SOMMAIRE

DATA / DONNÉES PERSONNELLES	
Les données, une composante du patrimoine informationnel de l'entreprise Cass. crim., 20 mai 2015, n°14-81.336 ; Cass. com., 25 juin 2013, n°12-17.037, FS-PBI	p. 2
Le Conseil d'Etat se prononce sur la conservation des données de connexion à des fins de sauvegarde de la sécurité nationale Conseil d'Etat, Chambre contentieuse, 21 avril 2021, N°393099	p. 3
La Commission européenne apporte des éclaircissements concernant les transferts de données personnelles vers le Royaume Uni Projet de de deux décisions d'adéquation relatives aux transferts des données à caractère personnel vers le Royaume-Uni	p. 4
PROPRIÉTÉ INTELLECTUELLE	
La cour d'appel de Paris apporte des précisions sur le régime applicable en matière de violation de licence de logiciel CA Paris, 19 mars 2021, n°19/17493	p. 5
CONTENUS ILLICITES / E-RÉPUTATION	
IKEA France, le procès d'une surveillance à échelle industrielle par la collecte illicite de données à caractère personnel Délibéré prévu le 15 juin 2021 (Tribunal correctionnel de Versailles)	p. 6
Mention de condamnations pénales sur internet et atteinte à la vie privée du condamné Cass. civ. 1ère, 17 février 2021, n°19-24.780	p. 7
STARTUP & LEGALTECHS / TENDANCES	
Publication d'un décret relatif à l'utilisation de la vidéo intelligente pour mesurer le port du masque dans les transports en commun Décret n°021-269 du 10 mars 2021 relatif au recours à la vidéo intelligente pour mesurer le taux de port de masque dans les transports	p. 9
ACTUALITÉ NUMÉRIQUE	p. 11

PARIS - NANTES - LYON
MONTPELLIER - LILLE

Bureaux intégrés

AIX-EN-PROVENCE
BORDEAUX
CLERMONT-FERRAND
LE HAVRE - MARSEILLE - METZ
NANCY - NICE - ROUEN

Réseau SIMON Avocats

ALGÉRIE - ARGENTINE
ARMÉNIE - AZERBAÏDJAN
BAHAMAS - BAHREÏN
BANGLADESH - BELGIQUE
BIRMANIE - BOLIVIE - BRÉSIL
BULGARIE - CAMBODGE
CAMEROUN - CHILI - CHINE
CHYPRE - COLOMBIE
COREE DU SUD - COSTA RICA
CÔTE D'IVOIRE - ÉGYPTE
EL SALVADOR
ÉMIRATS ARABES UNIS
ESTONIE - ÉTATS-UNIS
GUATEMALA - HONDURAS
HONGRIE - ÎLE MAURICE
ÎLES VIERGES BRITANNIQUES
INDE - INDONÉSIE - IRAN
ITALIE - KAZAKHSTAN
KOWEÏT - LUXEMBOURG
MADAGASCAR - MALTE
MAROC - MEXIQUE - NICARAGUA
OMAN - PANAMA - PARAGUAY
PÉROU - PORTUGAL - QATAR
RD CONGO - RÉPUBLIQUE DOMINICAINE - SENEGAL
SINGAPOUR - SUISSE - THAÏLANDE
TUNISIE - URUGUAY
VENEZUELA - VIETNAM
ZIMBABWE

Conventions transnationales

www.simonassocies.com
www.lettredunumerique.com

DATA / DONNÉES PERSONNELLES

Les données, une composante du patrimoine informationnel de l'entreprise
Cass. crim., 20 mai 2015, n°14-81.336 ;
Cass. com., 25 juin 2013, n°12-17.037, FS-PBI

Ce qu'il faut retenir :

Partant du postulat que le patrimoine informationnel correspond à l'ensemble des informations – au sens large – que possède une personne morale, nous pouvons nous interroger sur l'organisation et la méthode qui vont permettre de faire rentrer ces informations dans le patrimoine de l'entreprise.

Ainsi, parmi ces informations, nous trouvons les données qui entrent dans le champ du patrimoine informationnel dès lors qu'elles sont exploitées et source de valeur pour la personne morale qui en dispose, ce que la jurisprudence a reconnu en lui conférant un statut juridique particulier.

Pour approfondir :

Pour leur conférer la qualité de patrimoine informationnel au sein de l'entreprise, les données doivent faire l'objet d'une protection juridique appropriée (1) tout en s'assurant que ces mêmes données ne représentent pas un risque pour l'entreprise (2). Deux actions que nous proposons de voir successivement.

