Badge électronique : affaire Galeries Lafayette

Contrôle des heures de travail du salarié

Il convient de toujours informer les salariés de leur droit d'accès aux données nominatives les concernant, y compris de leur droit à communication des relevés de présences établis par pointeuse électronique. Le licenciement d'une vendeuse des Galeries Lafayette a été jugé dépourvu de cause réelle et sérieuse. La salariée avait été licenciée pour tricherie sur ses heures de travail (faute grave), sur la base des relevés de pointage présentés par son employeur qui ne correspondaient pas aux relevés et aux heures effectivement réalisées.

Notion de faute grave

La faute grave résulte d'un fait ou d'un ensemble de faits imputables au salarié qui constitue une violation des obligations découlant du contrat de travail d'une importance telle qu'elle rend impossible le maintien du salarié dans l'entreprise pendant la durée du préavis sans risque de compromettre les intérêts légitimes de l'employeur. La charge de la preuve de la gravité de la faute privative des indemnités de préavis et de licenciement incombe à l'employeur.

Mode de preuve écarté

La salariée a fait valoir avec succès que les garanties prévues par la loi en ce qui concerne les systèmes de pointage automatisés n'étaient pas respectées et que les relevés de la

badgeuse des Galeries Lafayette ne lui étaient donc pas opposables. Elle visait le défaut de déclaration à la CNIL, le défaut de fiabilité et d'infalsifiabilité du système d'enregistrement en application de l'article L3171-4 du code du travail, le défaut d'accès aux documents de décompte quotidien ou hebdomadaire par les salariés et les délégués du personnel, le défaut d'information des délégués du personnel à la mise en place du système de pointage et le défaut d'information en direction des salariés.

L'employeur justifiait qu'un correspondant informatique et liberté (CIL) avait été régulièrement désigné par les Galeries Lafayette, toutefois l'employeur ne démontrait pas qu'il avait informé sa salariée, par une note de service, un règlement intérieur ou tout autre document, de ses droits d'accès aux données à caractère personnel la concernant et du nom du responsable de traitement du système automatique au sein des Galeries Lafayette, le règlement intérieur de celles-ci ne comportant aucune information en ce sens. En conséquence les relevés de pointage visés dans la lettre de licenciement n'étaient pas opposables à la salariée.

Droit d'accès du salarié sur ses données nominatives

Aux termes de l'article D3171-14 du code du travail le droit d'accès aux informations nominatives prévu à l'article 39 de la loi 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés est applicable aux documents comptabilisant la durée de travail des salariés. L'article 39 de cette loi dispose notamment que toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir : 1° La confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de ce traitement ; 2° Des informations relatives aux finalités du traitement, aux

catégories de données à caractère personnel traitées et aux destinataires ou aux catégories de destinataires auxquels les données sont communiquées ; 3° Le cas échéant, des informations relatives aux transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne ; 4° La communication, sous une forme accessible, des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci ; 5° Les informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé… Une copie des données à caractère personnel est délivrée à l'intéressé à sa demande.

Télécharger la Décision

Télécharger

Contrat sur cette thématique

Vous disposez d'un modèle de document juridique sur cette thématique ? Besoin d'un modèle ? Complétez vos revenus en le vendant sur Uplex.fr, la 1ère plateforme de France en modèles de contrats professionnels

Vous avez une expertise dans ce domaine ?

Référencez votre profil sur Lexsider.com, la 1ère plateforme de mise en relation gratuite Avocats / Clients

Poser une Question

Posez une Question Juridique sur cette thématique, la rédaction ou un abonné vous apportera une réponse en moins de 48h.

E-réputation | Surveillance de marques

Surveillez et analysez la réputation d'une **Marque** (la vôtre ou celle d'un concurrent), d'une Personne publique (homme

politique, acteur, sportif …) sur tous les réseaux sociaux (Twitter, Facebook …). Testez gratuitement notre plateforme de Surveillance de Marque et de *Réputation numérique*.

Paramétrer une Alerte

Paramétrez une alerte de Jurisprudence sur ce thème pour être informé par email lorsqu'une décision est rendue sur ce thème

---

Divulgation de secret d'affaire sur Twitter

Free c/ NPA Conseil

La saisie de documents chez NPA Conseil sur l'initiative de la société Free a été déclarée recevable par les juges, la procédure suivra donc son cours. A l'origine des faits, la découverte par la société Free de Tweets présentés comme ceux de Didier Lombard (ex-PDG du groupe Orange) divulguant diverses informations couvertes par le secret des affaires et relatives à l'existence de négociations entre la société Free et la société groupe Canal+ portant sur une future offre commerciale et des détails de ladite offre.

Action en référé

La société Free a entrepris de connaître l'identité de la personne tenant ce compte Twitter ainsi que la source de ses informations. Elle a alors découvert que le compte de l'ex-PDG du groupe Orange avait été usurpé. Arguant que plusieurs éléments techniques d'identification de l'auteur, aboutissaient à la société NPA Conseil, la société Free a par

une requête sollicité et obtenu par ordonnance (article 145 du code de procédure civile), la désignation d'un huissier de justice aux fins de saisie de fichiers informatiques au siège de la société.

Saisie confirmée

Ont ainsi été saisis et mis sous séquestre plusieurs éléments susceptibles d'être en lien avec les tweets litigieux : traces horodatées de navigation d'un salarié de NPA Conseil, du portable du gérant de la société, traces de connexion Tweeter, messages textes horodatés …

Précisions de procédure

L'article 145 du code de procédure civile dispose que s'il existe un motif légitime de conserver ou d'établir avant tout procès la preuve de faits dont pourrait dépendre la solution d'un litige, les mesures d'instruction légalement admissibles peuvent être ordonnées à la demande de tout intéressé, sur requête ou en référé. Lorsqu'il statue en référé sur le fondement de ce texte, le juge n'est pas soumis aux conditions imposées par l'article 808 du code de procédure civile : il n'a notamment pas à rechercher s'il y a urgence et l'existence de contestations sérieuses ne constitue pas un obstacle à la mise en oeuvre de la mesure sollicitée.

L'article 145 a institué une procédure de recueil de preuves permettant au juge d'ordonner une mesure d'instruction légalement admissible sur requête ou en référé, s'il existe un motif légitime de conserver ou d'établir avant tout procès la preuve de faits dont pourrait dépendre la solution d'un litige.

Le secret des affaires ne constitue pas en lui-même un obstacle à l'application de ces dispositions, dès lors que le juge constate que les mesures qu'il ordonne procèdent d'un motif légitime et sont nécessaires à la protection des droits de la partie qui les a sollicitées.

En application de l'article 493 du code de procédure civile, le requérant peut saisir le juge d'une requête dans le cas où il est fondé à ne pas appeler la partie adverse, c'est-à-dire s'il existe des circonstances justifiant qu'il soit dérogé au principe de la contradiction.

Lorsque la loi permet ou la nécessité commande qu'une mesure soit ordonnée à l'insu d'une partie, celle-ci dispose d'un recours approprié contre la décision qui lui fait grief (article 17 du code de procédure civile). Le requis dispose alors d'un recours approprié, institué par l'article 496 alinéa 2 qui permet à tout intéressé, s'il est fait droit à la requête, d'en référer au juge qui a rendu l'ordonnance.

Lorsqu' un mandataire judiciaire, désigné sur requête sur le fondement de l'article 145 du code de procédure civile, appréhende des documents qu'il a placés sous séquestre, ainsi que le juge l'y a invité, une pratique s'est développée consistant pour le requérant à saisir le juge statuant en référé d'une demande de levée du séquestre. La procédure de référé est une procédure contradictoire et comme telle soumise aux exigences du procès équitable. Pour autant, la demande de levée de séquestre ne tend à obtenir du juge qu'une mesure d'instruction complémentaire, destinée à assurer l'efficacité de la mesure ordonnée sur requête. La demande de levée de la mesure de séquestre s'inscrit dans le prolongement de la mesure, laquelle, par hypothèse, n'a été autorisée que parce qu'elle était légalement admissible, notamment en ce qu'elle serait susceptible de porter atteinte au secret des affaires. Le caractère contradictoire de la procédure de levée de séquestre permet au requérant de s'assurer que celle-ci est bien effectuée sous le contrôle du juge. Elle ne saurait avoir

pour objet ou pour effet d'autoriser le requérant ou son représentant à se faire remettre ou même à prendre connaissance de documents excédant le cadre de l'ordonnance sur requête et susceptibles d'affecter les droits légitimes du requis.

Considérée dans son ensemble, la mesure probatoire et son exécution garantissent ainsi en l'espèce le droit à un procès équitable, par la possibilité offerte au requis d'engager la procédure de rétractation et de débattre contradictoirement du périmètre des mesures autorisées puis par le droit donné au requérant de s'assurer d'un contrôle effectif par le juge de la bonne exécution de la mesure qu'il a décidée à sa demande et enfin par l'existence d'un recours au bénéfice de l'ensemble des parties à l'encontre de la décision rendue par le juge saisi d'une demande de levée du séquestre. Une fois le périmètre de la mesure arrêté, la procédure de levée du séquestre opérée sous le contrôle du magistrat n'est qu'une modalité de l'exécution de sa décision, qui ne porte donc pas atteinte aux principes directeurs du procès.

Au cas présent, le président du tribunal de commerce de Nanterre, juge de la rétractation, saisi contradictoirement, a rejeté la demande de rétractation de l'ordonnance rendue sur requête, au visa de l'article 145 du code de procédure civile. Le juge de la rétractation a ainsi expressément retenu que la mesure sollicitée reposait sur un motif légitime et que celle ordonnée sur requête était proportionnée, justifiée et limitée, conformément aux exigences de l'article 145 du code de procédure civile.

Télécharger la Décision

Télécharger

Contrat sur cette thématique

Vous disposez d'un modèle de document juridique sur cette

thématique ? Besoin d'un modèle ? Complétez vos revenus en le vendant sur Uplex.fr, la 1ère plateforme de France en modèles de contrats professionnels

Vous avez une expertise dans ce domaine ?

Référencez votre profil sur Lexsider.com, la 1ère plateforme de mise en relation gratuite Avocats / Clients

Poser une Question

Posez une Question Juridique sur cette thématique, la rédaction ou un abonné vous apportera une réponse en moins de 48h.

E-réputation | Surveillance de marques

Surveillez et analysez la réputation d'une **Marque** (la vôtre ou celle d'un concurrent), d'une Personne publique (homme politique, acteur, sportif …) sur tous les réseaux sociaux (Twitter, Facebook …). Testez gratuitement notre plateforme de Surveillance de Marque et de *Réputation numérique*.

Paramétrer une Alerte

Paramétrez une alerte de Jurisprudence sur ce thème pour être informé par email lorsqu'une décision est rendue sur ce thème

---

Vendeur régulier en ligne : persistance du statut de consommateur

Professionnel ou consommateur ?

