« Toulouse Capitole Publications » est l'archive institutionnelle de l'Université Toulouse 1 Capitole.

L'IMPACT DU RGPD SUR L'ACTIVITÉ DES PLATES-FORMES EN LIGNE

ALEXANDRA MENDOZA-CAMINADE

Référence de publication : LPA 19 juin 2019, n° 145j8, p. 7

Pour toute question sur Toulouse Capitole Publications,

contacter portail-publi@ut-capitole.fr

En Europe, l'entrée en vigueur du RGPD a bouleversé les pratiques des entreprises en matière de protection des données personnelles. Spécialement, dans le cadre du commerce électronique, le respect du nouveau dispositif présente un enjeu considérable pour les plates-formes en ligne qui ont placé les données personnelles au cœur de leurs activités.

Le succès du commerce électronique a modifié les modes de consommation et constitue une source considérable de richesse, mais l'explosion du commerce en ligne est aussi un facteur de déstabilisation des échanges marchands en raison de l'importance prise par ce type de commerce et par les plates-formes en ligne*1*. Pour favoriser le commerce électronique et la croissance économique, un équilibre doit être établi entre la confiance du cyberconsommateur et les obligations imposées aux cybermarchands qui ne doivent pas nuire à leur développement. Parmi les obligations mises à la charge des sites de commerce électronique figure le respect du droit des données personnelles inscrit dans la stratégie de l'Union européenne en faveur de l'économie numérique. L'activité commerciale sur internet implique la collecte de données personnelles. Ainsi, le commerce électronique est nécessairement impacté par le nouveau dispositif de protection des données à caractère personnel. Pour autant, l'entrée en vigueur le 25 mai 2018 du règlement n° 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, dit RGPD, n'a pas modifié l'objectif de protection de la vie privée de la personne physique*2* qui s'accompagne désormais du renforcement du contrôle des personnes physiques sur leurs données personnelles et de la sécurité juridique et pratique*3*. Ce sont donc le RGPD et la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*4*, dite loi Informatique et libertés (LIL) qui sont applicables, mais le vaste chantier législatif ne sera totalement achevé qu'avec la révision de la directive n° 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, dite directive Vie privée et communications électroniques.

En l'état du droit positif, les entreprises doivent veiller à ce que leurs diverses opérations impliquant des données personnelles respectent le dispositif juridique actuel. Or cela s'avère difficile, notamment concernant les techniques commerciales en ligne utilisées pour mieux connaître les clients et répondre à leurs besoins, voire pour les devancer. Si ces technologies de prospection et de profilage de l'internaute apportent de nombreux bénéfices aux plates-formes commerciales, elles sont néanmoins très invasives à l'égard de la vie privée des individus. Face à ces techniques risquées pour la protection des données personnelles, les obligations imposées par le RGPD permettent-elles de garantir la protection de la vie privée de l'internaute ? Si le RGPD n'a pas directement modifié les modalités de traitement des données personnelles, notamment en matière de prospection commerciale, la nouvelle réglementation exerce sur les responsables de traitement une pression considérable par les nouvelles obligations qui leur sont imposées. Pourtant, alors que le RGPD fêtera sa première année d'entrée en vigueur le 25 mai

prochain, le constat est fait du retard important des entreprises, PME comme grandes entreprises, dans le respect de leurs obligations : 80 % des entreprises françaises et européennes ne seraient pas en conformité avec le RGPD*5*. À l'heure des premières lourdes condamnations sur le fondement du RGPD, les entreprises doivent absolument intégrer les prescriptions du RGPD*6*. En effet, à l'occasion du commerce en ligne, les données personnelles de l'internaute vont être soumises à des traitements multiples (I), et faire l'objet d'une exploitation par les entreprises (II).

I – Le traitement de données personnelles à l'occasion du commerce électronique

L'évolution et la sophistication des techniques ont conduit à une multiplication des traitements de données personnelles à l'occasion de la fréquentation des sites de commerce électronique (A), en particulier grâce à la technique des cookies (B).

A – Les différents traitements de données personnelles

Le commerce électronique donne lieu à de nombreuses techniques de marketing et prestations publicitaires reposant sur le traitement des données personnelles des internautes. Certaines plates-formes sont d'ailleurs basées sur le modèle économique de la collecte des données personnelles. Les plates-formes de commerce électronique peuvent se voir transmettre des données par l'internaute lui-même grâce aux informations qu'il transmet, ou de manière indirecte à l'occasion de la navigation de l'internaute sur internet par ses données de navigation.