1) La protection juridique des données

Les données, enjeu du siècle, qu'elles soient publiques, privées ou personnelles, doivent être protégées. Pour cela les données peuvent être protégées par :

- **Le droit d'auteur** en protégeant la structure ou l'agencement de la base de données sous condition de l'originalité (article L.112-3 du Code de la Propriété intellectuelle) ;

- **Le droit *sui generis* des bases de données** qui a été codifié au Titre IV du Livre III du Code de la Propriété intellectuelle qui est intégralement consacré aux Droits des producteurs de bases de données. Ce qui importe c'est que le producteur souhaitant bénéficier de la protection de ses données démontre qu'il est celui qui a investi dans la constitution de la base et que cet investissement est financier, matériel ou humain, qu'il est substantiel et qu'il porte sur la constitution, la vérification et/ou la présentation de la base ;

- **Le droit du secret des affaires** (article L.151-1 du Code de commerce) dès lors que ces données établissent une information secrète avec une valeur commerciale du fait de ce caractère secret.

C'est en établissant cette protection de ces données que l'entreprise va la faire rentrer dans son patrimoine informationnel, en mesurer non seulement sa valeur mais aussi les risques qu'elles peuvent lui engendrer.

2) Les risques à identifier en cas de cession de l'entreprise

Les risques liés aux données composant le patrimoine informationnel de l'entreprise relèvent principalement de leur conformité au Règlement Général sur la Protection de la Donnée (RGPD) qui encadre strictement l'utilisation qui en est faite.

Le non-respect de cette règlementation peut avoir de graves conséquences en cas de cession de l'entreprise. D'abord le cessionnaire s'expose aux risques inhérents à une non-conformité :
- Impossibilité d'exploiter les données,
- Amende administrative,
- Sanction pénale ;
- Risque réputationnel.

Ensuite, la cession peut être annulée purement et simplement. Ainsi, la connaissance par le cessionnaire du niveau de conformité est essentielle pour apprécier le niveau de risque et, partant, tenter de s'en prémunir.

Dès lors qu'il s'agit d'information, il est important de s'assurer que ces données peuvent être collectées. Dans le cas contraire, ces données deviennent une source de risque, car elles ne sont plus exploitables et elles peuvent engendrer un risque pénal. Ainsi des pratiques relatives à l'intelligence économique, qui sont légales voire aujourd'hui favorisées par les gouvernements, peuvent être interprétées comme étant de l'espionnage industriel entre Etats.

Au vu de la place de plus en plus importante que prennent les informations, et par voie de conséquence les données, dans le patrimoine informationnel de l'entreprise, il est important de bien établir leur protection pour bien mesurer les risques qu'elles peuvent engendrer en plus de la valeur que cette protection juridique va leur conférer.

A rapprocher : ***DSI – Comment gérer le patrimoine informationnel de l'entreprise ?*** **(IT Social, 2 mars 2016)** ; **Protection du patrimoine informationnel (2007, FedISA – CIGREF)** ; **Cass. crim., 20 mai 2015, n°14-81.336** (une personne a téléchargé des fichiers informatiques de données et les a diffusés à des tiers « *sans le consentement de leur propriétaire* ». Il est alors reconnu qu'une donnée peut être la chose d'autrui.) ; **Cass. com., 25 juin 2013, n°12-17.037, FS-PBI** (annulation d'une cession d'actifs [fichiers informatiques contenant des données personnelles] pour absence de déclaration à la CNIL sous l'empire de la Loi Informatique et libertés.)

Le Conseil d'Etat se prononce sur la conservation des données de connexion à des fins de sauvegarde de la sécurité nationale

Conseil d'Etat, Chambre contentieuse, 21 avril 2021, N°393099

Ce qu'il faut retenir :

Dans une décision en date du 21 avril 2021, le Conseil d'Etat s'est prononcé sur la conformité du droit français au droit européen en matière de conservation des données de connexion par les fournisseurs de services de communications électroniques.

Pour approfondir :

Aux termes d'une décision en date du 21 avril 2021, le Conseil d'Etat a estimé que la conservation généralisée des données de connexion par les fournisseurs de services de communications électroniques se justifiait dans le cadre de la lutte actuelle pour la sauvegarde de la sécurité nationale. En effet, le droit français impose à ces opérateurs de conserver les données de connexion des utilisateurs pendant une durée d'un an en vue de leur exploitation par les services de renseignement.

Le Conseil d'Etat énonce notamment « *[qu'à] la date de la présente décision, l'état des menaces pesant sur la sécurité nationale (…) justifie légalement que soit imposée aux opérateurs la conservation générale et indifférenciée des données de connexion.* »

Soulignons que les données de connexion se distinguent du contenu même des communications électroniques et portent sur plusieurs catégories de données parmi lesquelles les données d'identification de l'utilisateur de la communication, les données de trafic et les données de localisation.

Par cette décision, le Conseil d'Etat procède à un examen de la conformité du droit français à la réglementation européenne, faisant ainsi suite aux arrêts remarqués de la Cour de Justice de l'Union Européenne du 6 octobre 2020.

En effet, alors saisie par le Conseil d'Etat de plusieurs questions préjudicielles, la Haute juridiction européenne s'était opposée à la conservation généralisée et indifférenciée des données de connexion par les fournisseurs de services de communications électroniques et à leur transmission aux autorités nationales de sécurité et de renseignement.