Confirmation de la CJUE : une personne qui publie sur un site

Internet de nombreuses annonces de ventes, n’a pas automatiquement la qualité de « professionnel ». Cette activité peut être considérée comme une « pratique commerciale » si la personne agit à des fins qui entrent dans le cadre de son activité commerciale, industrielle, artisanale ou libérale. Un consommateur a acheté une montre d’occasion sur une plate-forme de vente en ligne. Après avoir constaté que la montre ne présentait pas les propriétés indiquées dans l’annonce de vente, le consommateur a exprimé au vendeur sa volonté de résilier le contrat. Le vendeur a refusé tout remboursement.

Informations légales sur le vendeur

Le consommateur a déposé une plainte auprès de la Commission bulgare de protection des consommateurs (CPC) qui a infligé au vendeur plusieurs amendes administratives sur le fondement d’une loi nationale sur la protection des consommateurs. Selon la CPC, le vendeur aurait omis d’indiquer dans chacune desdites annonces le nom, l’adresse postale et l’adresse électronique du professionnel, le prix total du produit mis en vente, tous droits et taxes compris, les conditions de paiement, de livraison et d’exécution, le droit du consommateur de se rétracter du contrat de vente à distance, les conditions, le délai et les modalités d’exercice de ce droit ainsi que le rappel de l’existence d’une garantie légale de conformité des produits vendus. Bref, toutes les mentions légales dont est débiteur un professionnel.

Critères de la qualification

Saisie de l’affaire, la CJUE a indiqué que, pour être qualifiée de « professionnel », au sens de la Directive 2005/29/CE du 11 mai 2005 relative aux pratiques commerciales

déloyales, il est nécessaire que la personne concernée agisse à des « fins qui entrent dans le cadre de son activité commerciale, industrielle, artisanale ou libérale » ou au nom ou pour le compte d'un professionnel. Le sens et la portée de la notion de « professionnel » doivent être déterminés par rapport à la notion de « consommateur », laquelle désigne tout particulier non engagé dans des activités commerciales ou professionnelles.

Il appartient à la juridiction nationale de juger, au cas par cas, sur la base de tous les éléments de fait dont elle dispose si une personne physique a agi à des fins qui entrent dans le cadre de son activité commerciale, industrielle, artisanale ou libérale en vérifiant, notamment, si la vente a été réalisée de manière organisée, si elle a un caractère de régularité ou un but lucratif, si l'offre est concentrée sur un nombre restreint de produits, et d'examiner le statut juridique et les compétences techniques du vendeur. En outre, pour considérer que l'activité en cause constitue une « pratique commerciale », la juridiction nationale doit vérifier que cette activité, d'une part, émane d'un « professionnel » et, d'autre part, constitue une action, omission, conduite, démarche ou communication commerciale « en relation directe avec la promotion, la vente ou la fourniture d'un produit aux consommateurs ». Dans ces circonstances, une personne physique, qui publie sur un site Internet, simultanément, un certain nombre d'annonces offrant à la vente des biens neufs et d'occasion ne doit être qualifiée de « professionnel » et une telle activité ne constitue une « pratique commerciale » que lorsque cette personne agit à des fins qui entrent dans le cadre de son activité commerciale, industrielle, artisanale ou libérale.

Télécharger la Décision

Télécharger

Vendre un Contrat sur cette thématique

Vous disposez d'un modèle de document juridique sur cette thématique ? Complétez vos revenus en le vendant sur Uplex.fr, la 1ère plateforme de France en modèles de contrats professionnels

Poser une Question

Posez une Question Juridique sur cette thématique, la rédaction ou un abonné vous apportera une réponse en moins de 48h.

E-réputation | Surveillance de marques

Surveillez et analysez la réputation d'une **Marque** (la vôtre ou celle d'un concurrent), d'une Personne publique (homme politique, acteur, sportif …) sur tous les réseaux sociaux (Twitter, Facebook …). Testez gratuitement notre plateforme de Surveillance de Marque et de *Réputation numérique*.

Paramétrer une Alerte

Paramétrez une alerte de Jurisprudence sur ce thème pour être informé par email lorsqu'une décision est rendue sur ce thème

---

Carte SIM à services préinstallés : pratique sanctionnable

Pratique commerciale agressive déloyale

Après les contentieux sur les logiciels préinstallés sur

ordinateur, la CJUE a qualifié la mise sur le marché de cartes SIM contenant des services payants préinstallés et préalablement activés, de pratique commerciale agressive déloyale lorsque les consommateurs n'en sont pas informés préalablement informés. Ce procédé commercial constitue notamment une fourniture non demandée qui peut être sanctionnée par une autorité nationale.

La CJUE a rappelé que la demande d'un service doit consister en un choix libre de la part du consommateur. Or, lorsque le consommateur n'a été informé ni des coûts des services ni même de leur préinstallation et de leur activation préalable sur la carte SIM qu'il a achetée, il ne saurait être considéré que celui-ci a librement choisi la fourniture de tels services. À cet égard, il est indifférent que l'utilisation des services ait pu, dans certains cas, nécessiter une action consciente de la part du consommateur. De même, il est indifférent que le consommateur ait eu la possibilité de faire désactiver ou de désactiver lui-même ces services, dès lors qu'il n'avait pas été préalablement informé de leur existence.

Affaire Vodafone Italia

En 2012, l'autorité italienne garante de la concurrence et du marché, AGCM a infligé des amendes aux sociétés Wind Tre et SIM pour avoir commercialisé des cartes SIM sur lesquelles étaient préinstallés et préalablement activés des services de navigation sur Internet et de messagerie vocale, dont les frais étaient facturés à l'utilisateur dans le cas où ce dernier ne demandait pas expressément leur désactivation. L'AGCM reprochait aux deux sociétés de ne pas avoir préalablement informé de manière adéquate les consommateurs du fait que ces services étaient préinstallés et préalablement activés et qu'ils étaient payants. Le service de navigation sur Internet pouvait même conduire à des connexions effectuées

à l'insu de l'utilisateur, notamment par des applications dites « always on ». Saisi par Wind Tre et Vodafone Italia, les juges italiens ont annulé les décisions de l'AGCM en déclarant que de telles sanctions relevaient de la compétence de l'autorité italienne des communications électroniques.

Compétence des autorités de concurrence

Sur le terrain de la compétence à prononcer des sanctions contre ce type de pratiques, les juges européens ont considéré qu'il n'existait pas de conflit entre la directive sur les pratiques commerciale déloyales et la directive « service universel » en ce qui concerne les droits des utilisateurs. En effet, cette dernière impose au prestataire de services de communications électroniques de fournir certaines informations dans le contrat, alors que la première régit des aspects particuliers des pratiques commerciales déloyales, telles que la « fourniture non demandée ». Le droit de l'Union ne s'oppose donc pas à une réglementation nationale en vertu de laquelle une « fourniture non demandée » doit être appréciée au regard de la directive sur les pratiques commerciales déloyales, avec la conséquence que, selon cette réglementation, l'ARN au sens de la directive « cadre » n'est pas compétente pour sanctionner un tel comportement.

professionnels

Poser une Question

Posez une Question Juridique sur cette thématique, la rédaction ou un abonné vous apportera une réponse en moins de 48h.

E-réputation | Surveillance de marques

Surveillez et analysez la réputation d'une **Marque** (la vôtre ou celle d'un concurrent), d'une Personne publique (homme politique, acteur, sportif …) sur tous les réseaux sociaux (Twitter, Facebook …). Testez gratuitement notre plateforme de Surveillance de Marque et de *Réputation numérique*.

Paramétrer une Alerte

Paramétrez une alerte de Jurisprudence sur ce thème pour être informé par email lorsqu'une décision est rendue sur ce thème

---

Achat de téléphone mobile volé

Autorisation du juge

L'identification des personnes ayant acquis un téléphone mobile volé pourrait être le futur moyen de lutter contre le vol. L'identification de la carte SIM utilisée pour passer des appels depuis un téléphone mobile volé sont des données personnelles dont la transmission aux officiers de police judiciaire est soumise à une autorisation du juge. La CJUE s'est prononcée sur le degré de gravité d'une infraction nécessaire pour permettre un accès à ces données : les

infractions pénales qui ne sont pas d'une particulière gravité (comme le vol) peuvent justifier un accès aux données à caractère personnel conservées par des fournisseurs de services de communications électroniques dès lors que cet accès ne porte pas une atteinte grave à la vie privée.

Conditions de la transmission des données de l'appelant

Dans le cadre de l'enquête sur un vol avec violences d'un portefeuille et d'un téléphone mobile, la police judiciaire espagnole a demandé au juge d'instruction responsable de l'affaire de lui accorder l'accès aux données d'identification des utilisateurs des numéros de téléphone activés depuis le téléphone volé durant une période de douze jours à compter de la date du vol. Le juge d'instruction a rejeté cette demande au motif, notamment, que les faits à l'origine de l'enquête pénale n'auraient pas été constitutifs d'une infraction « grave » – c'est-à-dire, selon le droit espagnol, une infraction sanctionnée d'une peine de prison supérieure à cinq ans –, l'accès aux données d'identification n'étant en effet possible que pour ce type d'infractions. Le Ministerio Fiscal (ministère public espagnol) a interjeté appel de cette décision qui a soulevé une question préjudicielle.

La CJUE a rappelé que l'accès aux données visant à l'identification des titulaires des cartes SIM activées avec un téléphone mobile volé, telles que les nom, prénom et, le cas échéant, adresse de ces titulaires, constitue une ingérence dans les droits fondamentaux de ces derniers, consacrés dans la Charte européenne. Toutefois, cette ingérence ne présente pas une gravité telle que cet accès devrait être limité, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, à la lutte

contre la criminalité grave. L'accès des autorités publiques à des données à caractère personnel conservées par les fournisseurs de services de communications électroniques serait possible sans qu'il importe que les informations relatives à la vie privée concernées présentent ou non un caractère sensible ou que les intéressés aient ou non subi d'éventuels inconvénients en raison de ladite ingérence.

L'infraction pénale suffit

S'agissant de l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales, la directive 95/46/CE du 24 octobre 1995 sur la protection des données ne limite pas cet objectif à la lutte contre les seules infractions graves, mais vise les « infractions pénales » en général. Par sa jurisprudence Tele2 Sverige et Watson e.a., C 203/15 et C 698/15 (arrêt du 21 décembre 2016), la CJUE avait jugé que seule la lutte contre la criminalité grave est susceptible de justifier un accès des autorités publiques à des données à caractère personnel conservées par les fournisseurs de services de communications qui, prises dans leur ensemble, permettent de tirer des conclusions précises concernant la vie privée des personnes dont les données sont concernées. Cette interprétation était toutefois motivée par le fait que l'objectif poursuivi par une réglementation régissant cet accès doit être en relation avec la gravité de l'ingérence dans les droits fondamentaux en cause que cette opération entraîne. En effet, conformément au principe de proportionnalité, une ingérence grave ne peut être justifiée dans ce domaine que par un objectif de lutte contre la criminalité devant également être qualifiée de « grave ». En revanche, lorsque l'ingérence n'est pas grave, ledit accès est susceptible d'être justifié par un objectif de prévention, de recherche, de détection et de poursuite d'« infractions pénales » en général.