Lors de l'inscription sur un site ou une plate-forme, ou à l'occasion d'une transaction réalisée en ligne, l'internaute saisit lui-même des informations personnelles qu'il livre pour les besoins de l'inscription ou de l'achat, informations qui pourront ensuite être traitées. Le cyberconsommateur laisse des traces lors de chaque transaction en renseignant les rubriques destinées à la formation et à l'exécution du contrat. La CJUE a ainsi rappelé que la société Amazon traite des données personnelles de ses clients dans le cadre de leur relation contractuelle*7*. L'internaute laisse également des traces lorsqu'il s'abonne à un fournisseur de service, lorsqu'il remplit un formulaire électronique ou lorsqu'il s'inscrit sur une liste de diffusion. Ces données de transaction que l'internaute livre constituent autant d'informations potentiellement personnelles.

Grâce au traçage électronique, les données peuvent aussi provenir de traces laissées lors la navigation par l'internaute*8* de boutique en boutique, au travers de bandeaux publicitaires sur lesquels il a cliqué, ou de réseaux sociaux sur lesquels il s'est promené. La simple consultation de sites laisse en effet des empreintes invisibles pour l'internaute mais qui fournissent de nombreuses informations sur les sites consultés, les transactions commerciales effectuées, les interlocuteurs. Sous réserve de quelques dispositions spéciales, les données liées à la navigation de l'internaute ne sont pas spécifiquement régies et elles sont soumises au régime juridique commun à l'ensemble des données*9*.

Les données semées consciemment ou non par l'internaute alimentent les masses de données détenues par les plates-formes qui permettent un traçage et un profilage sophistiqués de l'internaute. Le traitement des données permet de cerner au plus près l'internaute en déterminant ses goûts de cyberconsommateur. L'article 4, 4), du RGPD définit le profilage comme « toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour

évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ». La fréquentation des sites d'e-commerce conduit donc au traitement de données à caractère personnel de l'internaute avec des techniques de plus en plus invasives. L'internaute laisse des empreintes informatiques qui pour certaines présentent des risques plus importants encore pour la protection de ses droits en raison de leur caractère invisible.

B – De traitements risqués : le cas des cookies

S'agissant des services de commerce électronique, des témoins de connexion permettent de suivre l'internaute en jouant le rôle de mouchards électroniques*10*. Si plusieurs techniques permettent ainsi de tracer l'internaute, la plus répandue reste celle des cookies*11* : ces traceurs envoyés sur l'ordinateur de l'internaute par le site qu'il consulte, parfois à son insu, permettent de récolter des informations sur l'activité en ligne de l'utilisateur.

Par principe, les cookies de navigation ne présentent pas de risque pour la protection des données personnelles qu'il utilise car il vise à améliorer et à fluidifier de manière technique la navigation sur internet. C'est pourquoi ils bénéficient d'une exemption au régime juridique prévu par l'article 32, II, de la LIL*12*. En facilitant les transactions, les cookies peuvent également s'avérer un instrument de gestion du commerce électronique*13*. En revanche, les cookies qualifiés de comportementaux permettent souvent à une entreprise publicitaire de collecter des informations précises sur l'utilisateur afin de cibler son profil. Il s'agit de profiler l'internaute, notamment pour permettre une publicité personnalisée sous la forme de bandeaux publicitaires en fonction des goûts détectés. En traçant l'internaute, ces témoins de connexion peuvent porter gravement atteinte à sa vie privée*14*, car ils peuvent permettre de collecter des données à caractère personnel, même si ces fichiers n'en contiennent pas toujours. C'est pourquoi l'utilisation de cookies doit être conforme au régime juridique applicable à l'ensemble des techniques de traçage, en particulier la directive n° 2002/58/CE du 12 juillet 2002 dite Vie privée et le régime juridique français prévu en application l'article 32, II, de la LIL*15* : ces textes fixent un cadre légal précis à l'utilisation des cookies. Selon l'article 32, II, de la LIL, le responsable de traitement doit informer tout abonné ou utilisateur d'un service de communications électroniques « de toute action tendant à accéder, par voie de transmission électronique, à des informations déjà stockées dans son équipement terminal de communications électroniques, ou à inscrire des informations dans cet équipement, ainsi que des moyens dont il dispose pour s'y opposer ». Disposant alors de l'information nécessaire, il revient à la personne d'accepter le dispositif pour qu'il puisse être mis en œuvre. L'émetteur des cookies doit respecter les dispositions de l'article 32, II, de la LIL, et plus largement le droit des données personnelles, même si cela peut s'avérer difficile en pratique*16*.

