La Newsletter dédiée à la mise en conformité au RGPD

par @DerriennicParis

DERRIENNIC ASSOCIÉS

Conformité RGPD

#NewsDerriennicRGPD 17

Madame, Monsieur,

La période de rentrée nous a gratifiés d'un nombre conséquent de décisions et de publications en rapport avec la protection des données. Nous vous proposons ainsi une lettre RGPD composée des actualités suivantes :

- Bouton « J'aime » : un partage de responsabilité entre l'éditeur du site et Facebook ;
- Le RGPD bloque une mesure ordonnée sous le visa de l'article 145 ;
- « No-deal Brexit » : les conseils de la CNIL ;
- Nouvelles lignes directrices de la CNIL sur les cookies ;
- Zèle dans l'application du RGPD ;
- RGPD : refus de suppression d'une fiche Google My Business.

Nous vous en souhaitons une bonne lecture.

Bouton « J'aime » : un partage de responsabilité entre l'éditeur du site et Facebook

Par un très attendu arrêt du 29 juillet dernier (affaire C-40/17), la CJUE a tranché la question de la responsabilité en matière de données personnelle des gestionnaires de site internet insérant des boutons « J'aime ».

Les faits étaient simples : l'exploitant d'un site de vente en ligne, à l'instar de nombreux sites internet, a inséré un bouton « J'aime » sur son site permettant le transfert de données personnelles des visiteurs dudit site à FACEBOOK et ce, peu important que le visiteur clique ou non sur ledit bouton et/ou ait ou non un compte Facebook. Une association de consommateurs allemande a considéré que, par-là, le gestionnaire du site ne respecte pas la règlementation relative à la protection des données faute d'informer les personnes concernées d'un tel traitement et de recueillir leur consentement. Le gestionnaire du site considérait, quant à lui, ne pas avoir enfreint la réglementation notamment parce qu'il ignore les traitements des données qui sont transmises à FACEBOOK et n'a pas d'influence sur ceux-ci.

L'affaire a été portée devant les juridictions allemandes qui ont interrogé la CJUE sur la responsabilité d'un tel gestionnaire de site au regard de la Directive 95/46/CE sur la protection des données (abrogée par le RGPD) applicable alors aux faits.

Pour les juges européens, il convient de distinguer les traitements de données opérés via le module social « J'aime » selon deux catégories :

- d'une part, ceux effectués par FACEBOOK après transmission des données via le site et qui ne semblent pas pouvoir relever de la responsabilité du gestionnaire du site : en effet, a priori, le gestionnaire ne détermine ni les moyens ni les finalités de telles opérations ;
- d'autre part, ceux consistant en la collecte et la communication à FACEBOOK des données et qui semblent, quant à eux, relever d'une responsabilité conjointe du gestionnaire du site avec FACEBOOK si ces derniers déterminent bien conjointement les moyens et finalités de ces opérations.

S'il appartient à la juridiction du fond de faire les appréciations d'espèce pour confirmer ces points, la CJUE a précisé qu'il lui semble que l'insertion du bouton J'aime permet au gestionnaire du site d'optimiser ses actions publicitaires de sorte qu'il apparaît avoir accepté, à tout le moins implicitement, la collecte et la transmission de données de son site à FACEBOOK.

Le cas échéant, le gestionnaire est alors coresponsable de traitement de données des visiteurs de son site et a l'obligation de fournir les informations imposées par la règlementation au moment de la collecte de ces données (identité, finalité du traitement).

A noter que si l'arrêt de la CJUE a été rendu au visa de la Directive 95/46 CE, la solution pourrait tout à fait s'appliquer à l'ère du RGPD, lequel a repris les principes de la directive et même renforcé certaines obligations à ce titre (notamment en exigeant la conclusion d'un contrat entre coresponsables de traitement).

Quoiqu'il en soit, cet arrêt vient à nouveau préciser la responsabilité des exploitants de site internet qui utilisent des outils de réseaux sociaux (rappelons la coresponsabilité d'un gestionnaire d'une page fan Facebook retenue par la CJUE le 5 juin 2018).

