troisième et quatrième alinéa de l'article L331-21 du CPI, mais a déclaré conforme à celle-ci le cinquième alinéa dudit article à l'exception du mot « notamment » y figurant. Les requérantes soutenaient que le décret permettait un accès disproportionné aux données de connexion pour des infractions mineures au droit d'auteur, sans contrôle judiciaire préalable. Le Conseil d'État a rappelé la jurisprudence de la CJUE, selon laquelle l'accès aux

données d'identité civile est autorisé sans délai pour la poursuite des infractions pénales, mais doit en principe être soumis à un contrôle préalable indépendant. Le Conseil d'État a relevé que la Hadopi collecte chaque année un grand nombre de données et qu'un contrôle préalable pourrait entraver sa mission. Le Conseil d'État a donc saisi la CJUE de trois questions préjudicielles portant sur l'obligation de contrôle préalable pour les données d'identité civile associées à une adresse IP ainsi que sur la possibilité d'un contrôle adapté, automatisé ou interne à une autorité indépendante.

- Extraits –

« 95. Il découle de la jurisprudence de la Cour que, dans le domaine de la lutte contre les infractions pénales, seuls les objectifs de lutte contre la criminalité grave ou de prévention de menaces graves pour la sécurité publique sont de nature à justifier l'ingérence grave dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte que comporte l'accès des autorités publiques à un ensemble de données relatives au trafic ou de données de localisation, susceptibles de fournir des informations sur les communications effectuées par un utilisateur d'un moyen de communication électronique ou sur la localisation des équipements terminaux qu'il utilise et permettant de tirer des conclusions précises sur la vie privée des personnes concernées, sans que d'autres facteurs tenant à la proportionnalité d'une demande d'accès, tels que la durée de la période pour laquelle l'accès est sollicité à de telles données, puissent avoir pour effet que l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales en général soit susceptible de justifier un tel accès [arrêt du 2 mars 2021, *Prokuratuur* (Conditions d'accès aux données relatives aux communications électroniques), C-746/18, EU:C:2021:152, point 35].

96. En revanche, lorsque l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte que comporte l'accès des autorités publiques aux données relatives à l'identité civile conservées par les fournisseurs de services de communications électroniques, sans que ces données puissent être associées à des informations relatives aux communications effectuées, n'est pas grave dès lors que, prises dans leur ensemble, ces données ne permettent pas de tirer des conclusions précises concernant la vie privée des personnes dont les données sont concernées, ledit accès est susceptible d'être justifié par un objectif de prévention, de recherche, de détection et de poursuite des infractions pénales en général (voir, en ce sens, arrêt du 2 octobre 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, points 54, 57 et 60). »

CEPD, opinion 08/2024, 17 avr. 2024

L'Opinion 08/2024 du Comité européen de la protection des données (CEPD) aborde une question centrale en matière de protection des données personnelles dans le contexte des technologies émergentes. Elle clarifie les obligations des responsables de traitement et des sous-traitants concernant l'utilisation des données biométriques, en particulier dans le cadre de l'intelligence artificielle (IA). Cette opinion souligne l'importance du respect des principes de licéité, de loyauté et de transparence (article 5 du RGPD), ainsi que la nécessité d'une base légale solide pour le traitement des données biométriques. Elle rappelle également que ces données, considérées comme sensibles, sont soumises à des exigences renforcées en matière de protection. Enfin, le CEPD insiste sur la responsabilité des acteurs dans la mise en œuvre de mesures techniques et organisationnelles appropriées pour garantir la sécurité des données, conformément à l'article 32 du RGPD. Ainsi, les plateformes doivent proposer une

alternative équitable et abordable aux utilisateurs qui refusent le traitement de leurs données. Le consentement ne doit pas être conditionné à des frais excessifs, ce qui pourrait le rendre non libre. Les utilisateurs doivent être informés de manière claire et accessible des implications de leur choix.

Contexte - Le Comité européen de la protection des données (CEPD) a été saisi pour examiner la conformité au RGPD du modèle « consentement ou paiement » proposé par une grande plateforme en ligne. Ce modèle offre aux utilisateurs le choix entre consentir au traitement de leurs données personnelles à des fins de publicité ciblée ou payer pour accéder au service sans publicité. L'objectif de l'avis est de déterminer si ce modèle respecte les principes du RGPD. En effet, le projet impliquait la collecte, le stockage et l'analyse des données biométriques des employés, avec l'utilisation d'algorithmes d'IA pour identifier les individus. Cependant, des doutes ont été soulevés quant à la conformité du projet avec les principes du RGPD, notamment en ce qui concerne la proportionnalité, la minimisation des données et le consentement éclairé.

- Extraits -

« Le traitement des données biométriques, en raison de leur caractère sensible, doit être justifié par une base légale spécifique et répondre à des finalités clairement définies. Les responsables de traitement doivent s'assurer que les mesures techniques et organisationnelles mises en place garantissent un niveau de sécurité adapté aux risques, conformément à l'article 32 du RGPD. Par ailleurs, toute utilisation de technologies d'intelligence artificielle doit être transparente et respecter les droits des personnes concernées, notamment leur droit à l'information et à l'opposition. (…) Pour que le consentement soit valide, il doit être libre, spécifique, éclairé et univoque. Un modèle qui impose des frais disproportionnés pour refuser le traitement des données personnelles ne respecte pas le critère de liberté du consentement. Par conséquent, un tel traitement ne peut être fondé sur le consentement au sens de l'article 4(11) du RGPD ».

INTERNET ET DROIT DE LA PROPRIÉTÉ INTELLECTUELLE

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

Sacem/Deezer, 25 oct. 2023: *RLDI*, nov. 2023, n° 208.

Après avoir lancé le premier modèle de redistribution Artist-Centric focalisé sur les auteurs, compositeurs et éditeurs de musique, Deezer s'allie à la Sacem dans le cadre d'une étude ayant pour objectif d'explorer de nouvelles méthodes de redistribution de la valeur des écoutes en streaming. Ainsi, les données d'écoutes de la plateforme Deezer vont être analysées afin d'évaluer différents modèles économiques. L'ambition d'un tel projet est de permettre d'assurer une rémunération plus équitable pour les auteurs, compositeurs et éditeurs de cette industrie.

- Extraits -

« Cette initiative commune doit donc déterminer comment la monétisation des droits des auteurs, des compositeurs et des éditeurs de musique peut évoluer sur la base du modèle « *Artist-Centric* » proposé par Deezer.

Basées sur l'analyse approfondie des données de Deezer, des améliorations clés ont été intégrées dans le nouveau modèle Artist-Centric visant à se focaliser sur les artistes ; à la démonétisation de contenus non musicaux ; à lutter contre la fraude ; favoriser une approche centrée sur l'utilisateur (User-Centric). »

CSPLA, rapp. *De mission sur la science ouverte et le droit d'auteur*, 4 mars 2024

Le rapport du CSPLA examine l'évolution de la diffusion des publications scientifiques à l'ère de la science ouverte, en mettant en balance les impératifs d'accessibilité et les droits des auteurs. Il s'intéresse particulièrement aux différents modèles d'accès ouvert et à leur compatibilité avec le cadre juridique français et international du droit d'auteur.

Si la publication des travaux de recherche a toujours reposé sur l'intervention d'éditeurs assurant la validation et la diffusion des contenus, l'essor du numérique et des politiques de libre accès transforme profondément ce modèle. Plusieurs modèles d'accès ouvert existent, mais ils ne garantissent pas tous une diffusion de qualité et une juste reconnaissance des auteurs. Le rapport évalue leur impact sur la vitalité de l'édition scientifique et sur la rémunération et la reconnaissance des chercheurs. Plutôt que d'imposer une généralisation de l'accès ouvert, le rapport préconise un encadrement juridique préservant à la fois la liberté des chercheurs et la diversité des modèles de publication, en insistant sur le respect du droit d'auteur et la nécessité d'une coordination interministérielle. La mission met en garde contre une ouverture incontrôlée qui pourrait profiter principalement aux grandes plateformes numériques, sans garantir la qualité scientifique ni la juste rémunération des auteurs.

Le rapport recommande ainsi une approche mesurée, s'appuyant sur les modèles existants tout en évitant une standardisation excessive qui pourrait fragiliser l'écosystème de l'édition scientifique française.

- Extraits -

« Le scientifique-auteur, perçu à la fois dans son individualité et comme membre d'une communauté de chercheurs, a émergé avec la science moderne. […] L'identification d'un travail à un auteur constitue un enjeu symbolique central, qui, pour le scientifique en début de carrière, peut reléguer au second plan les autres attributs du droit d'auteur. » (p. 10)

« Le modèle diamant, en rendant les publications accessibles immédiatement et sans frais pour les auteurs ni les lecteurs, repose sur des financements institutionnels. Toutefois, il peut conduire à une perte d'indépendance des chercheurs vis-à-vis des financeurs et à une concentration accrue des publications au sein d'un nombre restreint de plateformes. » (p. 37)

« L'augmentation du coût des abonnements, supérieure à l'inflation, a fortement pesé sur les budgets des bibliothèques et des universités, accentuant les inégalités d'accès aux publications scientifiques. […] Cette évolution a cristallisé un sentiment de captation de la valeur créée par les chercheurs au bénéfice de quelques grands groupes internationaux. » (p. 21)

« Le droit d'auteur du chercheur ne constitue pas en soi un obstacle à la science ouverte, mais il doit être préservé comme un mécanisme garantissant la reconnaissance et la protection des travaux. […] Toute exception nouvelle à ce principe doit satisfaire au test en trois étapes de la convention de Berne. » (p.60)

« Les recommandations de l'Unesco et de l'Union européenne vont dans le sens d'une ouverture immédiate des publications financées sur fonds publics. Cependant, les États doivent veiller à encadrer cette évolution afin de préserver la diversité éditoriale et d'éviter une dépendance excessive aux plateformes numériques. » (p. 78)

« Sans cadre juridique suffisant, clair et ferme, le risque est grand d'une captation abusive de tous les écrits scientifiques par les grandes plateformes financées grâce à leurs recettes publicitaires et développant des modèles d'intelligence artificielle sans garantie de qualité scientifique ni de juste rémunération des auteurs. » (p. 83)

L. n° 2024-449, 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, art. 62, modifiant CPI, art. L. 131-4 : *Comm. com. électr.*, n° 7-8, juill.-août 2024, comm. 62, comm. P. Kamina

La loi n° 2024-449 du 21 mai 2024, visant à sécuriser et réguler l'espace numérique, a modifié l'article L. 131-4 du Code de la propriété intellectuelle. Cette modification porte sur les modalités de rémunération des auteurs en cas de cession de leurs droits.

L'ancienne version (en vigueur du 11 mai 1994 au 17 février 2024) disposait que :

« La cession par l'auteur de ses droits sur son œuvre peut être totale ou partielle. Elle doit comporter au profit de l'auteur la participation proportionnelle aux recettes provenant de la vente ou de l'exploitation.