La Cour de Justice de l'Union Européenne avait alors rappelé le principe de confidentialité des communications électroniques et des données de trafic y afférentes tel qu'énoncé par la Directive 2002/58/CE du 12 juillet 2002 dite « *Vie privée et communications électroniques* » (ci-après « la Directive »).

En effet, l'article 5 de la Directive consacre le principe de confidentialité tant des communications électroniques que des données relatives au trafic y afférentes, et l'interdiction à toute autre personne autre que les utilisateurs de stocker ces communications et données, sans leur consentement. Or, l'article 15 de cette Directive offre la possibilité aux Etats membres de limiter la portée de cette interdiction lorsque la mesure est « *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* ».

Dans la décision du 21 avril 2021, le Conseil d'Etat estime ainsi que l'encadrement de la conservation des données par le droit européen ne doit pas remettre en cause les exigences constitutionnelles de préservation de la sécurité nationale. En effet, il est énoncé que « *tout en consacrant l'existence d'un ordre juridique de l'Union européenne intégré à l'ordre juridique interne (…) l'article 88-1 [de la Constitution] confirme la place de la Constitution au sommet de ce dernier.* » Dès lors, les interprétations de la Cour de Justice de l'Union Européenne ne doivent pas mettre en péril les exigences constitutionnelles françaises.

Le Conseil d'Etat rappelle les exigences de sauvegarde des intérêts fondamentaux de la Nation, de prévention des atteintes à l'ordre public, de lutte contre le terrorisme ou encore de recherche des auteurs d'infractions pénales et souligne qu'elles constituent des objectifs de valeur constitutionnelle. Dans ce contexte, le Conseil d'Etat énonce que ces exigences « *qui s'appliquent à des domaines relevant exclusivement ou essentiellement de la compétence des Etats membres en vertu des traités constitutifs de l'Union, ne sauraient être regardées comme bénéficiant, en droit de l'Union, d'une protection équivalente à celle que garantit la Constitution.* »

Le Conseil d'Etat impose cependant au gouvernement français de procéder à un examen périodique de l'existence de menace sur la sécurité nationale, justifiant ici le recours à une conservation généralisée et indifférenciée des données de connexion. Le gouvernement est invité à modifier le cadre réglementaire actuel, dans un délai de six mois, afin d'y intégrer cette nouvelle exigence.

En outre, si la CJUE avait admis l'hypothèse d'une conservation ciblée des données dans des zones à risques, le Conseil d'Etat estime que cette option est techniquement peu réalisable et « *présenterait un intérêt opérationnel peu certain* ».

Soulignons que le Conseil d'Etat estime, concernant l'exploitation des données à des fins de renseignement, que le contrôle préalable de la Commission Nationale de Contrôle des Techniques de Renseignement (CNCTR) n'est pas suffisant. Le gouvernement est donc invité à modifier le cadre réglementaire actuel pour conférer à l'avis préalable de la CNCTR un caractère contraignant.

Enfin, il semble intéressant de noter que la Cour constitutionnelle belge s'est récemment illustrée par une position opposée à celle du Conseil d'Etat. La Cour constitutionnelle de Belgique a en effet, dans une décision en date du 22 avril 2021, annulé les dispositions de la loi belge imposant une conservation généralisée et indifférenciée des données de connexion, estimant que « *l'obligation de conservation des données relatives aux communications électroniques doit être l'exception, et non la règle.* »

A rapprocher : Conseil d'Etat, Communiqué de presse, 21 avril 2021, « *Données de connexion : le Conseil d'État concilie le respect du droit de l'Union européenne et l'efficacité de la lutte contre le terrorisme et la criminalité* » ; Cour constitutionnelle belge, 22 avril 2021, n°57/2021 ; Cour de Justice de l'Union Européenne, 6 octobre 2020, Affaire C-623/17 *Privacy International* et les affaires jointes C-511/18 *La Quadrature du Net e.a.* et C-512/18, *French Data Network e.a.*, ainsi que C-520/18 *Ordre des barreaux francophones et germanophone e.a.*

La Commission européenne apporte des éclaircissements concernant les transferts de données personnelles vers le Royaume Uni

Projet de de deux décisions d'adéquation relatives aux transferts des données à caractère personnel vers le Royaume-Uni

Ce qu'il faut retenir :

La Commission européenne a annoncé avoir engagé des démarches pour autoriser de façon générale les transferts de données à caractère personnel vers le Royaume Uni en publiant le 19 février 2021 deux projets de décisions dites « d'adéquation ».

Pour approfondir :

Par un accord de commerce et de coopération (« ACC ») en date du 24 décembre 2020, le Royaume-Uni et l'Union Européenne se sont entendus sur l'application transitoire du règlement européen sur la protection des données (« RGPD ») pendant une durée supplémentaire de six mois, jusqu'au 1er juillet 2021.