L'application de cet arrêt par les tribunaux et cours locaux sera particulièrement intéressante à suivre…

Lien vers la publication :

http://curia.europa.eu/juris/document/document.jsf;jsessionid=161AB9A86105EC535FE6C7F192FC7028?text=&docid=216555&pageIndex=0&doclang=FR&mode=req&dir=&occ=first&part=1&cid=12946363

Le RGPD bloque une mesure ordonnée sous le visa de l'article 145

Le Président du Tribunal de grande instance de Paris, par une ordonnance du 2 août 2019, a débouté un producteur d'œuvres audiovisuelles de sa demande de communication des éléments d'identification détenus par Orange concernant les adresses IP des internautes à l'origine d'opérations de téléchargement massif de ses œuvres, faute pour le producteur de démontrer le caractère licite du traitement des adresses IP ainsi réalisé.

Mile High Distribution, société canadienne productrice d'œuvres audiovisuelles, a constaté la présence de ses œuvres sur des plateformes d'échange de fichiers en ligne où lesdites œuvres étaient distribuées sans son autorisation.

Cette société a fait appel à la société de droit allemand Media Protector afin que cette dernière collecte notamment les adresses IP des personnes ayant procédé au téléchargement des œuvres, ainsi que le nom des fournisseurs d'accès auxquels se rattachent les adresses IP identifiées.

Par la suite, la société Mile High Distribution a sollicité du juge des requêtes du TGI de Paris qu'il ordonne à Orange S.A. de communiquer l'identité, les adresses postales et toutes informations utiles à l'identification des personnes titulaires des adresses IP collectées par la société Media Protector.

Par une ordonnance du 8 avril 2019, le juge a fait droit à cette demande.

Orange S.A. a sollicité la rétractation de cette ordonnance.

Selon elle, la mesure d'identification sollicitée ne pouvait être légalement admissible que si la collecte des adresses IP des contrefacteurs présumés avait été effectuée légalement. Or, elle estimait que la société Mile High Distribution ne versait au débat aucun élément tangible permettant de s'assurer de la légalité du traitement de données personnelles des adresses IP qu'elle a pu collecter, ni ne justifiait de la légalité du traitement mis en œuvre par ses soins.

Le juge des référés, souscrivant à l'argumentation d'Orange S.A., a (i) considéré que le RGPD était applicable à la collecte des adresses IP et (ii) estimé que la société Mile High Distribution était responsable du traitement. Il lui incombait donc de :

- désigner un représentant au sein de l'UE ;
- tenir un registre des traitements, au sein duquel une fiche devait être consacrée au traitement de données objet du litige ;
- s'agissant d'une collecte « *à grande échelle* » (895 adresses IP), désigner un délégué à la protection des données ;
- garantir une sécurité appropriée des données ;
- prévoir un « encadrement juridique particulier », au regard du transfert de données à caractère personnel en dehors de l'Union européenne (de la France vers le Canada).

La société Mile High Distribution ne produisant aucun élément de nature à considérer qu'elle se serait conformée aux obligations précitées, n'a pas démontré le caractère licite du traitement de données à caractère personnel d'adresses IP qu'elle mettait en œuvre, ce qui constitue, selon le juge des référés, un empêchement légitime à l'application des dispositions de l'article 145 du Code de procédure civile.

La société Mile High Distribution a, en conséquence, été déboutée de sa demande de

communication des éléments d'identification détenus par Orange S.A. concernant les adresses IP précitées.

Lien vers l'ordonnance :

https://www.legalis.net/jurisprudences/tgi-de-paris-ordonnance-de-refere-du-2-aout-2019/

« No-deal Brexit » : les conseils de la CNIL

A supposer qu'aucun report de date n'intervienne et en l'absence de ratification d'un accord de retrait, le Royaume-Uni deviendra un pays tiers à l'Union européenne au 1er novembre 2019. Cela signifie que les transferts de données à destination de ce pays seront considérés comme des transferts de données hors de l'UE et de l'EEE. La CNIL a précisé, dans une publication du 10 septembre 2019, ses recommandations et les étapes à suivre pour se préparer à cet éventuel « No-deal Brexit ».

La CNIL rappelle qu'au 1er novembre 2019, le Royaume-Uni ne sera pas considéré comme un pays assurant au niveau de protection adéquat sur la base d'une décision d'adéquation. Les organismes devront en conséquence encadrer les transferts de données vers le Royaume-Uni, par exemple à l'aide des outils suivants :

- clauses contractuelles types ;
- clauses contractuelles spécifiques dites « ad-hoc » ;
- règles contraignantes d'entreprises (ou binding coprorate rules, BCR) ;
- codes de conduites et mécanisme de certification.