Toutefois, la rémunération de l'auteur peut être évaluée forfaitairement dans les cas suivants (...) ».

La nouvelle version (en vigueur à partir du 21 mai 2024) dispose désormais que :

« La cession par l'auteur de ses droits sur son œuvre peut être totale ou partielle. Elle doit comporter au profit de l'auteur une ***rémunération appropriée et distincte*** *pour chaque mode d'exploitation. Cette rémunération est* ***proportionnelle*** *aux recettes provenant de la vente ou de l'exploitation. Toutefois, la rémunération de l'auteur peut être évaluée forfaitairement dans les cas suivants (...)".*

A la seconde phrase du premier alinéa de l'article L. 131-4 du code de la propriété intellectuelle, les mots : « la participation » sont remplacés par les mots : « une rémunération appropriée et distincte ». Toutefois, la rémunération forfaitaire à titre d'exception est maintenue.

Désormais, la loi n° 2024-449, 21 mai 2024 visant à sécuriser et à réguler l'espace numérique impose une rémunération proportionnelle aux recettes d'exploitation, renforçant ainsi les droits financiers des auteurs, avec une rémunération plus juste à leur égard puisque celle-ci est désormais "appropriée".

Cette nouvelle disposition vise à assurer une juste rémunération des créateurs à l'ère numérique, où les modes de diffusion et de monétisation des œuvres ont évolué. En effet, cette réforme vise à adapter le cadre juridique aux évolutions technologiques et aux nouveaux modes de diffusion des œuvres à l'ère numérique, garantissant ainsi une rémunération plus juste et transparente pour les créateurs.

Le commentaire de P. Kamina, publié dans la revue *Communication Commerce Électronique* (CCE), n° 7-8, juillet-août 2024, comm. 62, analyse en détail les implications de cette modification législative. Il souligne que cette évolution légale renforce les droits des auteurs en leur assurant une participation proportionnelle aux revenus générés par leurs œuvres, quel que soit le mode d'exploitation utilisé.

En résumé, la modification de l'article L. 131-4 du CPI par la loi n° 2024-449 du 21 mai 2024 vise à assurer une rémunération équitable et proportionnelle pour les auteurs, adaptée aux divers modes d'exploitation de leurs œuvres dans le contexte numérique actuel.

Décret n° 2023-497 du 22 juin 2023 relatif aux modalités de communication au public du prix des offres de livres neufs et d'occasion : *Comm. com. électr.*, n° 4, avr. 2024, chron. 5, obs. E. Emile-Zola-Place

Par ce texte, pris en application des principes établis par la loi relative au prix unique du livre, le pouvoir réglementaire entend renforcer la transparence de l'information délivrée au consommateur, tant pour les ouvrages neufs que pour ceux vendus d'occasion. Le décret modifie notamment les obligations des vendeurs en leur imposant de communiquer clairement et sans équivoque le prix de référence de l'ouvrage (prix éditeur ou prix public conseillé) ainsi que le prix effectivement pratiqué, lorsque ce dernier diffère en raison d'une offre promotionnelle ou d'un rabais pour les livres d'occasion. L'ambition affichée est de prévenir toute pratique commerciale trompeuse en garantissant une lisibilité renforcée des offres, conformément à l'objectif d'intérêt général de soutien et de régulation du marché du livre. Par

ailleurs, le texte s'inscrit dans la continuité des dispositions existantes visant à protéger la filière du livre et à promouvoir la biblio diversité, en maintenant notamment un encadrement strict du recours aux remises pour les ouvrages neufs et un contrôle accru des mentions liées à l'occasion.

Contexte - Avant la promulgation du décret, de nombreux acteurs du secteur – auteurs, éditeurs, libraires et associations de consommateurs – avaient fait état de dysfonctionnements dans la présentation des prix des livres. Plusieurs plateformes de vente en ligne, en particulier, ne distinguaient pas toujours clairement les ouvrages neufs de ceux d'occasion ou faisaient apparaître des écarts de prix non justifiés par rapport au prix éditeur. Ce manque de transparence portait à confusion pour l'acheteur et nuisait à la confiance dans la vente en ligne de livres, au détriment des librairies physiques et d'une saine concurrence. C'est dans ce contexte que le gouvernement a adopté le décret n° 2023-497, afin d'assurer un traitement homogène et loyal des différentes offres de livres, quelle que soit la modalité de distribution (physique ou numérique). Le texte crée une obligation renforcée de clarté et de visibilité du prix et prévoit des sanctions, administratives et pénales, à l'encontre des opérateurs qui ne s'y conformeraient pas.

- Extraits -

« (…) est considérée comme trompeuse toute offre de vente de livres, neufs ou d'occasion, dont la présentation ne ferait pas apparaître de manière explicite le prix de référence et le prix pratiqué… »

« (…) les vendeurs sont tenus de mentionner de façon lisible et non équivoque la distinction entre livre neuf et livre d'occasion ; la mention de toute réduction ou remise doit être accompagnée de l'indication du prix antérieurement pratiqué (…) »

« (…) le non-respect de ces prescriptions expose les contrevenants aux sanctions prévues par le Code de la consommation, sans préjudice des éventuelles actions civiles en réparation du préjudice subi. »

Cass. com., 6 mars 2024, n° 22-23.657, n°22-22.651 et n° 22-18.818, *B+L* : *RLDI*, n° 214, mai 2024, 4916

Dans ces trois arrêts rendus le 6 mars 2024, la Chambre commerciale de la Cour de cassation apporte des précisions importantes sur la responsabilité des plateformes en ligne en matière de contrefaçon de droits de propriété intellectuelle (DPI) et sur les obligations des intermédiaires techniques en vertu de la loi pour la confiance dans l'économie numérique (LCEN). Ces décisions confirment que les plateformes en ligne, bien qu'elles ne soient pas considérées comme des éditeurs de contenu, doivent prendre des mesures actives pour prévenir et retirer les contenus illicites dès qu'elles en ont connaissance. Les arrêts renforcent également les obligations de coopération des plateformes avec les titulaires de droits et clarifient les conditions dans lesquelles leur responsabilité peut être engagée. Ainsi dans ces arrêts, la Cour reconnaît que les plateformes en ligne ne peuvent pas se contenter d'un rôle passif dès lors qu'elles ont reçu une notification claire et précise concernant des contenus contrefaisants. Elles sont tenues de réagir promptement pour retirer ou bloquer l'accès à ces contenus.

De plus, elles doivent coopérer activement avec les titulaires de droits pour prévenir et mettre fin aux infractions. Cette obligation inclut la mise en place de mécanismes efficaces pour traiter les notifications de contenus illicites. La Cour confirme par la suite que les plateformes ne peuvent pas invoquer leur statut d'intermédiaire technique pour se soustraire à leurs obligations. Leur responsabilité peut être engagée si elles ne prennent pas des mesures appropriées pour retirer les contenus illicites dès qu'elles en ont connaissance. Enfin, les mesures prises par les plateformes pour retirer des contenus illicites doivent être proportionnées et ne pas entraver indûment la liberté d'entreprise. Toutefois, dans les cas d'espèce, le retrait des contenus contrefaisants était justifié au regard du préjudice causé aux titulaires de droits.

Faits – Les trois affaires concernent des plateformes en ligne (désignées sous les noms de code "B" et "L") qui hébergeaient des annonces ou des contenus publiés par des utilisateurs tiers, portant atteinte à des droits de propriété intellectuelle (marques et droits d'auteur). Les titulaires de droits avaient notifié aux plateformes la présence de ces contenus illicites, mais celles-ci n'avaient pas réagi suffisamment rapidement pour les retirer. Les titulaires de droits ont alors engagé des actions en justice pour obtenir le retrait des contenus litigieux et des dommages-intérêts.

- Extraits –

« 12. La Cour relève que, dès lors qu'une plateforme en ligne a connaissance de contenus illicites, elle est tenue de prendre des mesures appropriées pour les retirer ou en bloquer l'accès, conformément aux dispositions de l'article 6. I. 2 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN).

13. En l'espèce, les plateformes B et L, ayant reçu des notifications claires et détaillées concernant des contenus contrefaisants, n'ont pas agi avec la diligence requise pour mettre fin à l'infraction.

14. Par conséquent, la Cour estime que la responsabilité des plateformes peut être engagée pour manquement à leurs obligations légales. »

CJUE, 5e ch., 21 mars 2024, aff. C-10/22, *Liberi editori e autori (LEA) c/ Jamendo SA* : *Comm. com. électr.*, n° 5, mai 2024, comm. 43, ob. P. Kamina

Cet arrêt de la CJUE clarifie la compatibilité d'une législation nationale qui interdit aux entités de gestion indépendantes établies dans un autre État membre d'exercer l'activité d'intermédiation en matière de gestion du droit d'auteur sur son territoire. La Cour juge qu'une telle exclusion absolue contrevient à l'article 56 TFUE relatif à la libre prestation des services. La CJUE affirme que, bien que la directive 2014/26/UE (sur la gestion collective des droits d'auteur) ne prévoit pas explicitement le droit pour ces entités d'exercer leur activité dans un autre État membre, une interdiction totale est disproportionnée et constitue une restriction non justifiée au regard du principe de libre prestation des services.

Faits - Liberi editori e autori (LEA), un organisme de gestion collective italien, engage une action contre Jamendo SA, une entité de gestion indépendante luxembourgeoise, exerçant en Italie depuis 2004. LEA demande au Tribunal de Rome d'ordonner à Jamendo de cesser son

activité en Italie, soutenant que celle-ci est exercée illégalement au regard du droit national. Jamendo conteste cette interprétation et soutient que la transposition italienne de la directive 2014/26/UE est erronée, car elle ne reconnaît pas aux entités de gestion indépendantes les droits prévus par cette directive. L'affaire est renvoyée à la CJUE pour savoir si une interdiction nationale générale de telles entités est compatible avec le droit de l'Union.