La Cour considère donc que l'accès aux seules données visées par la demande en cause ne saurait être qualifié d'ingérence « grave » dans les droits fondamentaux des personnes dont les données sont concernées, puisque ces données ne permettent pas de tirer de conclusions précises concernant leur vie privée. La Cour en conclut que l'ingérence que comporterait un accès à de telles données est donc susceptible d'être justifiée par l'objectif de prévention, de recherche, de détection et de poursuite d'« infractions pénales » en général, sans qu'il soit nécessaire que ces infractions soient qualifiées de « graves ».

Télécharger la Décision

Télécharger

Vendre un Contrat sur cette thématique

Vous disposez d'un modèle de document juridique sur cette thématique ? Complétez vos revenus en le vendant sur Uplex.fr, la 1ère plateforme de France en modèles de contrats professionnels

Poser une Question

Posez une Question Juridique sur cette thématique, la rédaction ou un abonné vous apportera une réponse en moins de 48h.

E-réputation | Surveillance de marques

Surveillez et analysez la réputation d'une **Marque** (la vôtre ou celle d'un concurrent), d'une Personne publique (homme politique, acteur, sportif …) sur tous les réseaux sociaux (Twitter, Facebook …). Testez gratuitement notre plateforme de Surveillance de Marque et de *Réputation numérique*.

Paramétrer une Alerte

Paramétrez une alerte de Jurisprudence sur ce thème pour être informé par email lorsqu'une décision est rendue sur ce thème

Emails en entreprise : connivences injurieuses entre salariés

Injurier des collègues à leur insu

Un employeur est en droit de sanctionner un salarié (jusqu'au licenciement pour faute) lorsqu'il est établi que celui-ci injurie régulièrement sa direction ou ses collègues à leur insu. En l'espèce, l'employeur avait récupéré la messagerie professionnelle d'une ancienne salariée dans laquelle a été retrouvée de nombreux emails injurieux émis par une collègue toujours en poste.

Recevabilité des emails échangés

A noter que les emails en cause n'étaient pas identifiés comme personnels. A titre d'exemple, parmi les divers courriels litigieux, figuraient un email intitulé « Quelle pute » où la responsable de la salariée était insultée ou un email traitant de « connard » le directeur général délégué qui avait donné un conseil jugé inapproprié par la salariée. Certains des échanges contenaient également des images érotiques tournant en dérision certains collègues. Enfin, sur une période de trois mois consécutifs, plus de 1000 courriels personnels avaient été envoyés depuis la messagerie professionnelle de la salariée.

Licenciement fondé

Parmi les courriels envoyés dans le cadre professionnel, les juges ont retenu de très nombreux propos à caractère injurieux et dénigrants visant des salariés précis de la société (« qu'est-ce qu'il est con » ; « t'as pas vu un gros malabar rose passer » ; « je me suis barbouillée de citron et d'ail ce matin pour être certaine de repousser notre suceuse de sang aux cheveux gras » ; « ça se bouffe entre eux les cochons » ; « ils me donnent tous la gerbe » …). Aucun des courriels émanant de l'adresse électronique professionnelle de la salariée ne comportait de mention « personnel » et ceux-ci ont été envoyés pendant les heures de travail à une fréquence quotidienne élevée sur une période de temps importante. Ces faits, qui se sont reproduits à une fréquence quotidienne avec l'envoi de nombreux messages journaliers sur une période de temps significativement longue, caractérisaient bien un usage abusif de la messagerie professionnelle. Au regard du trouble important créé par l'affaire parmi les salariés de la société et au regard de l'atteinte à la dignité de plusieurs salariés aisément identifiables, la rupture immédiate du contrat de travail de la salariée était justifiée. Le licenciement fondé sur une faute grave a été confirmé.

Notion de faute grave

Il résulte des articles L.1234-1 et L.1234-9 du code du travail que lorsque le licenciement est motivé par une faute grave, le salarié n'a droit ni à un préavis ni à une indemnité de licenciement. La faute grave est celle qui résulte d'un fait ou d'un ensemble de faits imputables au salarié qui constituent une violation des obligations résultant du contrat de travail ou des relations de travail d'une importance telle qu'elle rend impossible la poursuite de l'exécution du contrat de travail entre les parties et rend nécessaire le départ immédiat du salarié de l'entreprise sans indemnités.

L’employeur qui invoque une faute grave doit en rapporter la preuve alors même que l’administration de la preuve en ce qui concerne le caractère réel et sérieux des motifs du licenciement n’incombe pas spécialement à l’une ou l’autre des parties, l’employeur devant toutefois fonder le licenciement sur des faits précis et matériellement vérifiables.

Télécharger la Décision

Télécharger

Vendre un Contrat sur cette thématique

Vous disposez d’un modèle de document juridique sur cette thématique ? Complétez vos revenus en le vendant sur Uplex.fr, la 1ère plateforme de France en modèles de contrats professionnels

Poser une Question

Posez une Question Juridique sur cette thématique, la rédaction ou un abonné vous apportera une réponse en moins de 48h.

E-réputation | Surveillance de marques

Surveillez et analysez la réputation d’une **Marque** (la vôtre ou celle d’un concurrent), d’une Personne publique (homme politique, acteur, sportif …) sur tous les réseaux sociaux (Twitter, Facebook …). Testez gratuitement notre plateforme de Surveillance de Marque et de *Réputation numérique*.

Paramétrer une Alerte

Paramétrez une alerte de Jurisprudence sur ce thème pour être informé par email lorsqu’une décision est rendue sur ce thème

---

Usage des réseaux sociaux par les aides-soignants

Secteur hospitalier, secteur sensible

L’usage des réseaux sociaux par les professionnels du secteur hospitalier peut poser de nombreuses difficultés juridiques, parmi lesquelles le droit au respect de la dignité de patients. Dans cette nouvelle affaire, le licenciement pour faute grave d’une aide-soignante en maison de retraite, a été validé par les juges.

Faute grave de l’aide-soignante

La faute grave se définit comme un fait ou un ensemble de faits, personnellement imputables au salarié, constituant une violation d’une obligation contractuelle ou un manquement à la discipline de l’entreprise, d’une gravité telle qu’elle rend impossible son maintien dans l’entreprise. La charge de la preuve de la gravité de la faute incombe à l’employeur. Le juge doit tenir compte des éléments qui lui sont alors soumis pour apprécier la gravité de la faute soutenue. En cas de doute, celui-ci profite au salarié. Le contrôle de la matérialité des faits reprochés auquel le juge doit procéder implique une appréciation de leur imputabilité au salarié, de leur caractère objectivement fautif et sérieux justifiant la rupture du contrat de travail, ainsi que de leur gravité rendant impossible le maintien dans l’entreprise.

En l’occurrence, l’employeur a découvert sur le compte Facebook de la salariée, une photographie prise par une autre

collègue de travail, dans l'appartement d'une résidente de la maison de retraite, clairement identifié, sur laquelle elle apparaissait en tenue de travail, portant un masque sur le visage et des gants d'hygiène, dans une pose festive, levant les bras en l'air en signe de victoire. Détail sordide, la résidente occupant cet appartement était en fin de vie, alitée, et donc présente au moment où la photographie a été prise. L'employeur, suivi par les juges, a considéré que ce comportement était contraire au code de déontologie et au règlement intérieur, le jugeant totalement inapproprié et inexcusable, en méconnaissance totale de ses valeurs morales ou éthiques régissant son mode de fonctionnement et la prise en charge des personnes hébergées.

Dignité des personnes âgées

L'article L.311-3 du code de l'action sociale et des familles pose le principe que toute personne prise en charge par des établissements et services sociaux et médico-sociaux a droit au respect de sa dignité, de son intimité. La charte des droits et libertés de la personne accueillie (arrêté du 8 septembre 2003 du ministère de la santé, de la famille et des personnes handicapées) ainsi que la charte des droits et libertés de la personne âgée dépendante et enfin la charte des valeurs de la résidence, rappellent ces principes de respect de l'intimité du résident et que la personne âgée en fin de vie doit pouvoir terminer sa vie dans le respect de ses convictions et en tenant compte de ses avis. Le règlement intérieur précisait également qu'il était nécessaire que soit observé un comportement réservé et digne, en tout point conforme aux bonnes moeurs, à la morale et à l'éthique, que toute familiarité avec les résidents est interdite.

La photographie postée sur Facebook mettait en évidence un comportement qualifié à juste titre de festif, notamment de la

salariée, en décalage avec la réserve attendue par l'employeur, dès lors que ce comportement a lieu dans la chambre d'une résidente, qui en tout état de cause est décédée peu de temps après. Même si la date exacte à laquelle ce comportement a eu lieu n'était pas établie avec certitude, un tel comportement traduisait un manque de respect à l'égard de la personne âgée résidente de cette chambre, dont l'état de santé était gravement altéré, constitutif d'une faute justifiant la rupture immédiate du contrat de travail étant observé que la publication de cette photographie a suscité une réaction d'émoi et de malaise au sein du personnel de la résidence.

Télécharger la Décision

Télécharger

Vendre un Contrat sur cette thématique

Vous disposez d'un modèle de document juridique sur cette thématique ? Complétez vos revenus en le vendant sur Uplex.fr, la 1ère plateforme de France en modèles de contrats professionnels

Poser une Question

Posez une Question Juridique sur cette thématique, la rédaction ou un abonné vous apportera une réponse en moins de 48h.

E-réputation | Surveillance de marques

Surveillez et analysez la réputation d'une **Marque** (la vôtre ou celle d'un concurrent), d'une Personne publique (homme politique, acteur, sportif …) sur tous les réseaux sociaux (Twitter, Facebook …). Testez gratuitement notre plateforme de Surveillance de Marque et de *Réputation numérique*.

Paramétrer une Alerte

Paramétrez une alerte de Jurisprudence sur ce thème pour être

informé par email lorsqu’une décision est rendue sur ce thème

---

Activité concurrente du salarié : la preuve par Facebook

L’obligation générale de loyauté

Une esthéticienne s’expose à un licenciement pour faute grave lorsqu’elle propose des prestations concurrentes à celles de son employeur. L’obligation générale de loyauté impose au salarié de ne pas exercer d’activité concurrente de celle de son employeur, même si le contrat de travail ne comporte pas de clause d’exclusivité.

Licenciement pour faute grave

La faute grave est celle qui résulte d’un fait ou d’un ensemble de faits imputables au salarié qui constituent une violation des obligations résultant du contrat de travail ou des relations de travail d’une importance telle qu’elle rend impossible le maintien du salarié dans l’entreprise et impose son départ immédiat. L’employeur qui invoque la faute grave doit en rapporter la preuve et les faits invoqués doivent être matériellement vérifiables. Il résulte enfin des articles L.1234-1 et L.1234-9 du code du travail que, lorsque le licenciement est motivé par une faute grave, le salarié n’a droit ni à un préavis, ni à une indemnité de licenciement.

En l’espèce, aux fins d’établir la réalité des griefs allégués, l’employeur a produit des captures d’écran de la page Facebook de « l’atelier d’esthétique » de la salariée comprenant des photographies d’ongles vernis, des remises promotionnelles, qu’il s’agisse de traitement des ongles, d’épilations, de soins du visage ou du corps, des invitations à prendre rendez-vous, l’indication des horaires d’ouverture … L’employeur a également produit diverses attestations de clientes qui indiquaient avoir eu connaissance de l’ouverture du salon d’esthétique de la salariée.