A l'issue de cette période, le sort des transferts de données à caractère personnel effectués vers le Royaume-Uni demeure pourtant incertain et, sans décision de la Commission européenne, de tels flux seront considérés comme des transferts vers un pays tiers.

Aux termes de l'article 45 alinéa 1er du RGPD, « *un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale peut avoir lieu lorsque la Commission a constaté par voie de décision que le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou l'organisation internationale en question assure un niveau de protection adéquat. Un tel transfert ne nécessite pas d'autorisation spécifique.* »

Ce mécanisme permet en effet la réalisation de transferts de données à caractère personnel vers des pays tiers, lorsque ces derniers garantissent un niveau de protection adéquat à travers leur droit national, à l'issue d'une procédure de décision d'adéquation initiée par la Commission européenne.

Dans ce contexte, la Commission européenne a annoncé le 19 février 2021 avoir engagé des démarches devant aboutir à l'adoption de deux décisions d'adéquation relatives aux transferts des données à caractère personnel vers le Royaume-Uni. Si l'une de ces décisions d'adéquation entre dans le cadre du Règlement européen pour la protection des données, la seconde est relative à la directive relative à la protection des données dans le cadre répressif.

Ces deux projets signifient que la Commission Européenne a considéré que la législation nationale du Royaume-Uni garantissait un niveau de protection substantiellement équivalent à celui offert par le RGPD.

Une fois publiés, ces projets de décision seront examinés par le Comité européen de la protection des données (« CEPD ») puis par un comité composé de représentants des états membres de l'Union européenne. A l'issue de chacune de ces étapes, les décisions d'adéquation pourront être adoptées dans leur version définitive.

Il doit être noté que ces décisions d'adéquation ne sont valides que pendant une période de quatre ans à compter de leur adoption, période à l'issue de laquelle la Commission européenne procèdera à une réévaluation afin de prendre en compte les évolutions nationales pertinentes, tant législatives que jurisprudentielles.

En outre, les transferts de données réalisés depuis le Royaume-Uni vers l'Union européenne sont quant à eux soumis à la législation britannique. Le Royaume-Uni a considéré à cet effet que l'Union européenne présentait un niveau de protection adéquat et que ces transferts pouvaient être réalisés librement.

Cette démarche illustre la volonté de maintenir les transferts de données existants entre le Royaume Uni et l'Union européenne et leur coopération en matière de lutte contre la criminalité.

A rapprocher : Communiqué de presse de la Commission européenne, « *Protection des données : la Commission européenne engage un processus concernant les flux de données à caractère personnel vers le Royaume Uni* », 19 février 2021 ; Accord de commerce et de coopération du 24 décembre 2020 entre l'Union européenne et la Communauté Européenne de l'énergie atomique, d'une part, et le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, d'autre part ; Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ; Directive (UE) 2016/680 du parlement européen et du conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins répressives

PROPRIÉTÉ INTELLECTUELLE

La cour d'appel de Paris apporte des précisions sur le régime applicable en matière de violation de licence de logiciel

CA Paris, 19 mars 2021, n°19/17493

Ce qu'il faut retenir :

La cour d'appel de Paris a, dans un arrêt du 19 mars 2021, considéré que la violation d'un contrat de licence de logiciel ne relevait pas de la responsabilité délictuelle mais de la responsabilité contractuelle.

Pour approfondir :

Par un arrêt en date du 19 mars 2021, la cour d'appel de Paris a exclu le régime de la contrefaçon au profit de celui de la responsabilité contractuelle en matière de violation d'un contrat de licence de logiciel.

Illustratif du principe de droit civil de non-cumul des responsabilités contractuelle et délictuelle, l'arrêt commenté apporte des éclaircissements sur les conséquences de ce principe en matière de violation d'un contrat de licence de programme d'ordinateur.

Dans le contexte d'espèce, la responsabilité délictuelle a été écartée puisque le demandeur s'appuyait, pour fonder son action en contrefaçon, sur une violation par son licencié de son contrat de licence GNU GLP v2. Le titulaire du droit reprochait à son licencié d'avoir encapsulé ledit logiciel dans un nouveau logiciel afin de le commercialiser.

La cour d'appel a estimé qu'était irrecevable l'action du titulaire des droits qui ne fonde ses demandes que sur le terrain délictuel de la contrefaçon en s'appuyant sur une violation de son contrat de licence.

Dès lors, aux termes de cet arrêt, si le fait générateur résulte d'un acte de contrefaçon, l'action doit être menée sur le fondement de la responsabilité délictuelle et si le fait générateur résulte d'un manquement contractuel, alors l'action doit être menée sur le terrain de la responsabilité contractuelle.