- Extraits -

« 53. Il y a lieu de considérer que cette directive n'harmonise pas les conditions d'accès des entités de gestion indépendantes à l'activité de gestion du droit d'auteur et, partant, qu'elle ne s'oppose pas à une législation d'un État membre qui exclut de manière générale et absolue la possibilité pour les entités de gestion indépendantes établies dans un autre État membre de prester dans ce premier État membre leurs services de gestion du droit d'auteur. »

« 77. Une mesure nationale qui ne permet pas aux entités de gestion indépendantes établies dans un autre État membre de prester en Italie leurs services de gestion du droit d'auteur et des droits voisins constitue manifestement une restriction à la libre prestation des services garantie à l'article 56 TFUE. »

« 98. Une réglementation nationale qui empêche, de manière absolue, toute entité de gestion indépendante, quelles que soient les exigences réglementaires auxquelles celle-ci est soumise en vertu du droit national de l'État membre dans lequel elle est établie, d'exercer une liberté fondamentale garantie par le traité FUE, apparaît aller au-delà de ce qui est nécessaire pour protéger le droit d'auteur. »

99. L'article 56 TFUE, lu en combinaison avec la directive 2014/26/UE, doit être interprété en ce sens qu'il s'oppose à une législation d'un État membre qui exclut de manière générale et absolue la possibilité pour les entités de gestion indépendantes établies dans un autre État membre de prester dans ce premier État membre leurs services de gestion du droit d'auteur. »

Cass. 1re civ., 15 nov. 2023, n° 22-23.266 : *JurisData* n° 2023-020293 ; *Comm. com. électr.* 2024, comm. 3, P. Kamina ; C. Masson, *Prescription et action en contrefaçon et droit d'auteur : plaidoyer pour un dualisme tempéré*, *Comm. com. électr.*, n° 4, avr. 2024, étude 6

La première chambre civile de la Cour de cassation, par un arrêt rendu le 15 novembre 2023, statue sur la question de savoir si une action en contrefaçon est soumise à la prescription de droit commun de l'article 2224 du code civil. La Cour de cassation confirme que l'action en contrefaçon se prescrit par cinq ans à compter du jour où le titulaire d'un droit a connu ou aurait dû connaître les faits lui permettant de l'exercer. Ainsi, elle rejette le pourvoi d'un artiste sculpteur qui arguait que ce délai de droit commun de cinq années pour agir n'était pas applicable à l'action en contrefaçon. La première chambre civile confirme le raisonnement des juges du fond qui ont jugé à bon droit que la prescription de droit commun contenue dans le code civil s'applique aux actions en contrefaçon de droit d'auteur.

Faits - Un artiste, sculpteur et peintre a été sollicité par le fondateur d'un musée afin de créer une œuvre destinée au musée en question. L'œuvre commandée est une sculpture représentant trois cheveux dans une demi-vasque circulaire. Cependant, selon cet artiste, cette œuvre a fait l'objet de plusieurs reproductions sans son autorisation par la suite. Parmi ces reproductions, l'exposition dans les jardins d'une société ayant pour activité la gestion de jardins botaniques

et parc animalier. Par conséquent, l'auteur assigne la société en contrefaçon de droit d'auteur afin de faire cesser le trouble illicite et d'obtenir une indemnisation. La Cour d'appel de Douai, par un arrêt rendu le 22 septembre 2022, prononce irrecevables les demandes de l'artiste d'indemnisation et de cessation du trouble illicite sur le fondement de la contrefaçon de droit d'auteur. En effet, les juges de fond retiennent que l'action en réparation se prescrit par cinq années, à compter du jour où le titulaire a connu ou aurait dû connaître les faits lui permettant d'exercer cette action. Par conséquent, l'auteur se pourvoit en cassation. Il argue que l'action aux fins de faire cesser les atteintes ne serait soumise à aucun délai de prescription. Selon lui, n'étaient pas prescrites ses demandes tendant à faire cesser les actes de contrefaçon par la remise entre ses mains de l'œuvre contrefaisante aux fins de destruction. Cela s'expliquerait par le principe que la propriété ne s'éteint pas par le non-usage. A l'occasion de cet arrêt, la Cour de cassation confirme que l'action en contrefaçon se prescrit par cinq ans à compter du jour où le titulaire d'un droit a connu ou aurait dû connaître les faits lui permettant de l'exercer. Ainsi, elle rejette le pourvoi de l'artiste et confirme le raisonnement des juges du fond qui ont jugé à bon droit que la prescription de droit commun contenue dans le code civil s'applique aux actions en contrefaçon de droit d'auteur. L'action était en effet prescrite en l'espèce.

- Extraits -

« **Énoncé du moyen**

6. M. [P] fait grief à l'arrêt de déclarer irrecevables ses demandes formées contre la société le potager des
Princes, alors « que si l'action en réparation des atteintes portées aux droits de l'auteur se prescrit par cinq ans à compter du jour où le titulaire a connu ou aurait dû connaître les faits lui permettant de l'exercer,
l'action aux fins de faire cesser lesdites atteintes n'est soumise à aucun délai de prescription, la propriété ne s'éteignant pas par le non usage ; qu'en retenant, pour déclarer irrecevable l'ensemble des demandes formées par M. [P] au titre de la contrefaçon de sa statue intitulée "Fontaine aux chevaux" ou "la Prueva", que la prescription des actions civiles en contrefaçon de droit d'auteur est soumise au délai quinquennal de l'article 2224 du code civil dont le point de départ est le jour où le titulaire a eu connaissance de la contrefaçon, même si celle-ci s'inscrit dans la durée, et que M. [P] a été informé de la présence de la statue litigieuse dans le jardin de la société le potager des Princes dès le rapport d'expertise du 3 septembre 2004 dans le cadre de l'instruction pénale qui a abouti à l'arrêt de la cour d'appel de Paris du 17 décembre 2008 reconnaissant son caractère contrefaisant, de sorte que le délai de prescription a expiré le 17 décembre 2013, cependant que n'étaient pas prescrites les demandes de M. [P] tendant à faire cesser les actes de contrefaçon par la remise entre ses mains de l'œuvre contrefaisante aux fins de destruction, la cour d'appel a violé les articles 544, 2224 et 2227 du code civil. »

Réponse de la Cour

7. Aux termes de l'article 2224 du code civil, les actions personnelles ou mobilières se prescrivent par cinq ans à compter du jour où le titulaire d'un droit a connu ou aurait dû connaître les faits lui permettant de l'exercer.

8. C'est à bon droit que, après avoir énoncé que la prescription des actions civiles en contrefaçon de droit d'auteur est soumise à ces dispositions, la cour d'appel a retenu que, le délai de prescription ayant commencé à courir le 17 décembre 2008, date à laquelle avait été admis le

caractère contrefaisant de l'œuvre exposée, l'action intentée le 5 mars 2021 était prescrite, même si la contrefaçon s'inscrivait dans la durée.

Cass. com., 6 mars 2024, n° 22-23.657, n° 22-22.651 et n° 22-18.818, FS-B : *RLDI*, n° 216, juill. 2024, note J. Groffe-Charrier

La Cour de cassation confirme que la mise à disposition d'un logiciel par téléchargement, accompagnée d'un contrat de licence d'utilisation visant à permettre son usage permanent contre paiement, constitue une vente impliquant un transfert de propriété. En conséquence, une clause de réserve de propriété peut être opposée à un sous-acquéreur, permettant au fournisseur d'exercer un droit de revendication sur le prix en cas de procédure collective. Elle rejette ainsi l'argument de Factofrance selon lequel la fourniture de logiciels ne constituerait qu'un contrat de louage et non une vente. En validant l'opposabilité des clauses de réserve de propriété, elle confirme la primauté du droit des fournisseurs sur les créances de prix par rapport à l'affactureur.

Faits - Les sociétés TD Synnex France et Arrow ECS ont vendu des logiciels et matériels informatiques à la société Overlap, qui les a ensuite fournis à des clients finaux, dont Evolium et Capgemini Technology Services. Ces ventes étaient assorties de clauses de réserve de propriété. Overlap a été placée en redressement puis liquidation judiciaire en 2013 et 2014, laissant impayées plusieurs factures. Les fournisseurs ont revendiqué leurs créances de prix auprès des clients finaux. Parallèlement, Factofrance, en tant qu'affactureur d'Overlap, revendiquait les mêmes créances au titre de la subrogation conventionnelle prévue dans son contrat d'affacturage. Les fournisseurs soutenaient que la vente des logiciels incluait un transfert de propriété, rendant les clauses de réserve de propriété opposables. Factofrance contestait cette qualification, estimant qu'il ne s'agissait que d'un droit d'utilisation et non d'une vente. Les litiges portaient sur la titularité des créances et l'application des clauses de réserve de propriété aux licences de logiciels.

- Extraits -

« 10. (22-23.657) "La mise à disposition d'une copie d'un logiciel par téléchargement et la conclusion d'un contrat de licence d'utilisation y afférente visant à rendre ladite copie utilisable par le client de manière permanente moyennant le paiement d'un prix implique le transfert du droit de propriété de cette copie. »

« 11. (22-23.657) "Dès lors, Tech Data est fondée à solliciter l'application de la clause de réserve de propriété pour cette cession de droit d'utilisation de ses logiciels, droit dont Evolium est sous-acquéreur. »

« 5. (22-22.651) Les parties n'ont pas entendu remettre en cause leurs accords antérieurs, notamment l'application des dispositions de l'article 5 des CGV de la société Arrow signées par la société Overlap. »

« 9 (22-22.651) La mise à disposition d'une copie d'un logiciel par téléchargement et la conclusion d'un contrat de licence d'utilisation y afférente impliquent le transfert du droit de propriété de cette copie. »

« 7. (22-18.818) "Toutefois, la première vente d'un exemplaire d'un logiciel [...] épuise le droit de mise sur le marché de cet exemplaire dans tous les États membres à l'exception du droit d'autoriser la location ultérieure. »

« 10. (22-18.818) "ETC, cédant des licences d'utilisation des logiciels, est fondée à solliciter l'application de la clause de réserve de propriété sur cette cession de droit d'utilisation de ses logiciels. »

Internet et droit de la consommation

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

- **Pratiques commerciales**

L. n° 2023-451, 9 juin 2023, visant à encadrer l'influence commerciale et à lutter contre les dérives des influenceurs sur les réseaux sociaux : *JO* 10 juin 2023, texte n° 1

Adoptée le 9 juin 2023, la législation encadrant les influenceurs vise à définir et réguler leur activité sur les réseaux sociaux, tout en luttant contre d'éventuelles dérives. Son objectif principal est d'apporter une meilleure protection aux influenceurs eux-mêmes et aux internautes, en clarifiant leur rôle et leurs responsabilités. Pour cela, elle introduit des définitions précises et renforce les obligations des plateformes en ligne.
L'article L. 7124-1 du code du travail est ainsi modifié : A la fin du 5ème alinéa, les mots : « de partage de vidéos » sont remplacés par les mots : « en ligne au sens du i de l'article 3 du règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) ».
Cette loi définit les influenceurs comme des personnes ou entités qui, en échange d'une rémunération, utilisent leur notoriété pour promouvoir des produits ou services sur internet. Elle encadre également l'activité des agents d'influenceurs (articles 7, 8, 9), leur imposant la défense des intérêts de leurs mandants. Par ailleurs, les plateformes en ligne doivent désormais signaler les contenus illicites (articles 1, 7, 10). Cette réglementation impose également de nouvelles obligations aux influenceurs et aux utilisateurs des réseaux sociaux. Certaines pratiques publicitaires sont interdites, et toute publication à caractère commercial doit être clairement identifiée par des mentions explicites comme "publicité" ou "collaboration commerciale". En cas de non-respect, des sanctions sont prévues (articles 3, 4, 5, 8). Afin de prévenir les abus et les escroqueries, des mesures ont été mises en place pour informer les abonnés sur la nature commerciale des contenus et sanctionner les comportements trompeurs. L'affichage obligatoire des retouches sur les photos et vidéos s'inscrit dans cette démarche (articles 5, 16). En cas de pratiques commerciales frauduleuses, des peines d'amende et d'emprisonnement peuvent être appliquées. Les plateformes sont également tenues de signaler les contenus illicites, sous la surveillance renforcée de la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) (articles 4, 9, 12). En clair, ce cadre juridique vise à protéger les consommateurs tout en favorisant un développement responsable du secteur de l'influence sur les réseaux sociaux.