Question de l’exclusivité

En défense, la salarié a produit son contrat de travail, soulignant qu’il ne comportait pas de clause d’exclusivité, laquelle serait en toute hypothèse illicite au regard de son emploi à temps partiel. Si n’est pas fautif, le salarié qui se prépare, sans recourir à aucun procédé déloyal à la création d’une entreprise concurrente de celle de son employeur et dont l’exploitation ne doit commencer qu’après la rupture de son contrat de travail, il ressort des pièces produites que la salariée fixait des rendez-vous et exerçait effectivement son activité directement concurrente, à proximité de celle de son employeur. Les messages échangés avec une apprentie démontraient suffisamment sa volonté de dissimuler son activité à son employeur, outre d’autres captures de pages Facebook comportant des messages explicites faisant référence à la mise à pied qui venait de lui être notifiée et à son espérance de voir ses clientes la suivre. La preuve de la faute grave était donc suffisamment rapportée.

Télécharger la Décision

Télécharger

Vendre un Contrat sur cette thématique

Vous disposez d'un modèle de document juridique sur cette thématique ? Complétez vos revenus en le vendant sur Uplex.fr, la 1ère plateforme de France en modèles de contrats professionnels

Poser une Question

Posez une Question Juridique sur cette thématique, la rédaction ou un abonné vous apportera une réponse en moins de 48h.

E-réputation | Surveillance de marques

Surveillez et analysez la réputation d'une **Marque** (la vôtre ou celle d'un concurrent), d'une Personne publique (homme politique, acteur, sportif …) sur tous les réseaux sociaux (Twitter, Facebook …). Testez gratuitement notre plateforme de Surveillance de Marque et de *Réputation numérique*.

Paramétrer une Alerte

Paramétrez une alerte de Jurisprudence sur ce thème pour être informé par email lorsqu'une décision est rendue sur ce thème

---

Liberté d'expression des élus sur Facebook

Droit d'expression de la minorité municipale

Les juges administratifs ont annulé une délibération municipale n'autorisant pas des conseillers municipaux

n’appartenant pas à la majorité municipale d’accéder à l’espace d’expression du site internet et de la page Facebook de la ville.

Facebook, extension du bulletin d’information municipale

La commune a soutenu sans succès qu’une page Facebook n’est pas un bulletin d’information générale au sens de l’article L. 2121-27-1 du code général des collectivités territoriales dès lors qu’elle n’est pas un support diffusé par la collectivité et qu’elle n’a pas un contenu visant l’information générale sur les réalisations et la gestion de la commune. Aux termes de l’article L. 2121-27-1 du code général des collectivités territoriales, dans les communes de 3 500 habitants et plus, lorsque la commune diffuse, sous quelque forme que ce soit, un bulletin d’information générale sur les réalisations et la gestion du conseil municipal, un espace est réservé à l’expression des conseillers n’appartenant pas à la majorité municipale. Les modalités d’application de cette disposition sont définies par le règlement intérieur adopté par la Commune. Pour l’application de ces dispositions, toute mise à disposition du public de messages d’information portant sur les réalisations et la gestion du conseil municipal doit être regardée, quelle que soit la forme qu’elle revêt, comme la diffusion d’un bulletin d’information générale.

La circonstance que la commune utilise Facebook pour la diffusion d’informations sans être maître de l’outil de diffusion n’a pas pour effet de faire perdre à son compte Facebook officiel sa qualité de publication d’information générale au sens de l’article L. 2121-27-1. Si des modalités adaptées à ce support doivent être définies afin de permettre

l’expression des conseillers municipaux sur ce compte, il n’apparait pas que celles-ci ne pourraient être mises en oeuvre pour des raisons pratiques ou techniques ; le contrôle des contenus publiés peut par exemple être assuré par le directeur de la publication dans les mêmes conditions que pour d’autres médias. La Commune avait donc l’obligation d’ouvrir un espace d’expression réservé aux conseillers n’appartenant pas à la majorité municipale sur le site internet et la page Facebook de la ville.

Exclusion de Twitter

En revanche, eu égard au nombre limité de caractères et aux modalités de son fonctionnement, le compte « Twitter » de la commune, qui sert principalement à relayer des informations disponibles sur d’autres médias ou à annoncer des événements, n’entre pas dans le champ des dispositions précitées de l’article L. 2121-27-1 du code général des collectivités territoriales.

Poser une Question

Posez une Question Juridique sur cette thématique, la rédaction ou un abonné vous apportera une réponse en moins de 48h.

E-réputation | Surveillance de marques

Surveillez et analysez la réputation d'une **Marque** (la vôtre ou celle d'un concurrent), d'une Personne publique (homme politique, acteur, sportif …) sur tous les réseaux sociaux (Twitter, Facebook …). Testez gratuitement notre plateforme de Surveillance de Marque et de *Réputation numérique*.

Paramétrer une Alerte

Paramétrez une alerte de Jurisprudence sur ce thème pour être informé par email lorsqu'une décision est rendue sur ce thème

---

Conservation des données de connexion : la CJUE saisie

Conservation généralisée et indifférenciée des données

Saisi par plusieurs associations de défense des libertés, le Conseil d'État a soumis à la CJUE plusieurs questions préjudicielles portant sur le périmètre de conservation des données de connexion des contributeurs à des contenus en ligne. Il conviendra d'une part, de déterminer la légalité de l'obligation, à la charge des opérateurs, de conserver de façon généralisée et indifférenciée les données de nature à permettre l'identification de quiconque a contribué à la

création du contenu ou de l'un des contenus des services dont elles sont prestataires, afin que l'autorité judiciaire puisse, le cas échéant, en requérir communication en vue de faire respecter les règles relatives à la responsabilité civile ou pénale (articles 34-1 et R. 10-13 du code des postes et des communications électroniques).

Périmètre de la saisine de la CJUE

En premier lieu, les juges suprêmes ont rappelé que l'obligation de conservation des données de connexion revête un caractère général sans être limitée à des personnes ou circonstances particulières n'est pas, par lui-même, contraire aux exigences découlant des stipulations de l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

En second lieu, la directive du 12 juillet 2002 concernant le traitement des données à caractère personnel ne s'applique pas aux activités concernant la sécurité publique, la défense, la sûreté de l'État ou aux activités de l'État dans des domaines relevant du droit pénal. Par ailleurs, son article 15 prévoit expressément que les États membres peuvent adopter des mesures législatives visant à limiter la portée de l'obligation de confidentialité des données à caractère personnel lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale – c'est-à-dire la sûreté de l'État – la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une

durée limitée lorsque cela est justifié pour des motifs tenant à la sûreté de l'Etat ou à la lutte contre les infractions pénales.

Contrôle de proportionnalité

La CJUE sera amenée à procéder à un contrôle de proportionnalité sur l'obligation de conservation généralisée et indifférenciée des données de connexion. Par son arrêt du 21 décembre 2016, Tele2 Sverige AB c/ Post-och telestyrelsen et Secretary of State for the Home Department c/ Tom Watson et autres (C-203/15 et C-698/15), la Cour a déjà jugé qu'une conservation préventive et indifférenciée des permet à l'autorité judiciaire d'accéder aux données relatives aux communications qu'un individu a effectuées avant d'être suspecté d'avoir commis une infraction pénale. Une telle conservation présente dès lors une utilité sans équivalent pour la recherche, la constatation et la poursuite des infractions pénales.

D'autre part, une telle conservation, dès lors qu'elle ne révèle pas le contenu d'une communication, n'est pas de nature à porter atteinte au « contenu essentiel » des droits consacrés par les articles 7 et 8 de la Charte européenne. En outre, la Cour a depuis lors rappelé, dans son avis 1/15 du 26 juillet 2017, que ces droits " n'apparaissent pas comme étant des prérogatives absolues " et qu'un objectif d'intérêt général de l'Union est susceptible de justifier des ingérences, même graves, dans ces droits fondamentaux, après avoir relevé que " la protection de la sécurité publique contribue également à la protection des droits et des libertés d'autrui " et que " l'article 6 de la Charte énonce le droit de toute personne non seulement à la liberté, mais également à la sûreté ". Dans ces conditions la question de déterminer si l'obligation de conservation généralisée et indifférenciée,

imposée aux fournisseurs, soulève une difficulté d'interprétation du droit de l'Union européenne.

Par ailleurs, la question de déterminer si les dispositions de la directive du 8 juin 2000 lues à la lumière de la Charte des droits fondamentaux de l'Union européenne, doivent être interprétées en ce sens qu'elles permettent à un État d'instaurer une réglementation nationale imposant aux opérateurs de conserver les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont ils sont prestataires, afin que l'autorité judiciaire puisse, le cas échéant, en requérir communication en vue de faire respecter les règles relatives à la responsabilité civile ou pénale, soulève également une seconde difficulté sérieuse d'interprétation du droit de l'Union européenne.

Télécharger la Décision

Télécharger

Vendre un Contrat sur cette thématique

Vous disposez d'un modèle de document juridique sur cette thématique ? Complétez vos revenus en le vendant sur Uplex.fr, la 1ère plateforme de France en modèles de contrats professionnels

Poser une Question

Posez une Question Juridique sur cette thématique, la rédaction ou un abonné vous apportera une réponse en moins de 48h.

E-réputation | Surveillance de marques

Surveillez et analysez la réputation d'une **Marque** (la vôtre ou celle d'un concurrent), d'une Personne publique (homme politique, acteur, sportif …) sur tous les réseaux sociaux

(Twitter, Facebook …). Testez gratuitement notre plateforme de Surveillance de Marque et de *Réputation numérique*.

Paramétrer une Alerte

Paramétrez une alerte de Jurisprudence sur ce thème pour être informé par email lorsqu'une décision est rendue sur ce thème

---

Signature électronique de l'emprunteur : risque maximal

Affaire Carrefour Banque

Sévère revers judiciaire pour la société Carrefour Banque. Une juridiction d'appel a considéré que la signature électronique d'un emprunteur de crédit à la consommation, ne reposait pas sur un procédé fiable d'identification au sens des (ex) articles 1316-1 et 1316-4 du code civil et du décret du 30 mars 2001. La société Carrefour Banque a été déboutée de ses demandes en exécution / remboursement du contrat de crédit. Suivant offre préalable signée électroniquement le même jour, la société Carrefour avait consenti à un particulier un prêt personnel d'un montant de 15 000 euros remboursable en 84 mensualités en contrepartie d'un taux d'intérêt nominal annuel de 8,27%. Par la suite, le prêteur s'est prévalu de la déchéance du terme mais n'a pu obtenir le remboursement du prêt consenti.

Conditions de la signature

électronique fiable

Selon l'ex article 1108-1 du code civil, lorsqu'un écrit était exigé pour la validité d'un acte juridique, il pouvait être établi et conservé sous forme électronique dans les conditions prévues aux articles 1316-1 et 1316-4 (« *i) L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité ; ii) La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose).* Lorsqu'elle est électronique, la signature consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé était présumée, jusqu'à preuve contraire, lorsque la signature électronique était créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans les conditions fixées par l'ancien décret n°2001-272 du 30 mars 2001. Ce dernier précisait qu'une signature électronique sécurisée devait satisfaire aux exigences suivantes : i) être propre aux signataires, ii) être créée par des moyens que le signataire puisse garder sous son contrôle exclusif, iii) garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable.