La CNIL ajoute qu'en cas de « *No-deal Brexit* », quel que soit le type d'organisme concerné, l'outil choisi pour encadrer le transfert de données vers le Royaume-Uni devra être mis en place et effectif à compter du 1er novembre 2019.

Elle rappelle également qu'en l'absence de garanties appropriées encadrant le transfert, ce dernier peut néanmoins être opéré sur la base de dérogations (cf. article 49 du RGPD). Toutefois, selon la CNIL, « *les responsables de traitement doivent s'efforcer de mettre en place des garanties appropriées et ne doivent recourir à ces exceptions qu'en l'absence de telles garanties* ».

Enfin, la CNIL indique également que « *pour les données personnelles envoyées depuis le Royaume-Uni vers l'Union Européenne, le gouvernement britannique a annoncé que la situation resterait inchangée et que la libre circulation des données vers l'UE serait permise sans besoin de garantie supplémentaire* ». Ainsi, les destinataires, dans l'UE, de données d'un responsable du traitement ou sous-traitant britannique n'auront, pour leur part, pas d'action à mener, si ce n'est se conformer aux dispositions du RGPD ou de « *tout autre cadre juridique spécifique applicable une fois les données reçues* ».

Lien vers la publication :

https://www.cnil.fr/fr/se-preparer-un-brexit-sans-accord-quelles-questions-quels-conseils-de-la-cnil

Nouvelles lignes directrices de la CNIL sur les cookies

Tenant compte de la nouvelle définition du consentement introduite par le RGPD, ainsi que des lignes directrices du CEPD sur le sujet, la CNIL a adopté de nouvelles lignes directrices, datées du 4 juillet 2019, relatives à l'application l'article 82 de la loi informatique et liberté aux opérations de lecture ou d'écriture dans le terminal d'un utilisateur.

1. La CNIL a adopté le 4 juillet 2019 de nouvelles lignes directrices sur les cookies, modifiant ainsi sa position quant à la façon de recueillir le consentement. Ces lignes directrices ont vocation à s'appliquer quels que soient les systèmes d'exploitation, les navigateurs ou les terminaux utilisés (y compris consoles de jeux vidéo, télévision connectée, véhicule connectée, assistant vocal, etc.).

Pour rappel, avant l'adoption de ces nouvelles lignes directrices, la CNIL recommandait de faire apparaitre un bandeau sur le site internet utilisant des cookies. Ce bandeau devait indiquer la finalité des cookies, ainsi que le fait que la poursuite de la navigation sur le site valait consentement à leur utilisation. Un lien vers une page permettant de paramétrer l'utilisation des cookies devait également apparaitre.

2. Dans ces nouvelles lignes directrices, la CNIL indique que le consentement, qui doit être conforme à la définition et aux conditions prévues aux articles 4 (11) et 7 du RGPD, doit, tout d'abord, demeurer libre. En conséquence, il « ne peut être valable que si la personne concernée est en mesure d'exercer valablement son choix et ne subit pas d'inconvénient majeurs en cas d'absence ou de retrait du consentement ». Ainsi, « la pratique qui consiste à bloquer l'accès à un site web ou à une application mobile pour qui ne consent pas à être suivi (« cookie walls ») n'est pas conforme au RGPD ».

Afin, ensuite, d'assurer le caractère spécifique du consentement, la personne concernée doit être en mesure de consentir « spécifiquement à chaque finalité ». Ainsi, « l'acceptation globale de conditions générales d'utilisation ne peut être une modalité valable de recueil du consentement, dans la mesure où celui-ci ne pourra être donné de manière distincte pour chaque finalité ».

Par ailleurs, afin d'assurer le caractère éclairé du consentement, l'information doit être rédigée en des termes « simples et compréhensibles par tous ». Elle doit en effet permettre aux utilisateurs d'être « parfaitement informés des différentes finalités des traceurs utilisés » et « l'utilisation d'une terminologie juridique ou technique trop complexe ne répond pas à l'exigence d'information préalable ». Cette information qui doit être complète, visible et mise en évidence au moment du recueil du consentement, doit informer les utilisateurs sur :

- l'identité du ou des responsables de traitement ;
- la finalité des opérations de lecture ou d'écriture des données ;
- l'existence du droit de retirer son consentement.