Contexte - Les influenceurs sont des créateurs de contenu actifs sur les réseaux sociaux, disposant d'une communauté d'abonnés qu'ils cherchent à influencer à travers leurs publications. Leur activité repose sur la promotion directe ou indirecte de biens et services (article 1 de la loi). Toutefois, de nombreuses dérives et escroqueries ont émergé, entraînant des préjudices pour les internautes. La loi n° 2023-451 du 9 juin 2023 est fondamentale en ce qu'elle encadre l'influence commerciale et lutte contre les dérives des influenceurs, à une ère où le secteur de l'influence est omniprésent sur les réseaux sociaux.

CJUE, 30 mai 2024, aff. C-662/22 et C-667/22, *Airbnb Ireland* : *JurisData* n° 2024-008148. – CJUE, 30 mai 2024, aff. C-663/22, *Expedia* : *JurisData* n° 2024-008149. – CJUE, 30 mai 2024, aff. C-664/22 et C-666/22, *Google Ireland* : *JurisData* n° 2024-008150 et *JurisData* n° 2024-008148

La Cour de justice de l'Union européenne (CJUE), par trois arrêts rendus le 30 mai 2024, répond à trois questions préjudicielles portant sur l'interprétation des mêmes textes. La Cour rejette la possibilité pour des États membres d'imposer à des fournisseurs de services d'intermédiation en ligne et de moteurs de recherche en ligne, établis dans un autre État membre, de s'inscrire à un registre tenu par une autorité de cet État membre, de communiquer à celle-ci une série d'informations détaillées sur leur organisation ainsi que de lui verser une contribution financière. La Cour interprète les dispositions nationales litigieuses au regard de la directive 2000/31/CE relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique »). Elle juge qu'il résulte de l'article 3 de la directive 2000/31 que chaque État membre veille à ce que les services de la société de l'information fournis par un prestataire établi sur son territoire respectent le droit national de cet État membre relevant du domaine coordonné (défini à l'article 2, h) de la directive 2000/31/CE). Ce même article ajoute que les États membres ne peuvent, pour des raisons relevant du domaine coordonné, restreindre la libre circulation des services de la société de l'information en provenance d'un autre État membre. Ainsi, la CJUE juge qu'un État membre ne peut, même pour des raisons de protection des consommateurs, imposer aux professionnels établis dans un autre État membre et proposant ses services sur son territoire des conditions d'exercice plus contraignantes que celles de la directive, comme l'inscription sur un registre national.

Faits - Le 30 mai 2024, la Cour de justice de l'Union européenne (CJUE) rend trois arrêts répondant à des questions préjudicielles similaires puisqu'elles concernaient l'interprétation des mêmes textes, notamment la directive 2000/31/CE du 8 juin 2000 et le règlement (UE) 2019/1150 du 20 juin 2019, promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne (règlement dit « Platform to business »).
Plusieurs sociétés ont saisi la justice en réaction à des mesures adoptées par l'Autorité de tutelle des communications (Italie, AGCOM). Ces mesures concernent les fournisseurs de services d'intermédiation en ligne et de moteurs de recherche en ligne. En effet, dans le cadre d'une mise en œuvre de manière effective du règlement (UE) 2019/1150 dit « Platform to business », l'Italie a imposé aux prestataires de services d'intermédiation et de moteurs de recherche en ligne de s'inscrire sur un registre tenu par l'AGCOM, de lui communiquer une série d'informations détaillées ainsi que de payer une contribution financière.
Dans la première affaire (CJUE, 30 mai 2024, aff. C-662/22 et C-667/22), il s'agit des sociétés Airbnb Ireland UC (société de droit irlandais) et Amazon Services Europe Sarl (société de droit luxembourgeois) qui s'opposent aux mesures adoptées par l'AGCOM.
S'agissant du deuxième contentieux (CJUE, 30 mai 2024, aff. C-663/22), une société étatsunienne (société Expedia Inc) qui gère des plateformes informatiques fournissant des services de réservation d'hébergements et de voyages conteste également les nouvelles mesures de l'AGCOM. La société Expedia Inc argue devant le juge italien que les obligations de communication à l'AGCOM (imposées par le droit italien) sont contraires au règlement 2019/1150. Sur la base de ce règlement, la société soutient qu'il serait impossible d'alourdir les exigences procédurales imposées aux fournisseurs de services d'intermédiation en ligne.

Enfin, le dernier litige très similaire (CJUE, 30 mai 2024, aff. C-664/22 et C-666/22) concernait les sociétés Google Ireland Ltd et Eg Vcation Rentals, elles aussi s'opposant aux mesures adoptées par l'AGCOM.
La CJUE répond à ces questions préjudicielles, dans trois arrêts rendus le 30 mai 2024. Elle affirme l'impossibilité pour des États membres d'imposer à des fournisseurs de services d'intermédiation en ligne et de moteurs de recherche en ligne, établis dans un autre État membre, de s'inscrire à un registre tenu par une autorité de cet État membre, de communiquer à celle-ci une série d'informations détaillées sur leur organisation ainsi que de lui verser une contribution financière. En effet, la Cour conclut que le seul fait que les mesures nationales en cause aient été adoptées dans le but déclaré d'assurer l'application du règlement (UE) 2019/1150 n'implique pas que ces mesures soient nécessaires pour garantir l'un des objectifs énumérés à l'article 3, § 4, a), i) de la directive, à savoir, la protection de l'ordre public, de la santé publique, de la sécurité publique, ou des consommateurs.

CJUE, 30 mai 2024, aff. C-662/22 et C-667/22, *Airbnb Ireland*

« Par ces motifs, la Cour (deuxième chambre) dit pour droit :

L'article 3 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 (« directive sur le commerce électronique »), doit être interprété en ce sens que :

il s'oppose à des mesures adoptées par un État membre, dans le but déclaré de veiller à l'application adéquate et effective du règlement (UE) 2019/1150 du Parlement européen et du Conseil, du 20 juin 2019, promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne, en vertu desquelles, sous peine de sanctions, les fournisseurs de services d'intermédiation en ligne, établis dans un autre État membre, sont soumis, en vue de prester leurs services dans le premier État membre, à l'obligation de s'inscrire à un registre tenu par une autorité de cet État membre, à celle de communiquer à celle-ci une série d'informations détaillées sur leur organisation ainsi qu'à celle de lui verser une contribution financière. »

CJUE, 30 mai 2024, aff. C-663/22, *Expedia*

« Par ces motifs, la Cour (deuxième chambre) dit pour droit :

Le règlement (UE) 2019/1150 du Parlement européen et du Conseil, du 20 juin 2019, promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne, doit être interprété en ce sens que :

il ne justifie pas, en vue de l'application adéquate et effective de ce règlement, l'adoption par un État membre de mesures en vertu desquelles, sous peine de sanctions, les fournisseurs de services d'intermédiation en ligne sont soumis, en vue de prester leurs services dans cet État membre, à l'obligation d'envoyer périodiquement à une autorité de ce dernier un document relatif à leur situation économique, dans lequel doivent être détaillées de nombreuses informations relatives notamment aux recettes réalisées par ces fournisseurs. »

Comm. UE, communiqué, 8 nov. 2024 (Temu) pratiques commerciales

Le règlement (UE) 2023/988 du Parlement européen et du Conseil du 10 mai 2023 relatif à la sécurité générale des produits (RSGP) dont l'applicabilité était prévue pour le 13 décembre 2024, accroit la protection des consommateurs. En effet, il impose l'existence d'un opérateur économique établi dans l'Union européenne responsable, non seulement pour veiller au respect des exigences en matière de sécurité des produits, mais aussi afin de veiller au respect des obligations spécifiques des places de marché en ligne qui ciblent les consommateurs.

Rappel - En vertu du règlement relatif à la coopération en matière de protection des consommateurs, le réseau CPC (*Consumer Protection Cooperation Network*), composé des autorités nationales de protection des consommateurs (en l'espèce de la Belgique, l'Allemagne et l'Irlande) et de la Commission européenne, a enjoint la société Temu de se mettre en conformité avec la législation européenne en matière de protection des consommateurs. Dans le communiqué émis par la Commission le 8 novembre 2024 à Bruxelles, il est indiqué que, dans le cadre de leurs achats sur la plateforme, les consommateurs sont confrontés à des pratiques problématiques telles que la proposition de fausses remises ou encore la fourniture de faux avis induisant le consommateur en erreur. Cette action est sans préjudice des procédures engagées par les autorités nationales (notamment par l'autorité hongroise de la concurrence, l'office polonais de la concurrence et de la protection des consommateurs et la direction générale de la concurrence, de la consommation et de la répression des fraudes en France) en relation avec les pratiques commerciales de la société. Parallèlement, la Commission avait ouvert le 31 mai 2024 une procédure formelle à l'encontre de la plateforme en raison de son récent statut de très grande plateforme en ligne et son manquement aux obligations plus strictes qui en découlent. Temu disposait d'un délai d'un mois pour répondre aux conclusions du réseau et proposer des engagements quant à la manière dont elle compte remédier aux problèmes.

- Extraits (français) -

« […] Principaux éléments de l'action coordonnée du réseau CPC

Le réseau CPC a recensé plusieurs types de pratiques problématiques concernant Temu, que les autorités considèrent comme contraires à la législation de l'UE en matière de protection des consommateurs, telles que :

- De fausses remises donnant l'impression erronée que des produits sont proposés au rabais alors qu'il n'en est rien ;
- Des pressions à la vente exercées sur les consommateurs pour qu'ils achèvent leurs achats en recourant à des tactiques telles que des allégations mensongères concernant des stocks limités ou de faux délais d'achat ;
- Une ludification forcée consistant à obliger les consommateurs à jouer à la « roue de la fortune » pour accéder à la place de marché en ligne tout en dissimulant des informations essentielles sur les conditions d'utilisation liées aux récompenses du jeu ;
- Des informations manquantes et trompeuses consistant à afficher des informations incomplètes ou inexactes sur les droits légaux des consommateurs à renvoyer les produits et à obtenir des remboursements. Temu omet également d'informer les consommateurs à l'avance du fait que leur commande doit atteindre un certain montant avant qu'ils puissent achever leurs achats ;

- De faux avis consistant en la fourniture d'informations inadéquates sur la façon dont Temu garantit l'authenticité des avis publiés sur son site web. Les autorités nationales ont relevé des avis dont elles soupçonnent qu'ils sont faux ;
- Des coordonnées cachées qui empêchent les consommateurs de contacter facilement Temu pour poser des questions ou introduire des réclamations.