Ainsi, le RGPD n'est pas le seul texte applicable et la directive Vie privée s'applique en complément. Or s'il est stabilisé du côté du droit des données personnelles avec l'entrée en vigueur du RGPD, le droit va encore subir des modifications du fait du remplacement de la directive n° 2002/58/CE du 12 juillet 2002 par un futur règlement concernant le respect de la vie privée, aussi appelé

règlement Vie privée et communications électroniques, ou encore dit ePrivacy. Le règlement ePrivacy comporte des règles relatives aux cookies, ainsi que des mesures de fréquentation et des règles d'opt-in en matière de marketing par voie électronique. Plusieurs dispositions sont très controversées*17*, en particulier s'agissant du rôle des navigateurs dans le consentement donné aux cookies, ou de l'admission des « cookie walls ». Cette dernière catégorie de cookies vise un dispositif qui interdit l'accès à un site internet tant que l'internaute n'a pas accepté l'installation de cookies sur son équipement. De plus en plus répandus, ces cookie walls sont fondamentaux pour les entreprises dont l'activité est fondée sur des prestations publicitaires basées sur l'analyse du comportement des internautes, mais ils posent un problème de compatibilité avec le droit des données personnelles*18*. Au sein du projet de règlement européen, leur admission est discutée. Ainsi, l'attente du texte finalisé génère de nombreuses incertitudes pour les entreprises concernant la conformité de leurs dispositifs aux nouvelles règles*19*, mais aussi concernant la rentabilité du nouveau modèle légal de communication en ligne. Le cadre juridique applicable est donc susceptible d'évoluer dans les mois à venir, et il faut encore attendre pour avoir un dispositif stabilisé. Par conséquent, le cadre normatif déjà complexe est en outre instable en raison de l'attente du futur règlement ePrivacy. Or dans le cadre du commerce électronique, l'internaute laisse des empreintes informatiques, visibles ou invisibles, dont les entreprises doivent désormais maîtriser les conditions de traitement.

II – L'exploitation des données personnelles à l'occasion du commerce électronique

En cas d'exploitation des données à caractère personnel, les principes généraux concernant la licéité du traitement (A) tendent à assurer une effectivité des droits des personnes concernées (B).

A – La licéité du traitement de données personnelles

Les données des personnes font l'objet de traitement, autrement dit elles sont collectées pour être stockées et analysées, et éventuellement cédées à d'autres entreprises. Or la stratégie de prospection commerciale de l'entreprise peut être impactée par le RGPD : ce dernier impose des conditions pour la licéité du traitement et pour le respect des droits de la personne concernée.

Pour que le traitement soit licite, il doit reposer désormais sur l'une des six conditions posées par l'article 6 du RGPD : l'intérêt légitime, le consentement, le traitement est nécessaire à l'exécution d'un contrat, nécessaire au respect d'une obligation légale, nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou nécessaire à l'exécution d'une mission d'intérêt public. La question se pose alors pour des techniques de prospection commerciale de déterminer quel fondement peut être utilisé par l'entreprise pour justifier de la licéité de son traitement. Jusqu'à l'entrée en vigueur du RGPD, le fondement essentiel était l'intérêt légitime : cet intérêt pouvait consister à développer et de fidéliser leur clientèle, autrement dit à exercer le commerce en ligne, et pour les consommateurs d'être informés d'offres commerciales*20*. Avec le RGPD, la solution est maintenue et ce fondement de l'intérêt légitime peut permettre d'éviter le recueil de consentement de la personne concernée. Cette évaluation implique un examen très précis des intérêts légitimes du responsable de traitement*21* : les attentes raisonnables de la personne concernée seront mises en balance avec les intérêts du professionnel, et la protection ainsi offerte par le RGPD au consommateur peut sembler insuffisante*22*. L'intérêt légitime constitue une

notion floue qui peut libérer les professionnels du recueil du consentement de l'utilisateur*23* : ce n'est que par exception que le consentement sera requis préalablement à la création du traitement.

Dans les cas où l'intérêt légitime ne peut être invoqué, le consentement de la personne est requis*24*, et implique que la personne concernée a donné son consentement spécifiquement pour une ou plusieurs finalités*25*. Les conditions de l'obtention du consentement sont renforcées par le RGPD*26*. En vertu du principe de minimisation, seules les données nécessaires à la finalité poursuivie doivent être recueillies. Or la pratique démontre souvent que ces diverses prescriptions du droit des données personnelles ne sont pas respectées*27*, en particulier en raison de l'utilisation de conditions générales d'utilisation par les plates-formes commerciales*28*.