La CNIL ajoute que l'utilisateur doit pouvoir identifier l'ensemble des entités ayant recours à des traceurs avant de pouvoir y consentir. La liste de ces entités doit ainsi être mise à disposition de l'utilisateur « directement lors du recueil de son consentement ».

Enfin, afin d'assurer le caractère univoque du consentement, « le fait de continuer à naviguer sur un site web, d'utiliser une application mobile ou bien de faire défiler la page d'un site web ou d'une application mobile » ne s'analyse

pas comme « des actions positives claires assimilables à un consentement valable ». De même, l'utilisation de cases pré-cochées ne saurait être considérée comme un acte positif clair visant à donner son consentement.

3. La CNIL ajoute que les organismes exploitant des traceurs doivent « mettre en œuvre des mécanismes permettant de démontrer, à tout moment, qu'ils ont valablement recueilli le consentement des utilisateurs ».

Quant aux personnes ayant donné leur consentement à l'utilisation de traceurs, elles doivent être en mesure de le retirer à tout moment, ce qui implique la mise en œuvre de « solutions conviviales » permettant de retirer le consentement aussi facilement qu'il a été donné.

La CNIL considère encore que les paramétrages du navigateur ne peuvent, en l'état de la technique, permettre à l'utilisateur d'exprimer la manifestation d'un consentement valide. Les raisons avancées par la CNIL sont :

- un niveau insuffisant d'information préalable des personnes ;
- l'absence de distinction des cookies par finalité ;
- l'impossibilité d'exprimer un choix sur d'autres technologies que les cookies (telle que le fingerprint par exemple) à des fins de suivi de la navigation.

4. Ces lignes directrices seront suivies d'une nouvelle recommandation qui précisera les modalités pratiques du recueil du consentement. Cette recommandation définitive sera publiée au premier trimestre 2020.

Comme la CNIL l'a indiqué, une période d'adaptation, s'achevant six mois après la publication de la future recommandation, sera laissée aux acteurs afin de leur donner le temps d'intégrer les nouvelles règles.

Liens vers la délibération :
https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000038783337&categorieLien=id

Zèle dans l'application du RGPD

Par une ordonnance de référé rendue le 22 avril 2019, le Président du Tribunal de grande instance de Metz a qualifié de trouble manifestement illicite le refus, par un employeur, de transmettre les informations requises par un cabinet d'experts CHSCT intervenant dans le cadre d'une expertise « risque grave », l'employeur ayant motivé ce refus par l'absence de recueil du consentement des salariés concernés.

Le CHSCT de l'hôpital de Saint-Avold avait confié une mission d'analyse au cabinet d'expertise Syndex, « pour mettre en évidence les facteurs de la dégradation des conditions de travail sur la santé et la sécurité des personnels, notamment en termes de souffrance au travail ».

Le cabinet Syndex, qui souhaitait adresser à chaque salarié de l'entreprise un questionnaire, a sollicité l'employeur afin qu'il lui communique leur adresse postale.

L'employeur, qui jusqu'alors n'avait contesté ni le principe d'une expertise pour risque grave, ni la méthodologie du cabinet Syndex, s'est opposé à la demande de ce dernier, en indiquant « ne pas être autorisé, dans le cadre de la protection des données personnelles des salariés, à communiquer les adresses postales ». Il invoquait, à ce titre, la nécessité, selon lui, d'obtenir le consentement individuel de chaque salarié.

Le CHSCT a alors saisi le Président du Tribunal de grande instance de Metz en référé, afin qu'il ordonne à l'employeur de communiquer les informations requises par le cabinet Syndex, pour que ce dernier soit en mesure de mener à bien sa mission.

Après avoir rappelé que l'employeur était tenu de fournir au CHSCT les informations nécessaires à l'exercice de sa mission, au titre de l'article L. 4614-13 du Code du travail, le Président du Tribunal de grande instance de Metz a considéré que l'employeur était responsable de la communication des adresses, ce qui constituait un premier traitement, tandis que le cabinet Syndex était responsable de l'exploitation du questionnaire, qui constituait un second traitement.

Le Président du Tribunal de grande instance de Metz a relevé, au surplus, que la communication des adresses par l'employeur au cabinet Syndex était nécessaire au respect d'une obligation légale à laquelle l'employeur était soumis, ce qui dispensait l'employeur de recueillir le consentement des personnes concernées.