En outre, le réseau CPC a demandé à Temu de lui fournir des informations qui lui permettront d'évaluer le respect par l'entreprise d'autres obligations découlant du droit de l'UE en matière de protection des consommateurs, telles que l'obligation d'informer clairement ces derniers du statut professionnel ou non du vendeur, de veiller à ce que les classements, les avis et les notations des produits ne leur soient pas présentés de manière trompeuse, de veiller à ce que les réductions de prix soient annoncées et calculées correctement et de veiller à ce que toute allégation environnementale soit exacte et étayée.

Prochaines étapes

Temu dispose à présent d'un délai d'un mois pour répondre aux conclusions du réseau CPC et proposer des engagements quant à la manière dont la plateforme compte remédier aux problèmes recensés en matière de protection des consommateurs. En fonction de la réponse de Temu, le réseau CPC pourra engager un dialogue avec l'entreprise. Si Temu ne répond pas aux préoccupations soulevées par le réseau CPC, les autorités nationales pourront prendre des mesures d'exécution pour garantir le respect de la législation. Elles pourront notamment infliger des amendes fondées sur le chiffre d'affaires annuel réalisé par Temu dans les États membres concernés. Cette possibilité est sans préjudice du pouvoir des autorités nationales de prendre des mesures d'exécution dans les procédures en cours.

[…]

Temu a été désignée en tant que très grande plateforme en ligne le 31 mai 2024 en vertu du règlement sur les services numériques. Quatre mois après sa désignation, Temu devait se conformer aux obligations les plus strictes applicables aux très grandes plateformes en ligne. Il s'agit notamment de l'obligation d'évaluer et d'atténuer dûment tout risque systémique découlant de son service. À la suite d'une enquête préliminaire, la Commission a ouvert, le 31 octobre 2024, une procédure formelle afin de déterminer si Temu a enfreint le règlement sur les services numériques dans des domaines liés à l'évaluation, à la gestion et à l'atténuation des risques, à la transparence des systèmes de recommandation, ainsi qu'à l'accès des chercheurs aux données. »

- Extraits (anglais) -

« […] Key elements of the CPC Network's coordinated action

The CPC Network identified several types of problematic practices on Temu, which they consider to be in breach of EU consumer protection laws, such as:

- Fake discounts: Giving the false impression that products are offered with a discount where there is none.
- Pressure selling: Putting consumers under pressure to complete purchases using tactics like false claims about limited supplies or false purchase deadlines.

- Forced gamification: Forcing consumers to play a ‘spin the fortune wheel' game to access the online marketplace, while hiding essential information about the conditions of use linked to the rewards of the game.
- Missing and misleading information: Displaying incomplete and incorrect information about consumers' legal rights to return goods and receive refunds. Temu also fails to inform consumers in advance that their order needs to reach a certain minimum value before they can complete their purchase.
- Fake reviews: Giving inadequate information about how Temu ensures the authenticity of reviews published on its website. National authorities found reviews which they suspect to be unauthentic.
- Hidden contact details: Consumers cannot easily contact Temu for questions or complaints.

In addition, the CPC Network requested information from Temu to assess the company's compliance with further obligations under EU consumer law, such as the obligation to inform consumers clearly whether the seller of a product is a trader or not; to ensure that product rankings, reviews, and ratings are not presented to consumers in a misleading manner; to ensure that price reductions are announced and calculated correctly; and to ensure that any environmental claims are accurate and substantiated.

Next steps

Temu now has one month to reply to the CPC Network's findings and propose commitments on how they will address the identified consumer law issues. Depending on Temu's reply, the CPC Network may enter a dialogue with the company. If Temu fails to address the concerns raised by the CPC Network, national authorities can take enforcement measures to ensure compliance. This includes the possibility to impose fines based on Temu's annual turnover in the Member States concerned. This is without prejudice to the power of national authorities to take enforcement measures in ongoing proceedings.

[…]

Temu was designated as a Very Large Online Platform (VLOP) on 31 May 2024 under the Digital Services Act (DSA). Four months from its designation, Temu had to comply with the most stringent obligations applicable to VLOPs. These include the obligation to duly assess and mitigate any systemic risks stemming from its services. Following a preliminary investigation, the Commission opened on 31 October 2024 formal proceedings to assess whether Temu may have breached the DSA in areas linked to the assessment, management, and mitigation of risks, to the transparency of recommender systems and to data access for researchers. »

Comm. UE, communiqué, 12 nov. 2024 (*Apple*)

Le communiqué de la Commission européenne du 12 novembre 2024 concerne une décision majeure dans le cadre d’une enquête antitrust visant Apple. Cette décision porte sur des pratiques anticoncurrentielles présumées liées à l’écosystème de l’App Store et à ses conditions d’accès pour les développeurs tiers. La Commission européenne souligne que les règles imposées par Apple aux développeurs d’applications, notamment les commissions obligatoires (souvent appelées « taxe Apple ») et les restrictions techniques, constituent une violation des règles de concurrence établies par l’article 102 du Traité sur le fonctionnement

*de l'Union européenne (TFUE)***.** *Ces pratiques sont considérées comme un abus de position dominante, limitant l'accès au marché et portant préjudice aux consommateurs et aux développeurs. La Commission estime que ces pratiques créent des barrières à l'entrée sur le marché, limitent l'innovation et entraînent des prix plus élevés pour les consommateurs finaux. Cette décision marque une étape importante dans la régulation des géants de la tech et renforce la volonté de l'UE de garantir une concurrence équitable dans le secteur numérique.*

Faits - L'enquête de la Commission européenne a été ouverte à la suite de plaintes déposées par plusieurs développeurs d'applications et associations professionnelles. Les griefs principaux concernent d'abord les commissions élevées (jusqu'à 30 %) prélevées par Apple sur les ventes d'applications et les achats intégrés (in-app purchases), également l'obligation pour les développeurs d'utiliser le système de paiement d'Apple, sans possibilité de proposer des alternatives. Enfin, les restrictions techniques empêchant les développeurs de communiquer directement avec les utilisateurs pour proposer des offres hors de l'App Store.

- Extraits -

Sur l'abus de position dominante : « Apple occupe une position dominante sur le marché des applications mobiles pour ses appareils iOS. En imposant des conditions restrictives aux développeurs, tels que des commissions élevées et l'obligation d'utiliser son système de paiement exclusif, Apple abuse de cette position dominante, en violation de l'article 102 du TFUE. »

Sur les commissions excessives : « Les commissions allant jusqu'à 30 % prélevées par Apple sur les transactions effectuées via l'App Store sont disproportionnées par rapport aux services rendus. Ces commissions entraînent une augmentation des coûts pour les développeurs, qui se répercutent in fine sur les consommateurs. »

Sur les restrictions techniques : « Apple interdit aux développeurs d'informer les utilisateurs de la possibilité de souscrire à des services ou d'effectuer des achats en dehors de l'App Store. Cette restriction empêche les développeurs de proposer des offres alternatives et limite la concurrence sur le marché. »

Sur les conséquences pour les consommateurs : « Les pratiques d'Apple ont pour effet de limiter le choix des consommateurs et de maintenir des prix artificiellement élevés. Cela nuit à l'innovation et à la diversité des services disponibles sur le marché. »

CJUE, 26 sept. 2024, aff. C-330/23, *Aldi Süd* : *JurisData* n° 2024-022294

Dans son arrêt du 26 septembre 2024, la Cour de justice de l'Union européenne (CJUE) apporte des précisions essentielles sur l'interprétation de l'article 6 bis de la directive 98/6/CE, relatif à l'annonce des réductions de prix. La Cour confirme que toute réduction de prix annoncée doit être calculée sur la base du prix antérieur effectif, défini comme le prix le plus bas pratiqué par le professionnel au cours des 30 jours précédant la réduction. La CJUE écarte l'application de la directive 2005/29/CE sur les pratiques commerciales déloyales dans ce cas spécifique, en vertu de l'article 3, paragraphe 4, qui prévoit que les règles sectorielles (comme la directive 98/6) priment sur les règles générales. Ainsi, une annonce de réduction de prix peut être considérée comme illicite sans qu'il soit nécessaire de démontrer son caractère trompeur, dès lors qu'elle ne respecte pas les exigences de l'article 6 bis. Cette décision renforce la protection des consommateurs en garantissant une information claire et

transparente sur les prix, tout en clarifiant les obligations des entreprises en matière de publicité promotionnelle.

Faits - l'affaire oppose une association de consommateurs à la chaîne de supermarchés Aldi Süd. L'association reproche à Aldi d'avoir annoncé des réductions de prix sur des produits alimentaires en utilisant des pourcentages ou des mentions valorisantes telles que « prix choc », sans que ces réductions ne soient calculées sur la base du prix le plus bas pratiqué au cours des 30 jours précédents. Aldi a annoncé des réductions de prix en pourcentage sans que celles-ci ne correspondent au prix le plus bas appliqué dans les 30 jours précédents. La chaîne de supermarché a également utilisé des allégations publicitaires comme « prix choc » pour des produits dont le prix annoncé était en réalité supérieur au prix le plus bas pratiqué pendant la période de référence

- Extraits -

« Toute annonce d'une réduction de prix doit indiquer le prix antérieur effectif, défini comme le prix le plus bas appliqué par le professionnel au cours des 30 jours précédant la réduction. Cette obligation s'applique tant aux réductions exprimées en pourcentage qu'aux allégations publicitaires valorisantes telles que "prix choc". »
(…) « En vertu de l'article 3, paragraphe 4, de la directive 2005/29/CE, les dispositions de la directive 98/6/CE priment sur les règles générales relatives aux pratiques commerciales déloyales. Ainsi, une annonce de réduction de prix peut être jugée illicite sans qu'il soit nécessaire d'examiner son caractère trompeur, dès lors qu'elle ne respecte pas les exigences de l'article 6 bis. »
(…) « L'objectif de l'article 6 bis est de garantir une information claire et transparente pour les consommateurs, afin qu'ils puissent prendre des décisions d'achat éclairées. Toute interprétation contraire irait à l'encontre de cet objectif. »

- **Pratiques restrictives et protection des consommateurs**

Cass. com., 4 sept. 2024, n° 22-12.321 FS-B*, Sté Up to Motion c/ Google France et Google Ire land* : *JurisData* n° 2024-014907 ; *Comm. com. électr*. 2024, comm. 97, Gr. Loiseau ; Contrats, conc. consom. 2024, comm. 172, S. Bernheim-Desvaux ; Contrats, conc. consom. 2024, comm. 149, N. Mathey

Cet arrêt de la chambre commerciale de la Cour de cassation du 4 septembre 2024 confirme que les clauses permettant à un hébergeur de suspendre immédiatement et de résilier unilatéralement un contrat en cas d'activité illicite du client ne sont pas abusives. Il réaffirme l'obligation des hébergeurs d'intervenir rapidement pour faire cesser des activités illicites, renforçant ainsi leur rôle dans la régulation du contenu en ligne. Elle établit que la suspension et la résiliation sans préavis sont justifiées lorsqu'une activité illicite est avérée, et que de telles clauses ne créent pas de déséquilibre significatif au détriment du client.