D'autres pratiques de prospection sont considérées risquées pour la protection de la vie privée. Aussi, en présence de technologies intrusives à des fins de prospection par voie électronique, un consentement exprès et spécifique de la personne visée est nécessaire de manière préalable en vertu de l'article L. 34-5 du Code des postes et des communications électroniques. Il faut cependant relever que « le recueil du consentement n'est pas requis lorsque le courrier électronique concerne des produits ou services analogues proposés par la même personne ». Dans ce cas, l'intérêt légitime peut fonder à nouveau la licéité du traitement.

À titre de garantie, le RGPD impose que la personne concernée soit informée de l'existence d'un profilage et qu'elle dispose d'un droit d'opposition. En outre, la personne dispose d'un droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé tel que le profilage s'il produit des effets juridiques la concernant ou s'il l'affecte de manière significative. À ce titre, le RGPD semble plus protecteur que ne l'était le droit antérieur*29*.

Quel que soit le fondement légal de la collecte, les droits de la personne concernée doivent être respectés, et certains d'entre eux s'avèrent délicats à respecter pour les entreprises.

B – Les droits de la personne concernée

L'un des objectifs de la réforme du RGPD est de permettre la maîtrise de leurs données personnelles, ce qui se caractérise par le droit à l'autodétermination informationnelle. À ce titre, le texte réaffirme la plupart des droits des personnes concernées dans un chapitre éponyme et en consacre deux nouveaux que sont le droit à l'effacement et le droit à la portabilité des données. Après sa consécration jurisprudentielle*30*, le droit à l'effacement des données est reconnu par le RGPD, ainsi que le droit à la portabilité qui consiste à permettre à la personne la libre circulation de ses données et donc la concurrence entre les opérateurs*31*.

Sont ainsi regroupés le droit à l'information et à l'accès aux données à caractère personnel, le droit de rectification, le droit à l'effacement, le droit à la limitation du traitement, le droit d'opposition, le droit à la portabilité et encore le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé*32*.

L'entreprise doit donc adapter sa politique commerciale en ligne afin de répondre aux diverses exigences de la réglementation, parmi lesquelles la mise en œuvre du droit d'information de la personne*33*. Il s'agit d'un droit fondamental puisqu'il lui permet de consentir de manière éclairée. Or

certaines plates-formes peinent à transmettre des informations de manière transparente. Ces informations étant nombreuses, une hiérarchisation a été préconisée par le G29 afin d'éviter la « lassitude informative »*34*. Le RGPD n'a pas fondamentalement modifié les droits des personnes concernées, et la question se pose de l'effectivité de ces mesures au profit de la maîtrise des données du consommateur.

Pour le responsable de traitement, le RGPD innove en instaurant le principe de la conformité ou compliance qui repose sur la régulation des acteurs. Ces derniers doivent mettre en œuvre un processus de mise en conformité permanent*35* et voient leurs obligations renforcées, notamment en matière d'information et de sécurité. À tout moment, ils doivent veiller au respect des principes de protection des données, y compris en cas de transferts de données hors Union européenne*36*. Ainsi, le traçage de l'internaute doit être conforme aux prescriptions du RGPD, que ce traçage soit opéré par le responsable de traitement ou par un sous-traitant. En effet, en cas de recours à la sous-traitance, le RGPD a consacré un régime spécifique du sous-traitant qui conduit à une reconnaissance du rôle des sous-traitants ainsi qu'à leur responsabilité autonome*37*. En cas de traitement de données personnelles pour le compte d'une autre entreprise, les sous-traitants sont soumis à des obligations spécifiques, telles que la notification des violations de données, l'obligation d'assurer la sécurité et la confidentialité des données, ou encore l'obligation de conseiller le responsable de traitement*38*. Les relations entre le sous-traitant et le client doivent être contractualisées selon des conditions fixées par le RGPD*39*. En cas de contentieux, le responsable de traitement encourt une responsabilité solidaire avec le sous-traitant en cas de participation au même traitement dès que chacun d'eux peut être tenu responsable d'un dommage causé par le traitement : il s'agit alors d'une responsabilité in solidum, à charge pour celui ayant indemnisé le préjudice en totalité de demander à l'autre la part correspondant à sa part de responsabilité dans le dommage. Le choix par le responsable de traitement d'un sous-traitant RGPD-compatible est donc essentiel*40*. Toutefois, la conception stricte de la sous-traitance qui cantonne le sous-traitant au rôle d'un simple exécutant, d'après les instructions du donneur d'ordre, a pour effet de développer les cas de co-traitance, conférant alors à la personne la qualité de responsable de traitement conjoint. L'insécurité juridique qui en découle pour les acteurs économiques est considérable.