La fiabilité d'un procédé de signature électronique était présumée jusqu'à preuve contraire lorsque ce procédé mettait en oeuvre une signature électronique sécurisée, établie grâce à un dispositif sécurisé de création de signature électronique et que la vérification de cette signature reposait sur l'utilisation d'un certificat électronique qualifié.

En l'espèce, la société Carrefour produisait aux débats un document intitulé « fichier de preuve de la transaction », par lequel la société Keynectis, en qualité de prestataire de

service de gestion de preuves, attestait que le fichier de preuve référencé contenait un document signé électroniquement (horodaté). Le document comportait plusieurs éléments d'information dont le nom de l'utilisateur, son adresse mail, son numéro de téléphone et le code à usage unique utilisé pour la transaction. Toutefois, ce dispositif ne répondait pas aux conditions légales de fiabilité et de certification. En effet, un dispositif sécurisé de création de signature électronique devait : i) Garantir par des moyens techniques et des procédures appropriées que les données de création de signature électronique ne pouvaient être établies plus d'une fois et que leur confidentialité est assurée ; ne pouvaient être trouvées par déduction et que la signature électronique est protégée contre toute falsification ; ne pouvaient être protégées de manière satisfaisante par le signataire contre toute utilisation par des tiers.

Par ailleurs, un dispositif sécurisé de création de signature électronique devait être certifié i) soit par les services du Premier ministre chargés de la sécurité des systèmes d'information, après une évaluation ; ii) Soit par un organisme désigné à cet effet par un Etat membre de la Communauté européenne.

Le document produit aux débats intitulé « attestation » ne contenait aucun élément de nature à caractériser l'existence de l'ensemble de ces exigences, il n'était par ailleurs pas produit le certificat de conformité. Ce document n'était donc pas suffisant pour établir d'une part que le procédé mettait en oeuvre une signature électronique sécurisée, établie grâce à un dispositif sécurisé de création de signature électronique, d'autre part que la vérification de cette signature reposait sur l'utilisation d'un certificat électronique qualifié. Aucune présomption de fiabilité du procédé de signature électronique ne pouvait être invoquée par la société Carrefour Banque.

Télécharger la Décision

Télécharger

Vendre un Contrat sur cette thématique

Vous disposez d'un modèle de document juridique sur cette thématique ? Complétez vos revenus en le vendant sur Uplex.fr, la 1ère plateforme de France en modèles de contrats professionnels

Poser une Question

Posez une Question Juridique sur cette thématique, la rédaction ou un abonné vous apportera une réponse en moins de 48h.

E-réputation | Surveillance de marques

Surveillez et analysez la réputation d'une **Marque** (la vôtre ou celle d'un concurrent), d'une Personne publique (homme politique, acteur, sportif …) sur tous les réseaux sociaux (Twitter, Facebook …). Testez gratuitement notre plateforme de Surveillance de Marque et de *Réputation numérique*.

Paramétrer une Alerte

Paramétrez une alerte de Jurisprudence sur ce thème pour être informé par email lorsqu'une décision est rendue sur ce thème

---

Géolocalisation du salarié : la déclaration CNIL insuffisante

Calcul des heures supplémentaires

Le calcul des heures de travail supplémentaires effectuées par le salarié peut dépendre directement de la licéité d'un dispositif de géolocalisation. Dans cette affaire, une entreprise a été condamnée à payer à l'un de ses salariés plus de 2 000 heures de travail supplémentaires.

Relevés de géolocalisation

Pour contester les relevés manuscrits présentés par le salarié, la société avait produit la totalité des relevés de géolocalisation du véhicule de service qu'elle avait confié au salarié. Pour être régulier, l'usage par un employeur d'un dispositif de géolocalisation des véhicules confiés à ses salariés pour l'exercice de leurs fonctions suppose notamment qu'au préalable : i) le comité d'entreprise ait été informé et consulté sur ce projet, ii) une déclaration à la CNIL ait été régulièrement effectuée, iii) que le salarié ait reçu une notification individuelle de la mise en oeuvre de ce traitement informatisé le concernant.

En l'espèce, la déclaration CNIL avait bien été effectuée et le salarié avait reçu la notification requise l'informant de ce que son véhicule ferait l'objet d'une géolocalisation. Toutefois, aucune preuve de la consultation du comité d'entreprise sur ce projet, consultation qui supposait que ce comité émette un avis à ce sujet, n'était rapportée (le comité d'entreprise avait simplement été informé et non consulté).

Consultation du comité d'entreprise

La consultation du comité d'entreprise, qui doit permettre à

ce dernier de donner son avis sur la pertinence et la proportionnalité entre l'utilisation de la géolocalisation et la finalité recherchée (surveillance des salariés, suivi du temps de travail, etc.) est expressément imposée à l'employeur par les articles L.2323-13 et L.2323-32 du code du travail qui, dans leur rédaction applicable au litige, disposent que :

Article L. 2323-13: « Le comité d'entreprise est informé et consulté, préalablement à tout projet important d'introduction de nouvelles technologies, lorsque celles-ci sont susceptibles d'avoir des conséquences sur l'emploi, la qualification, la rémunération, la formation ou les conditions de travail. Les membres du comité reçoivent, un mois avant la réunion, des éléments d'information sur ces projets et leurs conséquences sur chacun des sujets mentionnés au premier alinéa. » ; Article L. 2323-32, alinéa 3: « Le comité d'entreprise est informé et consulté, préalablement à la décision de mise en oeuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés. »

En l'espèce, il apparaît que si le but poursuivi dans la mise en oeuvre de ce dispositif de géolocalisation au sein de l'entreprise n'était pas sérieusement contestable, s'agissant de travailler avec le salarié sur l'organisation optimisée de son activité, il n'en reste pas moins que le comité d'entreprise n'a manifestement pas été régulièrement consulté à ce sujet, faute de preuve de ce que cet organe représentatif a émis sur ce sujet un avis, même implicite. Il apparaissait d'ailleurs que même l'information donnée au comité d'entreprise était ici critiquable, l'employeur ne justifiant aucunement de l'envoi aux membres du comité des documents et informations prévus par le 2ème alinéa de l'article L2323-13, ni du respect du délai d'un mois prévu par ce texte. En conséquence, les relevés d'horaires de travail tirés du dispositif de géolocalisation du véhicule de service du salarié ne lui étaient pas juridiquement opposables.

Télécharger la Décision

Télécharger

Vendre un Contrat sur cette thématique

Vous disposez d'un modèle de document juridique sur cette thématique ? Complétez vos revenus en le vendant sur Uplex.fr, la 1ère plateforme de France en modèles de contrats professionnels

Poser une Question

Posez une Question Juridique sur cette thématique, la rédaction ou un abonné vous apportera une réponse en moins de 48h.

E-réputation | Surveillance de marques

Surveillez et analysez la réputation d'une **Marque** (la vôtre ou celle d'un concurrent), d'une Personne publique (homme politique, acteur, sportif …) sur tous les réseaux sociaux (Twitter, Facebook …). Testez gratuitement notre plateforme de Surveillance de Marque et de *Réputation numérique*.

Paramétrer une Alerte

Paramétrez une alerte de Jurisprudence sur ce thème pour être informé par email lorsqu'une décision est rendue sur ce thème

---

Téléphonie : preuve de la surconsommation du salarié

Licenciement pour faute grave

Une société a licencié un agent de sécurité pour faute grave

pour utilisation à des fins privées du portable de la société ayant entraîné des surconsommations (plus de 10 000 euros). L'employeur reprochait au salarié d'avoir enlevé la carte SIM du téléphone portable mis à sa disposition pour la mettre dans son téléphone personnel (détournement du matériel professionnel à des fins personnelles).

Preuve des agissements fautifs

Il résulte des dispositions de l'article L.1231-1 du code du travail que le contrat à durée indéterminée peut être rompu à l'initiative de l'employeur ou du salarié; aux termes de l'article L.1232-1 du code du travail, le licenciement par l'employeur pour motif personnel est justifié par une cause réelle et sérieuse. Il résulte des dispositions combinées des articles L 1232-1, L 1232-6, L 1234-1 et L 1235-1 du code du travail que devant le juge, saisi d'un litige dont la lettre de licenciement fixe les limites, il incombe à l'employeur qui a licencié un salarié pour faute grave, d'une part d'établir l'exactitude des faits imputés à celui-ci dans la lettre, d'autre part de démontrer que ces faits constituent une violation des obligations découlant du contrat de travail ou des relations de travail d'une importance telle qu'elle rend impossible le maintien de ce salarié dans l'entreprise pendant la durée limitée du préavis.

Il ressortait des éléments factuels du dossier concernant les surconsommations téléphoniques établies par un listing fourni par la société ORANGE, que des connexions internet ont été effectuées par l'équipe de surveillance dont faisait partie le salarié licencié. Cependant des éléments apparaissaient incohérents et contradictoires :

– le listing attestant des dates, heures et durées de surconsommations ne permettait pas de retrouver les numéros de téléphones utilisés et ce alors qu'aux termes des factures produites, il apparaissait que la société possédait 7

téléphones et que seuls 4 téléphones auraient été abusivement utilisés ;

– un des numéros visés dans la lettre de licenciement n'apparaissait pas être attribué à la société ;

– il n'était pas établi que le salarié avait la responsabilité exclusive des téléphones qui étaient utilisés aux jours concernés (téléphones partagés) ;

– concernant l'utilisation loyale du matériel, la société n'a fait signer aucun document au salarié (charte ou autre) ;

Dans ces conditions, la société n'établissait pas les utilisations abusives.

Indemnisation du licenciement sans cause réelle et sérieuse

En application des articles L 1235-3 et L 1235-5 du code du travail, le salarié ayant eu une ancienneté supérieure à deux ans dans une entreprise occupant habituellement 11 salariés au moins, a pu prétendre, en l'absence de réintégration dans l'entreprise, à une indemnité qui ne pouvait être inférieure aux salaires des six derniers mois. Compte tenu de l'effectif de l'entreprise, des circonstances de la rupture, du montant de la rémunération versée, de son ancienneté de plus de 16 années, de ce qu'il n'a pu retrouver un nouvel emploi, le salarié a obtenu près de 23 000 euros d'indemnisation. Au regard des circonstances de la rupture intervenue brutalement alors que le salarié n'avait fait l'objet d'aucune sanction disciplinaire au préalable, le salarié a également obtenu 2000 euros à titre de dommages et intérêts pour son préjudice moral.

Télécharger la Décision

Télécharger

Vendre un Contrat sur cette thématique

Vous disposez d'un modèle de document juridique sur cette thématique ? Complétez vos revenus en le vendant sur Uplex.fr, la 1ère plateforme de France en modèles de contrats professionnels

Poser une Question

Posez une Question Juridique sur cette thématique, la rédaction ou un abonné vous apportera une réponse en moins de 48h.