Il doit être noté que cet arrêt se place dans un contexte jurisprudentiel particulièrement mouvant. En effet, la cour d'appel de Paris avait posé, par un arrêt en date du 16 octobre 2018, une question préjudicielle à la Cour de Justice de l'Union Européenne (ci-après « CJUE ») aux fins de connaître le régime applicable à la violation du périmètre des droits concédés sur un logiciel.

La CJUE s'était alors prononcée dans un arrêt du 18 décembre 2019 sur cette question épineuse, sans pour autant la trancher définitivement. La Haute juridiction européenne avait estimé que la violation d'une clause d'un contrat de licence de logiciel relevait de la notion d'atteinte aux droits de propriété intellectuelle, au sens de la directive 2004/48/CE et que le titulaire des droits devait pouvoir bénéficier des garanties prévues par cette directive.

Néanmoins, la CJUE avait précisé que « *le législateur national [restait] libre de fixer les modalités concrètes de protection desdits droits et de définir, notamment, la nature, contractuelle ou délictuelle, de l'action dont le titulaire de ceux-ci dispose, en cas de violation de ses droits de propriété intellectuelle, à l'encontre d'un programme d'ordinateur.* »

La cour d'appel de Paris a donc fait usage de la marge de manœuvres offerte par la Haute juridiction européenne et opté pour l'exclusion du régime de la responsabilité délictuelle au profit de celui de la responsabilité contractuelle en matière de violation d'une licence de logiciel.

Ce positionnement souffre cependant de sa rigidité puisqu'il a vocation à priver le titulaire des droits des mesures protectrices prévues par le Code de propriété intellectuelle. La Cour de Justice de l'Union Européenne avait pourtant, dans son arrêt du 18 décembre 2019, rappelé l'importance du bénéfice par le titulaire des droits des garanties offertes par la Directive 2004/48/CE.

A rapprocher : CA Paris, 19 mars 2021, n°19/17493 ; CJUE, 18 décembre 2019, affaire n°C-666/18

CONTENUS ILLICITES / E-RÉPUTATION

IKEA France, le procès d'une surveillance à échelle industrielle par la collecte illicite de données à caractère personnel
Délibéré prévu le 15 juin 2021
(Tribunal correctionnel de Versailles)

Ce qu'il faut retenir :

Après 8 ans d'enquête, quinze dirigeants de Ikea France – et notamment son Directeur de la sécurité – ont fait l'objet d'une ordonnance de renvoi devant le tribunal correctionnel de Versailles pour « *collecte de données à caractère personnel dans un fichier par un moyen frauduleux* », « *détournement de la finalité d'un traitement de données à caractère personnel* », « *divulgation illégale volontaire de données à caractère personnel* », « *violation du secret professionnel* ». La particularité de ce procès qui s'est ouvert en mars 2021 est l'importance accordée à la protection des données personnelles au vu des faits rapportés.

Pour approfondir :

Débuté le 22 mars 2021 devant le tribunal correctionnel de Versailles, le procès contre le géant suédois de l'ameublement aura duré deux semaines et s'est achevé le 1er avril 2021 par les plaidoiries du défendeur. Le délibéré est attendu pour le 15 juin 2021.

En substance, Ikea est accusée d'avoir mis en place un système illégal de surveillance généralisée de ses employés, de candidats, et de clients entre 2009 et 2012. Ikea aurait ainsi eu recours à une société d'investigations privées pour obtenir des informations sur les antécédents judiciaires ou le patrimoine de ses employés. La société d'investigations aurait notamment eu accès à des fichiers de police pour remplir sa mission.

Par son ordonnance, le juge d'instruction a renvoyé ces 15 dirigeants devant le tribunal correctionnel de Versailles pour pas moins de 81 chefs d'accusation et notamment la « *collecte de données à caractère personnel, par un moyen frauduleux, déloyal ou illicite* » et le détournement de finalité.

Au vu des faits allégués, la problématique des données personnelles a été au centre des débats. Cette affaire rappelle ce qui est interdit en matière de traitement de données personnelles.

Ainsi nous pouvons relever :

- Au niveau de l'information : les personnes concernées – c'est-à-dire les salariés d'Ikea, des clients, des candidats à l'embauche – n'ont pas été correctement informées sur ce traitement de leurs données personnelles. La collecte en elle-même apparaît donc bien illicite au sens de la réglementation applicable à la protection des données personnelles.
- S'agissant de la minimisation, la question se pose de savoir si les données traitées, donc les données concernant des informations financières ou des condamnations, étaient effectivement nécessaires au traitement envisagé.
- Par ailleurs, un tel traitement, qui porte nécessairement atteinte aux droits des personnes concernées, devrait faire l'objet d'une analyse d'impact préalable.

Mais en réalité, les débats qui ont animé pendant deux semaines le tribunal correctionnel de Versailles se sont concentrés sur la connaissance des dirigeants d'Ikea de ce système de surveillance et ont survolé la question du respect de la protection des données personnelles.