Faits - Une société exploitait un site internet facilitant l'obtention de certificats d'immatriculation de véhicules en France et avait conclu un contrat de référencement avec Google via son service "Google Ads". Les conditions générales du service prévoyaient la possibilité pour Google de suspendre et de résilier un compte sans préavis en cas de violation des politiques de Google ou pour des raisons légales. Après avoir été informé par le secrétaire d'État chargé du numérique que la société ne disposait pas de l'habilitation nécessaire du

ministère de l'Intérieur pour délivrer ces certificats, Google a suspendu puis résilié son compte. La société a contesté cette résiliation, arguant que la clause autorisant ces actions était abusive.

- Extraits –

« La faculté de suspendre immédiatement le compte d'un client était justifiée par l'atteinte portée par le contenu d'un site internet à l'ordre public, particulièrement en cas de publicité trompeuse. »

(…) **«** L'exercice de son droit de décider unilatéralement et sans préavis de la fin du contrat, légitimé par l'illicéité de l'activité, n'avait créé aucun déséquilibre significatif. »

(…) « En vertu de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, les hébergeurs ont l'obligation d'agir promptement pour retirer ou rendre inaccessible des données dont ils ont connaissance du caractère illicite. »

INTERNET ET DROIT DU TRAVAIL

Par A. Saint-Martin, Avocat, cabinet ASM, Montpellier

Cass. soc., 27 septembre 2023, n°20-22.465 FS-B : *Comm. com. électr.* 2023, comm. 79, G. Loiseau

L'arrêt rendu par la chambre sociale de la Cour de cassation porte sur la requalification d'un contrat de prestation de services en contrat de travail. La Cour de cassation a cassé la décision de la cour d'appel, celle-ci ayant privé sa décision de base légale en rejetant cette requalification, sans analyser concrètement les conditions effectives dans lesquelles le livreur exerçait son activité, telles que fixées par les stipulations contractuelles. La Cour de cassation rappelle que le lien de subordination est caractérisé par l'exécution d'un travail sous l'autorité d'un employeur qui a le pouvoir de donner des ordres et des directives, d'en contrôler l'exécution et de sanctionner les manquements de son subordonné. Autrement dit, peut constituer un indice de subordination, le travail au sein d'un service organisé lorsque l'employeur en détermine unilatéralement les conditions d'exécution. L'affaire a été renvoyée pour une nouvelle analyse des conditions réelles d'exécution du travail.

Faits - Dans cette affaire, M. [W] avait conclu le 23 avril 2014 un contrat de prestation de services avec la société TTT pour des activités de livraison. Après la rupture du contrat le 25 novembre 2014, M. [W] a saisi la juridiction prud'homale pour obtenir la requalification de cette relation en contrat de travail. La cour d'appel de Paris, dans un arrêt du 8 octobre 2020, avait rejeté sa demande, estimant que M. [W] n'apportait pas la preuve d'un lien de subordination caractérisant une relation de travail salarié. Ce dernier a alors formé un pourvoi en cassation.

- Extraits -

« Vu les articles L. 1221-1 et L. 8221-6 du code du travail :

9. Le lien de subordination est caractérisé par l'exécution d'un travail sous l'autorité d'un employeur qui a le pouvoir de donner des ordres et des directives, d'en contrôler l'exécution et de sanctionner les manquements de son subordonné. Peut constituer un indice de subordination le travail au sein d'un service organisé lorsque l'employeur en détermine unilatéralement les conditions d'exécution.

10. Pour débouter M. [W] de sa demande, l'arrêt retient que l'intéressé ne rapporte pas la preuve qu'il exerçait ses fonctions dans le cadre d'un service organisé, qu'il se contente d'affirmer, sans produire aucun élément, qu'il n'avait aucune liberté quant à la manière de réaliser son travail dans le choix des lieux d'achat et des biens commandés, qu'il ne justifie pas plus d'un pouvoir de contrôle par la société de son activité et de la faculté pour cette dernière de sanctionner ses agissements, qu'il n'est pas démontré que la société exerçait un contrôle assorti d'un pouvoir de sanction sur le port de la tenue TTT, qu'il ne ressort pas plus des éléments de la cause qu'il aurait été tenu de rendre compte de son activité à la société, que la réalité d'un pouvoir de notation de la société n'est pas plus démontrée, que la seule référence au contrat de prestation

de service qui prévoit un droit d'audit et de contrôle de la société n'est pas suffisante, l'existence d'une relation de travail dépendant des conditions de fait dans lesquelles est exercée l'activité du travailleur.

12. En se déterminant ainsi, sans analyser concrètement les conditions effectives dans lesquelles le livreur exerçait son activité, telles que fixées par les stipulations contractuelles, l'intéressé faisant valoir qu'il devait livrer des biens pour le compte de la société TTT sans pouvoir se constituer une clientèle propre ou travailler pour une société concurrente, devait utiliser une carte bancaire fournie par la société TTT pour effectuer les achats qui étaient ensuite livrés, ce dont il déduisait être intégré dans un service organisé, qu'il était rémunéré en fonction d'un taux horaire fixe et avait l'obligation de porter une tenue au logo de la société sous peine de sanction consistant en la résiliation du contrat et d'accepter la commande dès lors qu'il était connecté sans pouvoir la refuser, la cour d'appel a privé sa décision de base légale. »

Cass. soc., ass. plén., 22 décembre 2023, n° 20-20.648 B+R : *JurisData* n° 2023-023012

Dans cet arrêt fondateur, la Cour affirme que lorsque le droit à la preuve tel que garanti par l'article 6, §1 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales entre en conflit avec d'autres droits et libertés, notamment le droit au respect de la vie privée, il appartient au juge de mettre en balance les différents droits et intérêts en présence. Dans le cadre d'un procès civil, le juge doit apprécier si une preuve obtenue ou produite de manière illicite ou déloyale, 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.

Faits - L'arrêt de l'Assemblée plénière de la Cour de cassation du 22 décembre 2023 concerne un litige entre la société Abaque Bâtiment Services (ABS) et M. [Y] [B], engagé en qualité de responsable commercial « grands comptes » à partir du 14 octobre 2013. Travaillant depuis son domicile, il a été mis à pied à titre conservatoire le 28 septembre 2016, à la suite d'un entretien informel, puis convoqué à un entretien préalable à un éventuel licenciement le 7 octobre 2016. L'employeur a décidé de le licencier pour faute grave, en se fondant sur des enregistrements clandestins des entretiens réalisés à l'insu du salarié pour prouver son refus de fournir le suivi de son activité commerciale. La cour d'appel d'Orléans avait déclaré ces preuves irrecevables en raison de leur obtention déloyale. La Cour de cassation, opérant un revirement de jurisprudence, a cassé cette décision estimant que, dans un procès civil, une preuve obtenue de manière déloyale peut être admise si d'une part, elle est indispensable à l'exercice du droit à la preuve, et si d'autre part, l'atteinte aux droits de l'autre partie est proportionnée au but poursuivi.

- Extraits -

« Vu l'article L. 3171-4 du code du travail :

17. Selon l'article L. 3171-4 du code du travail, en cas de litige relatif à l'existence ou au nombre d'heures de travail accomplies, l'employeur fournit au juge les éléments de nature à justifier les horaires effectivement réalisés par le salarié. Au vu de ces éléments et de ceux fournis par le salarié à l'appui de sa demande, le juge forme sa conviction après avoir ordonné, en cas de besoin, toutes les mesures d'instruction qu'il estime utiles. Si le décompte des heures de travail

accomplies par chaque salarié est assuré par un système d'enregistrement automatique, celui-ci doit être fiable et infalsifiable.

18. Il résulte de ces dispositions, qu'en cas de litige relatif à l'existence ou au nombre d'heures de travail accomplies, il appartient au salarié de présenter, à l'appui de sa demande, des éléments suffisamment précis quant aux heures non rémunérées qu'il prétend avoir accomplies afin de permettre à l'employeur, qui assure le contrôle des heures de travail effectuées, d'y répondre utilement en produisant ses propres éléments. Le juge forme sa conviction en tenant compte de l'ensemble de ces éléments au regard des exigences rappelées aux dispositions légales et réglementaires précitées. Après analyse des pièces produites par l'une et l'autre des parties, dans l'hypothèse où il retient l'existence d'heures supplémentaires, il évalue souverainement, sans être tenu de préciser le détail de son calcul, l'importance de celles-ci et fixe les créances salariales s'y rapportant.

(…)

21. En application de l'article 624 du code de procédure civile, la cassation des dispositions de l'arrêt déclarant irrecevables les éléments de preuve obtenus par l'employeur au moyen d'enregistrements clandestins et écartant en conséquence les pièces litigieuses produites par celui-ci, entraîne la cassation des chefs de dispositif disant le licenciement sans cause réelle et sérieuse, condamnant la société ABS au paiement de diverses sommes (...). »

Cass. soc., 14 février 2024, n° 22-23 .073

La chambre sociale de la Cour de cassation a rendu une décision en date du 14 février 2024 mettant en avant le fait 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 met en avant l'importance pour les juges qui se trouvent face 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 de l'indispensabilité de la preuve litigieuse et de la proportionnalité de cette dernière. Dans cette affaire, était en cause l'utilisation de preuves fournies par un système de vidéosurveillance non conforme aux exigences légales.

Faits – Le litige oppose ici la société Pharmacie mahoraise à l'une de ses anciennes salariées. En l'espèce, Madame M occupait le poste de caissière au sein de la société Pharmacie mahoraise. A la suite de plusieurs anomalies constatées dans les stocks par la dirigeante, cette dernière a alors décidé d'examiner les enregistrements de vidéosurveillance ainsi que les journaux informatiques de vente afin de suivre les produits lors de leur passage en caisse. Leur consultation ayant révélé plusieurs anomalies graves à la caisse de la salariée, Madame M. a alors été licenciée pour faute grave. Estimant avoir été victime d'un licenciement sans cause réelle et sérieuse, la salariée de la pharmacie a formé un pourvoi en cassation contre l'arrêt de la cour d'appel qui l'a déboutée de ses demandes. Selon elle, les preuves issues de la vidéosurveillance utilisées par la dirigeante étaient totalement illicites en raison du fait que le dispositif mis en place par celle-ci n'était pas conforme aux exigences légales. En l'occurrence, la question qui se posait aux juges de la Cour de cassation était de savoir si la production d'une preuve obtenue de manière illicite, par un système de vidéosurveillance non conforme aux exigences légales pouvait être recevable pour justifier un licenciement. 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

d'un salarié au respect de sa vie privée en tenant compte du caractère proportionné de l'atteinte ainsi portée à la vie personnelle au regard du but poursuivi. Elle a alors conclu que la production des données personnelles issues du système de vidéosurveillance était indispensable à l'exercice du droit à la preuve de l'employeur et proportionnée au but poursuivi à savoir le droit de veiller à la protection de ses biens par la dirigeante.