E-réputation | Surveillance de marques

Surveillez et analysez la réputation d'une **Marque** (la vôtre ou celle d'un concurrent), d'une Personne publique (homme politique, acteur, sportif …) sur tous les réseaux sociaux (Twitter, Facebook …). Testez gratuitement notre plateforme de Surveillance de Marque et de *Réputation numérique*.

Paramétrer une Alerte

Paramétrez une alerte de Jurisprudence sur ce thème pour être informé par email lorsqu'une décision est rendue sur ce thème

---

Injures entre particuliers sur Facebook

Insultes sur Facebook

Les particuliers n'échappent pas aux condamnations pour injure

publique sur les réseaux sociaux. Un particulier a été condamné à 1000 euros de dommages-intérêts pour avoir insulté un distributeur de prospectus.

Injure accessible publiquement

Le profil public du compte Facebook de l'auteur comportait la photographie du distributeur accompagnée du message suivant : « *Voici l'enculé M. .. distributeur de prospectus a bord d'une Renault Captur bleue et blanche imm … qui s'amuse depuis plus de six mois a agressé et insulté avec ses parents mon fils de 17ans … vla l'homme ptif il habite Frouard n'hésitez pas à mettre des comms car je veux le chopper adroitement cet enculé de ces morts et qui font chier aussi une voisine dont je vais bricoler chez elle mais très grave ».*
 Ce message, comportant des termes manifestement outrageants et méprisants, accessibles à tous les internautes, constituait une injure publique envers un particulier au sens de l'article 29 de la loi du 29 juillet 1881 constitutive d'une faute.

Conditions de l'excuse de provocation

L'Auteur ne contestait pas avoir insulté le distributeur de prospectus mais a soutenu que cette insulte avait été précédée d'une provocation (insultes verbalesA). Toutefois, pour être excusable, l'auteur de l'injure doit répondre à une provocation alors qu'il est sous le coup de l'émotion que cette provocation a pu lui causer. Or, l'auteur a injurié la victime en diffusant un message sur son compte Facebook, il en résultait qu'il avait agi de manière réfléchie ; il ne pouvait en conséquence soutenir qu'il avait agi sous le coup de la provocation.

Télécharger la Décision

Télécharger

Vendre un Contrat sur cette thématique

Vous disposez d'un modèle de document juridique sur cette thématique ? Complétez vos revenus en le vendant sur Uplex.fr, la 1ère plateforme de France en modèles de contrats professionnels

Poser une Question

Posez une Question Juridique sur cette thématique, la rédaction ou un abonné vous apportera une réponse en moins de 48h.

E-réputation | Surveillance de marques

Surveillez et analysez la réputation d'une **Marque** (la vôtre ou celle d'un concurrent), d'une Personne publique (homme politique, acteur, sportif …) sur tous les réseaux sociaux (Twitter, Facebook …). Testez gratuitement notre plateforme de Surveillance de Marque et de *Réputation numérique*.

Paramétrer une Alerte

Paramétrez une alerte de Jurisprudence sur ce thème pour être informé par email lorsqu'une décision est rendue sur ce thème

---

Liberté d'expression du salarié sur Twitter

Mutation disciplinaire

Un salarié engagé par la société SNCF Mobilité en qualité

d’agent commercial et également membre du CHSCT (syndicat Force ouvrière) a été sanctionné suite à la publication de propos excessifs sur Twitter. A titre de sanction disciplinaire, le salarié a été affecté à une fonction d’agent d’accueil.

Abus d’expression sur Twitter

La sanction du salarié a été confirmée en raison de la publication sur le réseau social public Twitter de propos inappropriés à l’encontre de la direction de l’entreprise et de termes irrespectueux, injurieux et agressifs envers certains encadrants nommément désignés, mettant en cause leur probité et leurs compétences professionnelles. Ces propos, répétitifs et insistants, contraires à l’exercice normal et loyal de la liberté d’expression, constituaient une atteinte à l’image de l’entreprise et au respect du personnel encadrant.

Modalités d’acceptation d’une sanction par le salarié

Par requête, le salarié a saisi la formation de référé du conseil de prud’hommes et sollicité la suspension de la mesure de déplacement disciplinaire prononcée à son encontre. En défense, l’employeur a contesté avec succès l’existence d’un quelconque trouble manifestement illicite dès lors que le salarié avait donné son accord au déplacement temporaire objet de la sanction contestée. Il en déduit qu’il n’y a pas lieu à référé.

Par lettre, le salarié avait indiqué à son employeur qu’il ne souhaitait pas qu’une procédure de radiation soit engagée à

son encontre si bien qu'il se voyait contraint d'accepter la mesure de déplacement prononcée, mais qu'il estimait cette sanction injustifiée et irrégulière et qu'il entendait faire valoir ses droits en justice. Même si l'acceptation de la mutation a été faite sous la réserve de l'action en contestation de la sanction engagée devant le juge du fond, il n'en demeure pas moins que le salarié a donné son consentement à la sanction de déplacement, alors qu'il avait la possibilité de la refuser et d'empêcher ainsi sa mise en oeuvre. L'alternative donnée par l'employeur entre l'acceptation de la mesure de déplacement et, à défaut, la reprise de la procédure disciplinaire pouvant alors mener au licenciement, ne constitue pas une menace mais une information sur les possibilités offertes à la SNCF en conformité avec le droit disciplinaire. Elle permettait au salarié d'exprimer son consentement ou son refus en ayant clairement conscience de la portée de sa décision. En outre, le salarié ne justifiait d'aucun élément particulier de nature à caractériser un quelconque vice du consentement dans sa décision d'acceptation de la mesure de déplacement. Dès lors, le consentement du salarié a fait obstacle à ce que l'application de la sanction soit considérée comme manifestement illicite.

A noter que la demande d'explications écrites faite par l'employeur préalablement à la prise de la sanction a été qualifiée de mesure d'instruction de nature à permettre au salarié de faire valoir ses observations sur les griefs énoncés à son encontre. Cette procédure a pour but d'assurer l'effectivité du principe du contradictoire et ne peut s'analyser en une sanction.

Télécharger la Décision

Télécharger

Vendre un Contrat sur cette thématique

Vous disposez d'un modèle de document juridique sur cette thématique ? Complétez vos revenus en le vendant sur Uplex.fr, la 1ère plateforme de France en modèles de contrats professionnels

Poser une Question

Posez une Question Juridique sur cette thématique, la rédaction ou un abonné vous apportera une réponse en moins de 48h.

E-réputation | Surveillance de marques

Surveillez et analysez la réputation d'une **Marque** (la vôtre ou celle d'un concurrent), d'une Personne publique (homme politique, acteur, sportif …) sur tous les réseaux sociaux (Twitter, Facebook …). Testez gratuitement notre plateforme de Surveillance de Marque et de *Réputation numérique*.

Paramétrer une Alerte

Paramétrez une alerte de Jurisprudence sur ce thème pour être informé par email lorsqu'une décision est rendue sur ce thème

---

Noms de domaine similaires : le risque de confusion

Affaire Face Sud

Un exploitant individuel (EURL) a enregistré il y a près de 20 ans, le nom de domaine Facesud.fr pour exploiter une activité de travaux acrobatiques, travaux en hauteur, couverture, plomberie et travaux d'étanchéité. La SCM Face Sud a été

constituée par un tiers plusieurs années postérieurement à l'enregistrement du nom de domaine Facesud.fr, pour développer une activité d'escalade et de canyoning. Elle a par la suite déposé la marque « Face Sud » auprès de l'INPI ainsi que le nom de domaine « face-sud.fr ».

Action en nullité de marque

L'EURL Face Sud a fait assigner les SCM Face Sud devant le TGI en nullité de la marque « Face Sud » et radiation du nom de domaine face-sud.fr. L'EURL Face Sud reprochait au tiers d'avoir commis une faute en réservant un nom de domaine similaire au sien, l'ajout d'un trait d'union étant une différence inopérante.

Appréciation du risque de confusion

Le tiers poursuivi, suivi par les juges du fond, a soulevé en défense l'absence de risque de confusion. Pour qu'une faute soit établie, le demandeur doit rapporter la preuve d'un risque de confusion entre les sites, c'est à dire, en pratique, que les activités visées par les sites internet respectifs des parties soient concurrents, ce qui n'était pas le cas en l'espèce. La désignation des sites internet des deux parties présentait une indéniable ressemblance tout comme les emails de contact. Néanmoins, il ne peut y avoir de comportement fautif constituant une concurrence déloyale que s'il est démontré un risque de confusion. Or en l'espèce, hormis le caractère voisin des deux dénominations, les activités de chacune des parties ne présentaient qu'une similitude lointaine voire de complémentarité : les activités de loisirs et celles du BTP étant distinctes. La réalisation de travaux acrobatiques, qui peut nécessiter l'usage de cordes sur des surfaces verticales, ne peut entraîner un risque de

confusion avec la pratique d'activités sportives de plein air ces activités n'étant ni substituables, ni analogues aux travaux de bâtiment et aux travaux publics réalisés par l'EURL.

Télécharger la Décision

Télécharger

Vendre un Contrat sur cette thématique

Vous disposez d'un modèle de document juridique sur cette thématique ? Complétez vos revenus en le vendant sur Uplex.fr, la 1ère plateforme de France en modèles de contrats professionnels

Poser une Question

Posez une Question Juridique sur cette thématique, la rédaction ou un abonné vous apportera une réponse en moins de 48h.

E-réputation | Surveillance de marques

Surveillez et analysez la réputation d'une **Marque** (la vôtre ou celle d'un concurrent), d'une Personne publique (homme politique, acteur, sportif …) sur tous les réseaux sociaux (Twitter, Facebook …). Testez gratuitement notre plateforme de Surveillance de Marque et de *Réputation numérique*.

Paramétrer une Alerte

Paramétrez une alerte de Jurisprudence sur ce thème pour être informé par email lorsqu'une décision est rendue sur ce thème

---

Contrat de distribution de logiciel : 6 réflexes juridiques

Négocier un contrat de distribution de logiciel

Faire appel à un distributeur en circuits physiques ou électroniques est incontournable pour assurer des débouchés commerciaux à un logiciel. Certains distributeurs disposent déjà de contrats d'adhésion difficilement négociables. Toutefois, si une marge de négociation existe elle doit impérativement porter sur les points ci-dessous qui font l'objet de contentieux récurrents.

Exclure l'exclusivité contractuelle

L'éditeur du logiciel a pour principal objectif de maximiser ses revenus commerciaux. A ce titre, le contrat de distribution de logiciel est avant tout un contrat de distribution commercial avec ses clauses usuelles (reddition des comptes, objectifs de ventes …). Pour ce faire, l'éditeur doit pouvoir, pendant toute la durée de la licence, être libre de distribuer le logiciel autrement que par l'intermédiaire du distributeur et notamment de développer des produits concurrents. Il en va de même de l'exploitation du titre du logiciel qui devra être déposé à titre de marque verbale ou figurative. Chaque distributeur sera autorisé à utiliser l'une quelconque des marques commerciales de l'éditeur telle que figurant en annexe du contrat de distribution.