Il devait, selon le Président du Tribunal de grande instance, « être pris en compte la proportionnalité de la mesure quant aux données personnelles des salariés au regard du bénéfice de l'expertise envisagée ». En l'espèce, toujours selon le Président du Tribunal de grande instance, « il s'agit de la santé au travail des salariés en présence de risques graves dénoncés par le CHSCT à l'employeur ».

Par conséquent, le Président du Tribunal de grande instance de Metz a estimé que le refus de l'employeur de transmettre les informations requises constituait « une entrave au bon fonctionnement de l'expertise et dès lors un trouble manifestement illicite au sens de l'article 809 alinéa 1 du Code de procédure civile ».

Il a donc ordonné la communication, par l'employeur, des informations requises par le cabinet Syndex.

RGPD : refus de suppression d'une fiche Google My Business

Par une ordonnance de référé rendue le 11 juillet 2019, le Président du Tribunal de grande instance de Paris a débouté une dentiste de sa demande visant à obtenir la suppression de sa fiche entreprise Google My Business. En revanche, le juge des référés a accueilli sa demande visant à obtenir les éléments d'identification des personnes auteurs des avis litigieux.

Une dentiste parisienne avait constaté l'existence d'une fiche Google My Business comportant ses coordonnées professionnelles et des avis sur son activité qu'elle jugeait dénigrants et insultants.

Elle a assigné en référé Google Ireland Limited (ci-après désignée « Google ») afin qu'il lui soit enjoint, sous astreinte :

- A titre principal, de supprimer ses données personnelles de tous les produits et services de la marque Google (et donc de sa fiche entreprise);
- A titre subsidiaire, supprimer les avis incriminés insultants et dénigrants;
- En toute hypothèse, de communiquer les données d'identification des auteurs des avis incriminés.

Sur la demande de suppression de la fiche entreprise Google My Business, le juge des référés a rappelé les dispositions du préambule du RGPD qui affirment que le droit à la protection des données à caractère personnel n'est pas un droit absolu et doit être mis en balance avec d'autres droits fondamentaux.

A cet égard, il relève que :

- La fiche entreprise ne porte pas atteinte au droit fondamental à la protection des données à caractère personnel de la demanderesse dès lors que ces données ne relèvent pas de la sphère privée ;

- Le traitement opéré par Google poursuit des finalités légitimes permettant un accès rapide par des internautes à des informations pratiques sur les professionnels de santé ;

- L'identification de chaque professionnel concerné, sur un forum où les internautes postent leurs avis, relève d'un intérêt légitime d'information du consommateur. Le juge rappelle à cette occasion que les droits de la personnalité des professionnels en cause sont protégés par la possibilité de signaler les propos dépassant les limites admissibles de la liberté d'expression ;

- La suppression pure et simple de la fiche de la demanderesse contreviendrait au principe de la liberté d'expression, alors même qu'elle dispose de la possibilité d'agir spécifiquement contre les personnes à l'origine d'avis.

En conséquence, celui-ci a estimé que la demanderesse « ne peut exiger l'effacement de données traitées dans le cadre de la fiche entreprise dans la mesure où ce traitement est "nécessaire à l'exercice de la liberté d'expression et d'information" », qui, nous le rappelons, est l'une des exceptions prévues au droit à l'effacement par l'article 17 du RGPD.

Compte tenu de ces éléments, le juge des référés a considéré que le caractère illicite du traitement n'était pas démontré et qu'il n'y avait pas eu de la part de Google de refus manifestement injustifié d'interruption du traitement des données personnelles.

Ainsi, en l'absence de démonstration d'un trouble manifestement illicite et compte tenu de l'existence de contestations sérieuses élevées en défense, la demande portant sur l'effacement des données a été rejetée.

Concernant la demande de suppression des avis litigieux, le juge des référés n'y a pas fait droit dès lors qu'il a considéré que ces avis n'excédaient pas les limites admissibles de la liberté d'expression, à l'exception d'avis qualifiés d'injurieux mais qui avaient déjà été supprimés par Google au moment de l'instance.

En revanche, le juge des référés a ordonné à Google de communiquer à la demanderesse l'ensemble des données en sa possession permettant l'identification des personnes ayant écrit les avis litigieux afin qu'elle puisse engager « des procédures pour l'indemnisation du préjudice causé par les commentaires " insultants et dénigrants" ».

https://www.legalis.net/jurisprudences/tgi-de-paris-ordonnance-de-refere-du-11-juillet-2019/