- Extraits –

« 7. La cour d'appel a d'abord relevé qu'il était démontré qu'après avoir constaté des anomalies dans les stocks, la société avait envisagé l'hypothèse de vols par des clients d'où le visionnage des enregistrements issus de la vidéo protection, ce qui avait permis d'écarter cette piste.

8. Elle a ensuite constaté, par motifs propres, que les inventaires confirmant des écarts injustifiés, la responsable de la société avait décidé de suivre les produits lors de leur passage en caisse et de croiser les séquences vidéo sur lesquelles apparaissent les ventes de la journée avec les relevés des journaux informatiques de vente, ce contrôle ayant été réalisé du 10 juin au 27 juin 2016 et, par motifs adoptés, qu'un recoupement des opérations enregistrées à la caisse de la salariée (vidéo/journal informatique) avait ainsi révélé au total dix-neuf anomalies graves en moins de deux semaines.

9. Elle a enfin retenu que le visionnage des enregistrements avait été limité dans le temps, dans un contexte de disparition de stocks, après des premières recherches restées infructueuses et avait été réalisé par la seule dirigeante de l'entreprise.

10. De ces seules constatations et énonciations, dont il résulte qu'elle a mis en balance de manière circonstanciée le droit de la salariée au respect de sa vie privée et le droit de son employeur au bon fonctionnement de l'entreprise, en tenant compte du but légitime qui était poursuivi par l'entreprise, à savoir le droit de veiller à la protection de ses biens, la cour d'appel a pu déduire que la production des données personnelles issues du système de vidéosurveillance était indispensable à l'exercice du droit à la preuve de l'employeur et proportionnée au but poursuivi, de sorte que les pièces litigieuses étaient recevables.

11. Le moyen, qui est inopérant en ses deuxième à quatrième branches, n'est donc pas fondé pour le surplus.

PAR CES MOTIFS, et sans qu'il y ait lieu de statuer sur le pourvoi incident, qui est éventuel, la Cour :

REJETTE les pourvois ; »

Cass. soc., 25 septembre 2024, n° 23-13.992 FS-B : *JurisData* n° 2024-016440 ; *JCP* E 2024, 1359, B. Bossu

Dans cet arrêt, la Cour de cassation a commencé par rappeler deux principes. Le premier relatif au respect de la vie privée du salarié prévu à l'article L.1121-1 du code du travail, et le second au sujet des principes de licéité et de loyauté quant à la production d'un moyen de preuve, prévus aux articles 6 du code civil et 9 du code de procédure civil. Sur la recevabilité de la preuve apportée par l'employeur pour justifier le licenciement pour faute grave, la cour considère que la reproduction sur une clé USB unique de seules les données strictement

professionnelles était indispensable à l'exercice du droit à la preuve de l'employeur et que l'atteinte à la vie privée de la salariée était strictement proportionnée au but poursuivi. À contrario, la Cour de cassation rejette le pourvoi de la demanderesse en considérant que c'est à bon droit que la cour d'appel a constaté une violation à l'obligation de discrétion du fait de l'impression et de la copie de documents professionnels, bien que l'ancienne salariée ait fait valoir le défaut de manquement à son obligation de discrétion en l'absence de divulgation aux tiers et de constatation du caractère confidentiel des documents copiés et imprimés.

Faits - Le litige opposait une salariée, demanderesse au pourvoi en cassation, à son ancien employeur, après que ce dernier l'ait licenciée pour faute grave en raison de la copie sur clés USB non sécurisées de données sensibles auxquelles elle n'avait pas accès, et ce sans autorisation. La Cour d'appel de Lyon dans une décision du 25 janvier 2023 l'avait déboutée de ses demandes d'allocation de dommages et intérêts et au paiement d'indemnités.

- Extraits -

« [...] 7. La cour d'appel, après avoir relevé que l'employeur faisait valoir qu'il avait agi de manière proportionnée afin d'exercer son droit à la preuve, dans le seul but de préserver la confidentialité de ses affaires, a d'abord constaté, par motifs propres et adoptés, que celui-ci démontrait qu'il existait des raisons concrètes qui justifiaient le contrôle effectué sur les clés USB, au regard du comportement de la salariée qui, selon le témoignage de deux de ses collègues, avait, courant juin et juillet 2017, travaillé sur le poste informatique d'une collègue absente et imprimé de nombreux documents qu'elle avait ensuite rangés dans un sac plastique placé soit au pied de son bureau soit dans une armoire métallique fermée.

[...] 8. Elle a, ensuite, relevé que pour établir le grief imputé à la salariée, l'employeur s'était borné à produire les données strictement professionnelles reproduites dans une clé unique (Verbatim 64 GB) après le tri opéré par l'expert qu'il avait mandaté à cet effet, en présence d'un huissier de justice, les fichiers à caractère personnel n'ayant pas été ouverts par l'expert et ayant été supprimés de la copie transmise à l'employeur, selon procès-verbal de constat en date du 11 septembre 2017.

De ces constatations et énonciations, dont il ressortait que la production du listing de fichiers tiré de l'exploitation des clés USB était indispensable à l'exercice du droit à la preuve de l'employeur et que l'atteinte à la vie privée de la salariée était strictement proportionnée au but poursuivi, la cour d'appel, qui a déduit, abstraction faite des motifs critiqués par le moyen mais qui sont surabondants, que les pièces relatives au contenu des clés USB litigieuses étaient recevables, a légalement justifié sa décision.

[...] 12. En l'état de ces constatations, la cour d'appel a pu en déduire, sans avoir à procéder à une recherche inopérante, que ces faits, nonobstant l'ancienneté de la salariée, constituaient une faute grave rendant impossible son maintien dans l'entreprise. »

CA Paris, 27 sept. 2023, n° 21/02239 : *JurisData* n° 2023-021844 ; *Comm. com. électr.* 2024, comm. 12, É.-A. Caprioli

Par cette décision, la Cour d'appel de Paris se prononce sur la validité d'un licenciement prononcé pour faute grave, au regard des obligations respectives du salarié et de l'employeur

dans la relation de travail. La Cour y réaffirme que l'employeur, s'il dispose d'une marge d'appréciation pour apprécier la gravité des faits reprochés, doit néanmoins fonder la sanction disciplinaire sur des éléments objectivement vérifiables et proportionnés. Elle souligne également l'importance du respect, par le salarié, de la charte informatique et des règles internes visant à encadrer l'usage des outils professionnels. En l'espèce, la Cour retient que la détention, sur le réseau de l'entreprise, de nombreux fichiers pornographiques accessibles à d'autres salariés constitue un manquement suffisamment grave pour justifier un départ immédiat. La portée de cet arrêt réside dans la délimitation d'un cadre protecteur pour l'employeur comme pour le salarié : tout abus (ici l'usage détourné des ressources de l'entreprise) peut conduire à un licenciement pour faute grave, à condition que les faits reprochés et leur gravité soient démontrés avec précision.

Faits – M. B., salarié depuis plusieurs années et occupant des fonctions administratives, disposait d'un accès élargi au réseau informatique de la société Dem@lone. L'employeur a découvert que de nombreux fichiers à caractère pornographique, dont certains mettant en scène M. B. lui-même dans les locaux de l'entreprise, étaient enregistrés dans un répertoire professionnel potentiellement visible par d'autres salariés. À la suite de cette découverte, l'employeur a convoqué le salarié à un entretien préalable, puis l'a licencié pour faute grave. Saisi par M. B., qui contestait tant la cause réelle et sérieuse du licenciement que la gravité de la faute, le conseil de prud'hommes a validé la faute grave, tout en accordant un rappel de prime sur chiffre d'affaires. Devant la cour d'appel, M. B. a réitéré ses demandes indemnitaires, soutenant que la conservation de fichiers personnels, fit-elle jugée inconvenante, ne saurait caractériser une faute grave. La société Dem@lone, pour sa part, contestait le versement de la prime et réclamait la confirmation de la qualification de faute grave.

- Extraits -

« (…) La Cour retient que ces faits sont fautifs eu égard au nombre et au volume des fichiers pornographiques sauvegardés sur le réseau informatique de l'entreprise, à leur accessibilité à toutes les personnes connectées au réseau de l'entreprise et à leur contenu pornographique et désadapté […] Cette faute est d'une gravité telle qu'elle imposait le départ immédiat du salarié. »

« (…) c'est en vain que M. [B] soutient que les documents se trouvaient dans un 'dossier personnel'. La structure de rangement démontrait, au contraire, une localisation dans un répertoire d'usage professionnel, auquel l'employeur pouvait légitimement accéder […] »

« (…) les agissements de M. [B] ont porté atteinte au fonctionnement normal de l'outil informatique et, partant, à l'image de la société. Ils justifient la privation des indemnités de rupture dès lors qu'ils ont rompu le lien de confiance et de loyauté inhérent à la relation de travail. »

Cass. soc., 14 février 2024 : RG n° 21-19.802 F-D : *JurisData* n° 2024-001709 ; *Comm. com. électr*. 2024, alerte 131, Cabinet Racine

Par un arrêt en date du 14 février 2024, la chambre sociale de la Cour de cassation a mis en avant l'importance du principe de limitation des finalités dans l'utilisation des données personnelles. En effet, dans cet arrêt il a été jugé que lorsque le traitement des données recueillies au moyen d'un système de géolocalisation, installé dans un véhicule conduit par le salarié d'une entreprise, avait pour seule finalité le suivi des chauffeurs routiers dans leurs

déplacements afin de localiser les marchandises sensibles, ce traitement ne pouvait en aucun cas être détourné de sa finalité première pour en satisfaire une autre sous peine de porter atteinte à la vie privée et aux libertés individuelles du salarié.