Mettre en place une copropriété sur les données clients

Afin de développer sa clientèle, l'éditeur pourra négocier une clause de copropriété sur le fichier clients (données des acheteurs) du distributeur. Les acheteurs du logiciel devront être informés en amont de cette possibilité de cession de leurs données personnelles (RGDP) qui présentera notamment l'avantage, par exemple, de bénéficier des mises à jour.

Mettre en place et gérer des clefs d'activation

Mettre en place une base de données de gestion des clefs d'activation sera déterminant pour assurer le respect des droits de propriété intellectuelle de l'éditeur du logiciel. A cette fin, la vente / le téléchargement du logiciel pourra être assortie d'une procédure d'activation. La collecte des données personnelles des utilisateurs pourra intervenir au cours de cette phase.

Suivre la reddition des comptes

Le suivi de la reddition des comptes et du suivi des ventes est un des points déterminants du **contrat de distribution de logiciel.** A toutes fins utiles, la clause suivante pourra être stipulée : *« La gestion comptable de la distribution est confiée au Distributeur pour l'ensemble des recettes d'exploitation. Un état des charges et recettes résultant de toutes les exploitations sera arrêté par le Distributeur à la fin de chaque semestre calendaire et transmis à l'Editeur dans les trois mois suivant l'expiration de la période de comptes.*

Les justificatifs afférents à tous les revenus provenant de ces exploitations seront tenus à la disposition de l'Editeur ou de ses mandataires au Siège social du Distributeur aux heures d'ouverture de celui-ci. A réception des relevés précités, le Distributeur établira une facture qui sera payable à réception par l'Editeur. »

Prendre garde à la résiliation abusive

Comme tout contrat commercial, la résiliation abusive du **contrat de distribution de logiciel** pourra être sanctionnée par les juridictions. Dans une affaire jugée récemment sur la rupture d'un contrat de distribution de plusieurs logiciels, les juridictions ont considéré qu'un délai de préavis de six mois était suffisant pour échapper à une rupture brutale de relations commerciales.

A titre de rappel, au sens de l'article L 442-6,1,5° du code de commerce : « *engage la responsabilité de son auteur et l'oblige à réparer le préjudice causé le fait, par tout producteur, commerçant, industriel ou personne immatriculée au répertoire des métiers … de rompre brutalement, même partiellement, une relation commerciale établie, sans préavis écrit tenant compte de la durée de la relation commerciale et respectant la durée minimale de préavis déterminée, en référence aux usages du commerce, par des accords interprofessionnels. Les dispositions qui précèdent ne font pas obstacle à la faculté de résiliation sans préavis, en cas d'inexécution par l'autre partie de ses obligations ou en cas de force majeure* ». L'application de l'article L.442-6 du code de commerce suppose la réunion de trois conditions : i) l'existence de relations commerciales établies, ii) une rupture brutale, c'est-à-dire imprévisible, soudaine et

violente et en conséquence préjudiciable, et iii) que ladite rupture ne repose pas sur de justes motifs.

Prévoir la résiliation anticipée du contrat de distribution de logiciel

L'éditeur du logiciel doit pouvoir changer de distributeur commercial, notamment en cas d'insuffisance des ventes. Plusieurs autres hypothèses de sortie contractuelle anticipée pourront être envisagées. A titre d'exemple, le contrat de commercialisation et de distribution de logiciels peut comporter une clause de résiliation anticipée qualifiable par les parties de clause d'intuitu personae : « *l'Éditeur pourra résilier le contrat avec effet immédiat si les actionnaires actuels du Distributeur venaient à cesser de contrôler leur société à moins que l'Éditeur n'approuve ledit transfert de propriété en actions* ». Il a été jugé que la mise en oeuvre de cette clause de résiliation anticipée pour changement de contrôle n'est subordonnée ni à la constatation préalable du transfert de propriété des titres cédés ni à la notification de ce transfert. Cette clause n'impose pas plus à la partie qui s'en prévaut de faire connaître à sa cocontractante les motifs de la résiliation.

Télécharger la Décision

Télécharger 1 | Télécharger 2 | Télécharger 3 | Télécharger 4

Vendre un Contrat sur cette thématique

Poser une Question

Posez une Question Juridique sur cette thématique, la rédaction ou un abonné vous apportera une réponse en moins de 48h.

E-réputation | Surveillance de marques

Surveillez et analysez la réputation d'une **Marque** (la vôtre ou celle d'un concurrent), d'une Personne publique (homme politique, acteur, sportif …) sur tous les réseaux sociaux (Twitter, Facebook …). Testez gratuitement notre plateforme de Surveillance de Marque et de *Réputation numérique*.

Paramétrer une Alerte

Paramétrez une alerte de Jurisprudence sur ce thème pour être informé par email lorsqu'une décision est rendue sur ce thème

---

Données personnelles religieuses

Affaire des témoins de Jéhovah

Collecter des données personnelles en porte à porte ne dispense pas du respect des obligations en matière de traitement des données personnelles. La CJUE a considéré qu'une communauté religieuse, telle que celle des témoins de Jéhovah, est responsable, conjointement avec ses membres prédicateurs, du traitement des données à caractère personnel collectées dans le cadre d'une activité de prédication de porte-à-porte. La commission finlandaise de protection des données est en droit d'interdire à la communauté religieuse

des témoins de Jéhovah en Finlande, de collecter ou de traiter des données à caractère personnel dans le cadre de l'activité de prédication de porte-à-porte effectuée par ses membres, sans que les conditions légales prévues pour le traitement de telles données soient respectées.

Porte à porte et collecte domestique de données

Les membres de cette communauté prennent, dans le cadre de leur activité de prédication de porte-à-porte, des notes sur les visites rendues à des personnes que ni eux ni la communauté ne connaissent. Les données collectées peuvent comporter le nom et l'adresse des personnes démarchées ainsi que des informations portant sur leurs convictions religieuses et leur situation familiale. Elles sont collectées à titre d'aide-mémoire afin de pouvoir être retrouvées pour une éventuelle visite ultérieure, sans que les personnes concernées y aient consenti ni en aient été informées. La communauté des témoins de Jéhovah et les paroisses qui en dépendent organiseraient et coordonneraient l'activité de prédication de porte-à-porte de leurs membres, notamment en établissant des cartes à partir desquelles des secteurs seraient répartis entre les membres prédicateurs et en tenant des fiches sur les prédicateurs et le nombre de publications de la communauté diffusées par ceux-ci.

En outre, les paroisses de la communauté des témoins de Jéhovah géreraient une liste des personnes ayant exprimé le souhait de ne plus faire l'objet de visites de la part des membres prédicateurs ; les données à caractère personnel figurant sur cette liste seraient utilisées par les membres de la communauté.

L’activité de prédication de porte-à-porte des membres de la communauté des témoins de Jéhovah ne relève pas des exceptions prévues par le droit de l’Union en matière de protection des données à caractère personnel. En particulier, cette activité n’est pas une activité exclusivement personnelle ou domestique à laquelle ce droit ne s’applique pas. La circonstance que l’activité de prédication de porte-à-porte est protégée par le droit fondamental à la liberté de conscience et de religion (article 10 de la charte des droits fondamentaux de l’Union européenne), n’a pas pour effet de lui conférer un caractère exclusivement personnel ou domestique, en raison du fait qu’elle dépasse la sphère privée d’un membre prédicateur d’une communauté religieuse.

Traitement non automatisé de données personnelles

Ensuite, la CJUE a rappelé que les règles du droit de l’Union en matière de protection des données à caractère personnel ne s’appliquent, cependant, au traitement manuel des données que lorsque ces dernières sont contenues dans un fichier ou sont appelées à figurer dans un fichier. En l’espèce, comme le traitement de données à caractère personnel est effectué de manière non automatisée, la question s’est posée de savoir si les données ainsi traitées sont contenues dans un fichier ou sont appelées à figurer dans un tel fichier.

À cet égard, la Cour a conclu que la notion de « fichier » couvre tout ensemble de données à caractère personnel collectées dans le cadre d’une activité de prédication de porte-à-porte et comportant des noms et des adresses ainsi que d’autres informations concernant les personnes démarchées, dès lors que ces données sont structurées selon des critères déterminés permettant, en pratique, de les retrouver aisément

aux fins d’une utilisation ultérieure. Pour qu’un tel ensemble relève de cette notion, il n’est pas nécessaire que celui-ci comprenne des fiches, des listes spécifiques ou d’autres systèmes de recherche.

Notion de responsable du traitement des données

En ce qui concerne la question de savoir qui peut être considéré comme responsable du traitement des données à caractère personnel, la Cour a jugé que la notion de « responsable du traitement » peut concerner plusieurs acteurs participant à ce traitement, chacun d’entre eux devant alors être soumis aux règles du droit de l’Union en matière de protection des données à caractère personnel. Ces acteurs peuvent être impliqués à différents stades du traitement et à des degrés divers, de telle sorte que le niveau de responsabilité de chacun d’entre eux doit être évalué en tenant compte de toutes les circonstances pertinentes du cas d’espèce. Une personne physique ou morale qui influe, à des fins qui lui sont propres, sur le traitement des données à caractère personnel et participe, de ce fait, à la détermination des finalités et des moyens de ce traitement peut être considérée comme étant responsable du traitement. En outre, la responsabilité conjointe de plusieurs acteurs ne présuppose pas que chacun d’eux ait accès aux données à caractère personnel.

En l’occurrence, il apparaît que la communauté des témoins de Jéhovah, en organisant, coordonnant et encourageant l’activité de prédication de ses membres, participe, conjointement avec ses membres prédicateurs, à la détermination de la finalité et des moyens du traitement des données à caractère personnel des personnes démarchées, ce qu’il appartient toutefois à la

juridiction finlandaise d'apprécier au regard de l'ensemble des circonstances de l'espèce. Le droit de l'Union en matière de protection des données permet de considérer une communauté religieuse comme responsable, conjointement avec ses membres prédicateurs, du traitement des données à caractère personnel effectué par ces derniers dans le cadre d'une activité de prédication de porte à porte organisée, coordonnée et encouragée par cette communauté, sans qu'il soit nécessaire que la communauté en question ait accès aux données ni qu'il doive être établi qu'elle a donné à ses membres des lignes directrices écrites ou des consignes relativement à ce traitement.

Télécharger la Décision

Télécharger

Vendre un Contrat sur cette thématique

Vous disposez d'un modèle de document juridique sur cette thématique ? Complétez vos revenus en le vendant sur Uplex.fr, la 1ère plateforme de France en modèles de contrats professionnels

Poser une Question

Posez une Question Juridique sur cette thématique, la rédaction ou un abonné vous apportera une réponse en moins de 48h.

E-réputation | Surveillance de marques

Surveillez et analysez la réputation d'une **Marque** (la vôtre ou celle d'un concurrent), d'une Personne publique (homme politique, acteur, sportif …) sur tous les réseaux sociaux (Twitter, Facebook …). Testez gratuitement notre plateforme de Surveillance de Marque et de *Réputation numérique*.