Il faut dire qu'au moment des faits incriminés, entre 2009 et 2012, le Règlement Européen sur la Protection des Données, le RGPD, n'était pas encore entré en application, cette dernière datant du 25 mai 2018. En revanche, la loi informatique et libertés qui date de 1978 était quant à elle déjà en vigueur, comme le rappelle d'ailleurs la présidente du tribunal. Or, cette loi comportait déjà un grand nombre des principes édictés par le RGPD.

Quoi qu'il en soit, cette problématique de la collecte illicite de données à caractère personnel pour établir une surveillance quasi industrielle méritait d'être traitée et ainsi l'importance du respect de la mise en conformité au RGPD dans les entreprises.

Il faudra donc attendre le résultat du délibéré du tribunal correctionnel de Versailles prévu pour le 15 juin pour découvrir si la problématique des données personnelles sera remise à la place centrale qu'elle mérite dans ce procès.

A rapprocher : *Espionnage chez Ikea : le parquet confirme un système « à grande échelle »* (Le Monde, 14 mars 2018) ; *Espionnage à Ikea : la procureure dénonce la lâcheté de la direction et veut une « peine exemplaire »* (Libération, 30 mars 2021)

Mention de condamnations pénales sur internet et atteinte à la vie privée du condamné
Cass. civ. 1ère, 17 février 2021, n°19-24.780

Ce qu'il faut retenir :

Faute de s'inscrire dans un débat d'intérêt général, la mention de condamnations pénales sur un site internet accessible à tous porte atteinte au droit au respect de la vie privée du condamné.

Pour approfondir :

En l'espèce, le dirigeant d'une société spécialisée dans la supplémentation nutritionnelle a été déclaré coupable d'infractions pénales commises dans l'exercice de son activité professionnelle. Les premières condamnations, prononcées par un arrêt devenu définitif, concernaient des faits d'exercice illégal de la pharmacie, de commercialisation de médicaments sans autorisation de mise sur le marché et d'infraction à la règlementation de la publicité des médicaments. Les secondes, prononcées par un second arrêt des chefs de fraude fiscale et d'omission d'écritures en comptabilité, ont quant à elles été amnistiées par suite d'une décision de la Cour de révision et de réexamen des condamnations pénales le 11 avril 2019.

L'intéressé a découvert que les deux affaires et l'ensemble des condamnations pénales précitées, y compris celles amnistiées, étaient recensées sur le site internet **www.psiram.com**. Ce site, dédié selon sa page d'accueil aux « *croyances irrationnelles* », invitait par ailleurs les visiteurs à consulter l'avis nécrologique de son père sur le site **www.dansnoscoeurs.fr**.

L'intéressé a donc assigné l'auteur de la page litigieuse sur le fondement de l'article 9 du Code civil, en suppression de cette page et en indemnisation du préjudice subi.

S'agissant des condamnations pénales, la Cour d'appel de Paris a écarté le grief d'atteinte à la vie privée, aux motifs que, d'une part, les condamnations litigieuses concernaient son activité professionnelle et avaient été rendues publiques par les juridictions répressives et, d'autre part, que l'intéressé ne pouvait se prévaloir de l'ancienneté des faits ou d'un droit à l'oubli dès lors qu'à la date de la publication de la page litigieuse, les condamnations pénales n'avaient pas encore été amnistiées par la Cour de révision.

Cette position est censurée par la Cour de cassation au visa des articles 8 et 10 de la Convention EDH et de l'article 9 du Code civil.

De façon classique, cette dernière rappelle *tout d'abord* ce que recouvrent respectivement le droit au respect de la vie privée et le droit à la liberté d'expression.

- A propos du droit au respect de la vie privée (protégé par l'article 8 de la Convention EDH et l'article 9 du Code civil), la Cour de cassation indique que si ce droit ne peut être invoqué pour se plaindre d'une atteinte à la réputation lorsqu'elle résulte de manière prévisible des propres actions de l'intéressé (telle une infraction pénale), la mention dans une publication, des condamnations pénales dont il a fait l'objet, y compris à l'occasion de son activité professionnelle, porte atteinte au droit au respect de sa vie privée (***CEDH, 28 juin 2018, M.L. et W.W. c/ Allemagne, n°60798/10 et 65599/10***).

- A propos de la liberté d'expression (telle que protégée par l'article 10 de la Convention EDH), la Cour précise que si toute personne a le droit à la liberté d'expression, son exercice peut être soumis à certaines restrictions ou sanctions prévues par la loi.