Faits - M. Y. a été engagé en tant que chauffeur au sein de la société Corsi France International Transports. À la suite de la constatation de certaines irrégularités dans son travail, l'employeur a utilisé les données issues du système de géolocalisation installé sur le véhicule de ce dernier pour justifier son licenciement pour faute grave. Contestant ce licenciement, le chauffeur a saisi la juridiction prud'homale. Dans cet arrêt, deux questions se présentaient à la Cour de cassation. En effet, dans un premier temps le salarié revendiquait le bénéfice de la prime de treizième mois qui ne lui aurait pas été versée par son employeur. La société quant à elle revendiquait le fait que cette prime avait été valablement supprimée quelques années plus tôt. Les juges de la Cour de cassation ont finalement approuvé la cour d'appel et estimé que la suppression de cette prime était opposable au salarié de sorte que celui-ci ne pouvait se prévaloir d'aucun droit au maintien de la prime litigieuse. Dans un second temps, le salarié a reproché à la société d'avoir utilisé un système de géolocalisation qui constituait, selon lui, une restriction au droit des personnes et aux libertés individuelles et collectives et qui n'était pas justifié par la nature des tâches à accomplir ni proportionné au but recherché. En effet, ce dernier a invoqué un détournement par l'employeur de la finalité du système qui avait initialement pour but le suivi des chauffeurs routiers dans leurs déplacements, et qui a finalement été utilisé pour contrôler la durée de travail, surveiller le salarié, et contrôler en permanence sa localisation en couvrant les pauses et les périodes de repos. Par cet arrêt, il a alors été question pour les juges de se demander si le système de géolocalisation utilisé par la société était licite et si les données recueillies par ce système pouvaient servir de fondement afin de justifier le licenciement pour faute du chauffeur. Les juges de la Cour de cassation ici n'approuve pas la cour d'appel et estime que le traitement des données personnelles avait été détourné de sa finalité et avait porté atteinte à la vie personnelle du salarié de sorte que les preuves tirées de la géolocalisation étaient illicites et ne pouvaient donc pas fonder le licenciement pour faute du salarié.

- Extraits -

« 9. Pour débouter le salarié de ses demandes au titre du licenciement sans cause réelle et sérieuse, après avoir rejeté celles formées au titre de l'illicéité des moyens de contrôle, l'arrêt retient que le système de géolocalisation utilisé par la société était licite comme respectant les exigences légales dès lors que, s'agissant de conducteurs routiers, salariés itinérants qui ne disposaient pas d'une autonomie dans l'organisation de leur travail, l'employeur était légitime à recourir à ce système de géolocalisation afin de contrôler la durée du travail, ce qui ne pouvait être effectué par d'autres moyens de contrôle et que le salarié ne pouvait invoquer un détournement de la finalité du système mis en place qui visait à suivre l'ensemble des chauffeurs routiers dans leurs déplacements, la sanction n'étant pas un objectif en soi, mais la conséquence d'un manquement du salarié à ses obligations contractuelles.

10. Il énonce ensuite que les erreurs de manipulation reprochées au salarié consistant à enregistrer en temps de travail ou en disponibilité des heures de repos, ou à gonfler artificiellement la durée de certaines tâches, sont établies, au vu des pièces produites.

11. En statuant ainsi, alors qu'elle avait constaté que les données recueillies au moyen du système de géolocalisation installé dans le véhicule conduit par le salarié et qui avait pour seule finalité déclarée auprès de la Commission nationale informatique et libertés et présentée au comité d'entreprise et soumise à l'information des salariés, le suivi des chauffeurs routiers dans leurs déplacements afin de localiser les marchandises sensibles et de permettre un meilleur

choix en exploitation, avaient été utilisées par l'employeur pour, d'une part, contrôler la durée du travail quand le véhicule était pourtant équipé d'un chronotachygraphe et, d'autre part, surveiller le salarié et contrôler en permanence sa localisation en couvrant les pauses et les périodes de repos, entrant alors dans la sphère de sa vie personnelle, ce dont il résultait que l'employeur avait détourné de sa finalité le traitement des données personnelles issues de la géolocalisation et avait porté atteinte à la vie personnelle du salarié, en sorte que ce moyen de preuve tiré de la géolocalisation était illicite, la cour d'appel a violé le texte susvisé.

[…]

PAR CES MOTIFS, et sans qu'il y ait lieu de statuer sur les autres griefs, la Cour :

CASSE ET ANNULE, mais seulement en ce qu'il déboute M. [F] de ses demandes au titre du licenciement sans cause réelle et sérieuse et en dommages-intérêts pour rupture abusive ainsi qu'en ce qu'il statue sur les dépens et l'application de l'article 700 du code de procédure civile, l'arrêt rendu le 20 mai 2021, entre les parties, par la cour d'appel de Dijon ; ».

CEDH, 20 févr. 2024, n° 48340/20, *aff. Dede c/ Türkiye : Comm. com. électr*. 2024, alerte 126, Cabinet Racine

Par cette décision, la Cour européenne des droits de l'homme (CEDH) se prononce sur le respect par la Türkiye de ses obligations conventionnelles, notamment au regard du droit à la liberté d'expression consacré par l'article 10 de la Convention européenne des droits de l'homme (CEDH). La Cour y réaffirme que les États disposent d'une marge d'appréciation pour encadrer l'exercice de la liberté d'expression, surtout s'agissant de questions liées à la sécurité nationale ou à l'ordre public. Toutefois, elle souligne aussi que toute restriction doit être prévue par la loi, poursuivre un but légitime et, surtout, respecter le principe de proportionnalité. En l'espèce, la Cour condamne les mesures jugées excessives imposées au requérant, en rappelant qu'elles ne peuvent être justifiées par une simple invocation de la préservation de l'ordre public. La portée de cet arrêt réside dans la délimitation d'un cadre protecteur destiné à éviter l'abus d'autorité pouvant conduire à des violations graves et systématiques du droit à la liberté d'expression.

Faits - Monsieur Dede, journaliste indépendant, avait publié plusieurs articles critiques à l'encontre des autorités turques, abordant notamment des sujets sensibles liés à la politique sécuritaire du pays. À la suite de la parution de ces articles, il avait fait l'objet de poursuites pour « atteinte à la sûreté de l'État » et « propagande terroriste », infractions prévues par le Code pénal turc. Placé en détention provisoire durant plusieurs mois, il a vu ses requêtes de remise en liberté rejetées à de multiples reprises. Dans le cadre de la procédure interne, les juridictions turques ont estimé que ses écrits et déclarations participaient à saper l'autorité de l'État. Contestant la légitimité et la proportionnalité des mesures dont il avait été l'objet, Monsieur Dede a saisi la Cour de Strasbourg, alléguant une violation de son droit à la liberté d'expression (article 10) et de son droit à la liberté et à la sûreté (article 5).

- Extraits –

« (…) l'article 10 de la Convention exige que toute restriction à la liberté d'expression poursuive un but légitime et soit strictement nécessaire dans une société démocratique… »

« (…) les juridictions internes doivent s'assurer que la qualification pénale retenue ne soit pas détournée de sa finalité légitime en vue d'étouffer la critique ou le débat public, éléments essentiels de la vie démocratique… »

« (…) la Cour relève un manque de proportionnalité manifeste entre la mesure de détention provisoire prolongée imposée au requérant et la gravité alléguée des faits, entraînant une violation de l'article 5 combiné avec l'article 10 de la Convention. »

Cass. soc., 14 février 2024, n°22-18.014 F-D : *JurisData* n° 2024-001741 ; *Comm. com. électr*. 2024, comm. 36, A. Lepage

La chambre sociale de la Cour de cassation, dans un arrêt en date du 14 février 2024, a eu l'occasion de réaffirmer le principe selon lequel le droit à l'image est une composante essentielle des droits de la personnalité. En fondant sa décision sur l'article 9 du code civil, la Cour rappelle notamment que la captation, la conservation, la reproduction ou encore l'utilisation de l'image d'une personne, y compris d'un salarié par son employeur, sans son consentement explicite constitue une atteinte ouvrant droit à réparation. Les juges retiennent ici que la seule constatation de l'atteinte au droit à l'image ouvre droit à réparation. Ainsi, l'arrêt met en avant l'importance pour les employeurs d'obtenir le consentement préalable de leurs salariés avant toute utilisation de leur image.

Faits – Le litige oppose ici la société American Express Carte à l'un de ses anciens salariés. En l'espèce, Monsieur E occupait le poste de conseiller art de vivre en charge de fonctions de conciergerie au sein de la société American Express Carte. Dans le cadre de ses activités, la société a diffusé en 2012 et 2015, auprès de ses clients, des plaquettes de présentation des concierges comportant une photographie du visage et une du buste de chacun d'entre eux. Après avoir été licencié par lettre du 1er mars 2017, le salarié a alors saisi la juridiction prud'homale de diverses demandes à titre salarial et indemnitaire, notamment au titre de la violation de son droit à l'image. Le salarié soutient n'avoir jamais donné son consentement pour la diffusion de son image dans ces plaquettes. Estimant avoir été victime de la violation de son droit à l'image, le salarié de la société American Express Carte - France a formé un pourvoi en cassation contre l'arrêt rendu par la cour d'appel de Versailles le déboutant de ses demandes estimant qu'il ne produisait pas de preuves suffisantes et notamment le document critiqué, pour établir l'atteinte revendiquée. Dans cette décision, les juges de la Cour de cassation ont dû se demander si la simple reconnaissance par l'employeur de l'utilisation et la diffusion de l'image de son salarié suffisait à caractériser l'atteinte au droit à l'image, sans qu'il ne soit nécessaire pour le salarié de produire le document critiqué. Les juges de la Cour de cassation, pour casser et annuler l'arrêt de la cour d'appel, retiennent ici que l'employeur ne contestait pas avoir utilisé et diffusé l'image du salarié pour réaliser les plaquettes et que le salarié quant à lui affirmait n'avoir jamais donné son accord pour cette utilisation.

- Extraits -

« Vu l'article 9 du code civil :

5. Il résulte de ce texte que le droit dont la personne dispose sur son image porte sur sa captation, sa conservation, sa reproduction et son utilisation, et que la seule constatation d'une atteinte ouvre droit à réparation.

6. Pour débouter le salarié de ses demandes de dommages-intérêts au titre de son droit à l'image, l'arrêt retient d'abord qu'il reproche à la société d'avoir utilisé son nom de famille et son image à l'occasion de deux campagnes publicitaires en 2012 et 2015. Il indique ensuite que la société soutient principalement qu'il ne s'agissait pas d'une campagne publicitaire mais d'une simple plaquette de présentation des concierges, adressée aux clients, réalisée à partir des photographies individuelles du visage et du buste des concierges ainsi que de photographies collectives. Il retient enfin que le salarié qui ne produit aucune pièce utile à l'appui de sa prétention, notamment pas le document critiqué, ne met pas la cour en mesure d'apprécier la réalité de l'atteinte invoquée.

7. En statuant ainsi, alors que l'employeur ne contestait pas avoir utilisé l'image du salarié pour réaliser une plaquette adressée aux clients, que le salarié faisait valoir dans ses écritures qu'il n'avait pas donné son accord à cette utilisation et que la seule constatation de l'atteinte au droit à l'image ouvre droit à réparation, la cour d'appel a violé le texte susvisé. »

Rédaction assurée par

Adrien DOUAY
Margaux DAMBRINE
Océane GONZALEZ
Margot AMBROSINO
Renée FAUST
Yasmina AL ABAD
Zoé TASSIN DUPRÉ
Emma BAUDIN