Paramétrer une Alerte

Paramétrez une alerte de Jurisprudence sur ce thème pour être

informé par email lorsqu'une décision est rendue sur ce thème

---

Harcèlement sexuel en ligne : renforcement des sanctions

Nouvel article 222-33 du code pénal

Le nouvel article 222-33 du code pénal tel que modifié par la loi n°2018-703 du 3 août 2018 renforce les sanctions en matière de harcèlement sexuel électronique (trois ans d'emprisonnement et 45 000 € d'amende au lieu de deux ans d'emprisonnement et de 30 000 € d'amende).

Définition du harcèlement sexuel

Pour rappel, le harcèlement sexuel est le fait d'imposer à une personne, de façon répétée, des propos ou comportements à connotation sexuelle ou sexiste qui soit portent atteinte à sa dignité en raison de leur caractère dégradant ou humiliant, soit créent à son encontre une situation intimidante, hostile ou offensante. L'infraction pénale est également constituée : i) lorsque ces propos ou comportements sont imposés à une même victime par plusieurs personnes, de manière concertée ou à l'instigation de l'une d'elles, alors même que chacune de ces personnes n'a pas agi de façon répétée ; ii) lorsque ces propos ou comportements sont imposés à une même victime, successivement, par plusieurs personnes qui, même en l'absence de concertation, savent que ces propos ou comportements caractérisent une répétition. Est également assimilé au

harcèlement sexuel le fait, même non répété, d'user de toute forme de pression grave dans le but réel ou apparent d'obtenir un acte de nature sexuelle, que celui-ci soit recherché au profit de l'auteur des faits ou au profit d'un tiers.

Renforcement des sanctions

Les peines liées au harcèlement sexuel sont également portées à trois ans d'emprisonnement et 45 000 € d'amende lorsque les faits sont commis : i) Par une personne qui abuse de l'autorité que lui confèrent ses fonctions ; ii) Sur un mineur de quinze ans ; iii) Sur une personne dont la particulière vulnérabilité, due à son âge, à une maladie, à une infirmité, à une déficience physique ou psychique ou à un état de grossesse, est apparente ou connue de leur auteur ; iv) Sur une personne dont la particulière vulnérabilité ou dépendance résultant de la précarité de sa situation économique ou sociale est apparente ou connue de leur auteur ; v) Par plusieurs personnes agissant en qualité d'auteur ou de complice.

Répression des cyberviolences et du cybersexisme

Le harcèlement électronique présente certaines spécificités. Les outils numériques ne font pas nécessairement apparaître de nouveaux comportements mais ils leur donnent une nouvelle visibilité et des moyens pour se renforcer. Il convient de distinguer cyberviolence et cybersexisme. La cyberviolence peut être définie comme un acte agressif intentionnel utilisant des outils numériques. Le cybersexisme désigne quant à lui l'ensemble des comportements et propos sexistes diffusés sur un support numérique ; ils ne visent pas nécessairement

une personne en particulier mais participent d'un environnement intimidant ou entretiennent une atmosphère oppressante.

Les violences numériques apparaissent comme un phénomène en forte augmentation, difficiles à appréhender dans leur diversité et leur complexité. Elles se doublent d'un sentiment d'impunité lié à l'absence de proximité physique et à l'anonymat prévalant dans le monde numérique. Au vu des conséquences lourdes pour les victimes, le législateur a donc mieux réprimé ces dérives.

Un groupe de travail des Nations Unies sur les cyberviolences estimait en 2015 que 73 % des femmes auraient été confrontées à des violences en ligne ou en auraient été directement victimes. La même étude relève que dans les 28 pays de l'Union européenne, 18 % des femmes auraient subi une forme grave de violence sur Internet dès l'âge de 15 ans. Le rapport du Haut Conseil à l'égalité sur les violences faites aux femmes en ligne de novembre 2017 renvoie quant à lui à la publication d'un rapport du Lobby européen des femmes d'octobre 2017 dressant un panorama de l'ampleur de ces violences (Cartographie de l'état de violence en ligne contre les femmes « En finir avec l'impunité des violences faites aux femmes en ligne : une urgence pour les victimes », rapport n° 2017-11-16 du 16 novembre 2017). Ainsi, dans le monde entier, les femmes seraient 27 fois plus susceptibles d'être harcelées en ligne que les hommes. En Europe, 9 millions de filles ont déjà été victimes d'une forme de violences en ligne quand elles avaient 15 ans. Selon un autre rapport des Nations-Unies, 73 % de femmes ont déclaré avoir été victimes de violence sexuelle en ligne, et 18 % d'entre elles ont été confrontées à une grave violence sur internet.

Selon les données du ministère de l'éducation nationale figurant dans la dernière enquête « victimation et climat scolaire » de décembre 2017, 18 % des collégiens déclarent avoir subi au moins une atteinte via les réseaux sociaux ou

par téléphone portable (usurpation d'identité, vidéos humiliantes ou diffusion de rumeurs). Ils sont 11 % à déclarer avoir été insultés ou humiliés via ces nouvelles technologies (10 % pour les garçons et 13 % pour les filles). Pour 7 % des collégiens en classe de troisième, ce nombre d'atteintes peut s'apparenter à du cyber-harcèlement : 8 % pour les filles contre 6 % pour les garçons.

Au niveau européen, une enquête sur les violences faites aux femmes à l'initiative de l'agence des droits fondamentaux de l'Union européenne (FRA) en 2014 montrait que le cyberharcèlement au moyen de courriers électroniques, de SMS ou sur Internet « affecte avant tout les jeunes femmes ». Dans l'Union européenne, 4 % des femmes âgées de 18 à 29 ans, soit 1,5 million de femmes en ont été victimes au cours des 12 mois précédant l'entretien.

Les raids numériques

Le nouveau dispositif légal vise également à sanctionner les phénomènes de raids numériques. Ces raids sont majoritairement dirigés contre des femmes, prennent généralement la forme d'insultes liées au sexe et comprenant des références très crues et explicites. Ils comprennent parfois des menaces, notamment de viol ou de mort. Ils s'opèrent par le croisement de plusieurs médias sociaux ou plateformes. Ils surviennent à des niveaux inhabituellement élevés d'intensité et de fréquence (nombreuses menaces ou messages par jour ou même par heure) et sont perpétrés sur une durée inhabituelle (des mois ou même des années). Enfin, ils impliquent de nombreux agresseurs dans une démarche concertée et souvent coordonnée. Les raids numériques sont difficiles à réprimer dans la mesure où il faut pouvoir démontrer le caractère concerté des messages, chaque auteur n'étant parfois responsable que d'une seule publication. Le harcèlement naît de leur accumulation et de leur répétition.

L’outrage sexiste

Le nouveau dispositif légal a également tenu compte de l’outrage sexiste. Apparue dans l’espace médiatique dans les années 2010, la question du harcèlement dit « de rue » a fait l’objet de plusieurs publications, d’abord par des associations ou des collectifs, notamment au travers du documentaire Femmes de la rue de la belge Sofie Peteers, de la pétition « Stop aux violences sexuelles dans les transports en commun » ou de la campagne d’Osez le Féminisme « #TakeBackTheMetro ».

Enregistrement frauduleux de nom de domaine

Affaire UFE

L’Union des français de l’étranger (UFE) a obtenu le transfert du nom de domaine www.ufepaca.org enregistré par son ancien président. L’UFE est une Association reconnue d’utilité publique créée en 1927 dont l’objet social est de créer et de maintenir un contact étroit entre les Français de l’étranger et la France et de défendre les intérêts moraux et matériels des Français résidant ou ayant résidé hors de France. Elle est présente dans 100 pays avec 170 Représentations. Ces représentations sont majoritairement à l’étranger, mais il existe quelques représentations en France Métropolitaine, principalement pour les anciens expatriés et en particulier en

Région PACA.

Dépôt frauduleux de nom de domaine

C’est précisément sur l’ajout d’une entité géographique à un nom de domaine incluant une marque déposée, que s’est prononcée la juridiction. L’ancien président de l’Association UFE PACA, avait réservé, à son nom, le nom de domaine www.ufepaca.org auprès d’un registar dans l’Etat d’Arizona aux USA. Il avait également déposé les statuts constitutifs de l’Association UNION DES FRANÇAIS ET EUROPÉENS EXPATRIES sous le signe UFE PACA. Il avait également enregistré un second nom de domaine ufee.eu pour le compte de l’entreprise dont il était le gérant. Enfin, il avait déposé à son nom personnel auprès de l’INPI la marque française verbale UFE PACA.

Action en contrefaçon de marque de l’UFE

Selon acte d’huissier, l’UFE a fait assigner son ancien président devant le TGI en contrefaçon de marque, dépôt frauduleux et transfert à son profit de la marque UFE PACA, radiation des deux noms de domaines ufepaca.org et ufe.eu et concurrence déloyale. Le dépôt frauduleux de la marque UFE PACA a été retenu. Aux termes de l’article 712-6 du code de la propriété intellectuelle, si un enregistrement a été demandé soit en fraude des droits d’un tiers, soit en violation d’une obligation légale, ou conventionnelle, la personne qui estime avoir un droit sur la marque, peut revendiquer sa propriété en justice. A moins que le déposant soit de mauvaise foi, l’action en revendication se prescrit par cinq ans à compter de la publication de la demande d’enregistrement. En déposant, en son nom personnel, dans un contexte conflictuel avec l’Association UFE, en toute connaissance de cause, la marque

UFE PACA en vue d'entraver l'activité de cette dernière a fait un dépôt frauduleux de marque.

Le dépôt du nom de domaine ufepaca.org enregistré sous un nom personnel sur un registrar dans l'Etat d'Arizona aux USA occultant le nom du déposant, a été jugé contrefaisant. Au sens de l'article L713-3 du Code de la propriété intellectuelle « Sont interdits, sauf autorisation du propriétaire, s'il peut en résulter un risque de confusion dans l'esprit du public : a) La reproduction, l'usage ou l'apposition d'une marque, ainsi que l'usage d'une marque reproduite, pour des produits ou services similaires à ceux désignés dans l'enregistrement ; b) L'imitation d'une marque et l'usage d'une marque imitée, pour des produits ou services identiques ou similaires à ceux désignés dans l'enregistrement. ». De surcroît, il existait entre les noms de domaine en présence, un très fort risque de confusion (identité et similarité des produits et services).

Télécharger la Décision

Télécharger

Vendre un Contrat sur cette thématique

Vous disposez d'un modèle de document juridique sur cette thématique ? Complétez vos revenus en le vendant sur Uplex.fr, la 1ère plateforme de France en modèles de contrats professionnels

Poser une Question

Posez une Question Juridique sur cette thématique, la rédaction ou un abonné vous apportera une réponse en moins de 48h.

E-réputation | Surveillance de marques

Surveillez et analysez la réputation d'une **Marque** (la vôtre ou celle d'un concurrent), d'une Personne publique (homme

politique, acteur, sportif …) sur tous les réseaux sociaux (Twitter, Facebook …). Testez gratuitement notre plateforme de Surveillance de Marque et de *Réputation numérique*.

Paramétrer une Alerte

Paramétrez une alerte de Jurisprudence sur ce thème pour être informé par email lorsqu'une décision est rendue sur ce thème