La Cour de cassation rappelle *ensuite* qu'en cas de conflit entre deux droits ayant la même valeur normative, il convient de procéder à « *une mise en balance* » afin de parvenir à un juste équilibre entre ces deux droits (***Cass. civ. 1ère, 21 mars 2018, n°16-28.741 ; Cass. ass. plén., 25 oct. 2019, n°17-86.605***) et ce, conformément à la jurisprudence de la Cour européenne (***CEDH, 23 juillet 2009, Hachette Filipacchi Associés, n°12268/03***). Afin de déterminer si l'atteinte à la vie privée est caractérisée, il appartient alors au juge de concilier et mettre en balance les droits invoqués, en fonction des intérêts en jeu et, par suite, de privilégier la solution la plus protectrice de l'intérêt le plus légitime. Pour ce faire, le juge doit procéder « *de façon concrète* » et minutieuse à l'examen de chacun des critères suivants (***Cass. civ. 1ère, 21 mars 2018, n°16-28.741***) : la notoriété de la personne visée, son comportement antérieur, l'objet, le contenu, la forme et les répercussions de la publication incriminée, mais aussi et surtout, la contribution de cette publication à un débat d'intérêt général (***CEDH, 10 novembre 2015, n°40454/07, Couderc et Hachette Filipacchi associés c/ France***).

Or, en l'espèce, la Cour de cassation relève que la Cour d'appel n'a pas recherché si l'article publié sur le site **www.psiram.com** s'inscrivait dans un débat d'intérêt général qui aurait justifié la reproduction des condamnations pénales de l'intéressé. Elle rappelle en effet que si le sujet à l'origine de l'article relève de l'intérêt général, encore faut-il par ailleurs que le contenu de l'article soit de nature à nourrir le débat public sur le sujet en question (***CEDH, 29 mars 2016, n°56925/08, Bédat c/ Suisse [GC]***) ; ce que la Cour d'appel a omis de vérifier.

Il résulte donc de cette décision que le fait que des condamnations pénales soient rendues publiques ne signifie pas qu'elles échappent nécessairement et automatiquement à la sphère protégée de la vie privée et qu'il convient, pour le déterminer, d'établir, d'une part, si la publication incriminée contribue ou non à un débat d'intérêt général et, d'autre part, si son contenu est de nature à nourrir le débat public sur le sujet.

La Cour de cassation s'inscrit ainsi dans la droite ligne de la jurisprudence européenne, laquelle n'hésite pas à rappeler l'importance de ce contrôle, notamment s'agissant de faits judiciaires et de mention de condamnations pénales dans la presse (***CEDH, 7 février 2012, Axel Springer c/ Allemagne, n°39954/08*** *: reconnaissant l'existence d'un débat d'intérêt général au regard de la notoriété de la victime, de la gravité de l'infraction, des circonstances de l'arrestation [en pleine Oktoberfest] ;* ***CEDH, 28 juin 2018, M.L. et W.W. c/ Allemagne, n°60798/10 et 65599/10*** *: de même au regard de la notoriété de la victime, de la large couverture médiatique de l'affaire, de la gravité du crime*).

La CNIL, consciente des risques d'atteintes à la vie privée en cas de diffusion de décisions de justice sur internet (« *open data judiciaire* ») avait d'ailleurs préconisé une occultation (terme qui englobe les procédés d'anonymisation et la pseudonymisation) des décisions de justice (***CNIL, Délibération 01-057 du 29 novembre 2001***). La loi pour une République numérique du 7 octobre 2016, puis la Loi de réforme de la justice du 23 mars 2019, ont par suite consacré ce principe pour toute décision de justice accessible au public. Ainsi, désormais, « *les noms et prénoms des personnes physiques mentionnées dans la décision, lorsqu'elles sont parties ou tiers, sont occultés préalablement à la mise à la disposition du public* », de même que tout élément permettant d'identifier les parties, les tiers, les magistrats et les membres du greffe « *lorsque sa divulgation est de nature à porter atteinte à la sécurité ou au respect de la vie privée de ces personnes ou de leur entourage* » (***COJ, art. L.113-1***).

S'agissant de l'avis nécrologique du père de l'intéressé, la Cour d'appel de Paris avait considéré que dans la mesure où le faire-part de décès avait été publié par la famille sur un site internet accessible à tous (ce que l'intéressé ne pouvait ignorer), celui-ci ne pouvait arguer d'une atteinte à sa vie privée. La Cour de cassation censure ce raisonnement. Elle rappelle classiquement que le fait que des informations soient déjà dans le domaine public ne les soustrait pas automatiquement à la protection de l'article 8 de la Convention, dès lors que l'intérêt à publier ces informations doit toujours être mis en balance avec des considérations liées à la vie privée. Elle en déduit donc en l'espèce que la seule circonstance que le faire-part ait été publié sur internet et soit ainsi accessible à tous, ne permet pas, à elle seule, d'écarter l'existence d'une violation du droit au respect de la vie privée de l'intéressé.

A rapprocher : CEDH, 28 juin 2018, *M.L. et W.W. c/ Allemagne*, n°60798/10 et 65599/10 ; Cass. civ. 1ère, 21 mars 2018, n°16-28.741 ; Cass. ass. plén., 25 oct. 2019, n°17-86.605 ; CEDH, 23 juillet 2009, *Hachette Filipacchi Associés*, n°12268/03 ; CEDH, 10 novembre 2015, n°40454/07, *Couderc et Hachette Filipacchi associés c/ France* ; CEDH, 29 mars 2016, n°56925/08, *Bédat c/ Suisse [GC]* ; CEDH, 7 février 2012, *Axel Springer c/ Allemagne*, n°39954/08 ; CNIL, Délibération 01-057 du 29 novembre 2001

STARTUP & LEGALTECHS / TENDANCES

Publication d'un décret relatif à l'utilisation de la vidéo intelligente pour mesurer le port du masque dans les transports en commun

Décret n°021-269 du 10 mars 2021 relatif au recours à la vidéo intelligente pour mesurer le taux de port de masque dans les transports

Ce qu'il faut retenir :

Dans le contexte de la crise sanitaire, les exploitants de services de transports public collectif ont été autorisés par un décret en date du 10 mars 2021 à mettre en place des dispositifs de vidéoprotection intelligente aux fins de mesurer le taux de port de masque.

Pour approfondir :

Depuis le 10 mars 2021, les exploitants de services de transports en commun peuvent recourir à des dispositifs de visionnage des images des voyageurs. Ces dispositifs sont destinés, dans le contexte sanitaire actuel, à mesurer le taux du port du masque, à produire des évaluations statistiques sur le respect de cette obligation et à adapter la sensibilisation du public.
Saisie pour avis, la CNIL avait considéré le 17 décembre 2020 que le déploiement de ce dispositif répondait à la nécessité pour le gouvernement de prendre toutes les mesures nécessaires pour protéger la population et poursuivait des objectifs de santé publique.

L'autorité de contrôle française avait alors indiqué qu'il pouvait être envisagé de limiter les droits des personnes concernées.

En effet, conformément à l'article 23 du Règlement (UE) 2016/679 sur la protection des données, le droit d'opposition des personnes concernées peut être limité « *lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir* » des objectifs importants d'intérêt public et notamment de santé publique.

L'autorité de contrôle française rappelait toutefois dans son avis que « *la préservation de l'anonymat dans l'espace public est une dimension essentielle pour l'exercice des [libertés individuelles] ; la captation et l'analyse systématiques de l'image des personnes dans ces espaces sont incontestablement porteuses de risques pour leurs droits et libertés fondamentaux* ».

En cas de limitation des droits des personnes concernées, il doit être noté le caractère impératif des garanties à apporter en matière de protection des données. En effet, les dispositifs de captation et d'analyse systématique des images des personnes sont par essence porteurs de risques et peuvent créer un sentiment de surveillance généralisée des citoyens.

Dans ce contexte, le décret précise que les images collectées ne font ni l'objet de stockage, ni l'objet d'une transmission à des tiers. Il doit également être noté que les images sont instantanément transformées en données anonymes afin d'établir le pourcentage de personnes portant effectivement un masque de protection.

En outre, le décret indique que les traitements ne portent que sur le nombre de personnes détectées et sur le pourcentage de personnes portant un masque, à l'exclusion de toute autre donnée permettant de classer ou de réidentifier les personnes. La CNIL avait par ailleurs estimé dans son avis que l'usage de caméras intelligentes n'avait pas vocation à traiter des données biométriques ou à constituer un dispositif de reconnaissance faciale.

Enfin, soulignons le caractère temporaire de cette mesure, dont le déploiement est limité à une durée maximale d'un an et dans le contexte de la crise sanitaire.

A rapprocher : Décret n°2021-269 du 10 mars 2021 relatif au recours à la vidéo intelligente pour mesurer le taux de port de masque dans les transports ; Délibération n°2020-136 du 17 décembre 2020 portant avis sur un projet de décret relatif au recours à la vidéo intelligente pour mesurer le taux de port de masque dans les transports

***

ACTUALITÉ NUMÉRIQUE SIMON ASSOCIÉS

VIDÉO / INTERVIEW

CHRONIQUE D'UNE MORT ANNONCÉE

Interview de Fabrice DEGROOTE, pour notre rubrique « Réflexions d'Experts »

Voir la vidéo

ÉVÉNEMENTS

7 ENTREPRISES SUR 10 PENSENT ÊTRE CONFORME AU RGPD, ET VOUS ?

Webinar organisé par Mission RGPD et Simon Associés le 25 mai 2021 à 11h00,
et coanimé par Thibaut VERGNE et Amira BOUNEDJOUM
En savoir plus - S'inscrire

RGPD 3 ANS APRÈS : BILAN ET RETOUR D'EXPÉRIENCE

Webinar organisé par Simon Associés le 25 mai 2021 à 17h00, et animé par Amira BOUNEDJOUM
En savoir plus - S'inscrire

NOUVEAUTÉ

MISSION RGPD ANNONCE LA NOUVELLE VERSION DE SON LOGICIEL

Les équipes ont mis l'accent sur l'expérience utilisateur avec comme objectif de rendre toujours plus accessible le RGPD.

En savoir plus