En pratique, la mise en conformité au RGPD s'avère complexe pour les entreprises qui peinent à appliquer le nouveau dispositif et qui devront encore prochainement intégrer le futur règlement ePrivacy. Les incertitudes juridiques sont nombreuses pour les acteurs du commerce en ligne, mais les sanctions prévues par le RGPD et les premières condamnations spectaculaires doivent les inciter à se conformer plus que jamais au nouveau régime actuel et à venir.

Notes de bas de page

1 –

Dans un souci de réguler la croissance débridée du commerce en ligne, l'OMC vient de s'emparer de la question afin de mettre en place des règles multilatérales.

2 –

L. n° 78-17, 6 janv. 1978, relative à l'informatique, aux fichiers et aux libertés, art. 1er.

3 –

RGPD, consid. 7.

4 –

Loi modifiée par la loi n° 2018-493 du 20 juin 2018, puis réécrite par l'ordonnance n° 2018-1125 du 12 décembre 2018 (JO, 13 déc. 2018, texte n° 5).

5 –

À peine 6 % d'entre elles respecteraient le RGPD. Parmi les justifications avancées figure « la trop grande variété des sources de données à gérer, à comprendre et à maîtriser pour 43 % des entreprises », avec de multiples supports et points de contact entre l'entreprise et ses clients et prospects ; 36 % des entreprises avancent également la complexité des outils à disposition pour protéger les données : Rolland S., « Le RGPD, une vraie révolution… lente au démarrage », 17 avr. 2019, La Tribune.

6 –

Et ce d'autant que la Commission nationale informatique et libertés (Cnil) vient d'annoncer qu'après l'achèvement de la phase de transition entre l'ancienne législation et la nouvelle, elle vérifiera désormais pleinement le respect des nouvelles obligations et nouveaux droits issus du cadre européen : Cnil, « Cnil, quelle stratégie de contrôle pour 2019 ? », 19 avr. 2019.

7 –

Aussi ce domaine ne relève pas nécessairement des dispositions du contrat, mais du droit de la protection des données personnelles : CJUE, 28 juill. 2016, n° C-191/15, VK c/ Amazon EU : Berlin D., « Vilain temps pour Amazon ! », JCP G 2016, 967.

8 –

Dès 1996, la Cnil s'alarmait de ce que l'internet devenait le « monde des traces invisibles qui défient les principes de la protection des données » : Cnil, 17e rapport d'activité 1996, 1997, La Documentation française, p. 67.

9 –

Différentes appellations existent : données de connexion, de navigation, de trafic ou encore données de transaction. Selon l'article 2, b), de la directive n° 2002/58/CE du 12 juillet 2002 dite Vie privée et communications électroniques, l'expression de données de trafic désigne « toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation ».

10 –

La technique du traçage est envisagée à l'article 32, II, de la LIL comme « toute action tendant à accéder, par voie de transmission électronique, à des informations déjà stockées dans son équipement terminal de communications électroniques, ou à inscrire des informations dans cet équipement ».

11 –

Évoquant la technique de « l'empreinte digitale » ou fingerprinting : Fauchoux V. et a., Le droit de l'internet, 3e éd., 2017, LexisNexis, n° 349.

12 –

Les dispositions de l'article 32, II, de la LIL ne sont pas applicables si le cookie a pour finalité exclusive de permettre ou faciliter la communication par voie électronique, ou s'il est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur.

13 –

Évoquant « (…) un outil légitime et utile, par exemple pour évaluer l'efficacité de la conception d'un site et de la publicité faite pour ce site, ainsi que pour contrôler l'identité des utilisateurs effectuant des transactions en ligne » : RGPD, consid. 25.

14 –

V. en ce sens : dir. n° 2002/58/CE, dite Vie privée et communications électroniques, consid. 24.

15 –

La directive n° 2002/58/CE du 12 juillet 2002, modifiée par la directive n° 2009/136/CE du 25 novembre 2009, a été transposée en droit français par l'ordonnance n° 2011-1012 du 24 août 2011 dont les dispositions figurent dans la LIL en son article 32, II.

16 –

Par une décision récente confirmant la sanction prononcée par la Cnil à l'encontre d'un éditeur de presse pour non-respect de la réglementation en matière de cookies, le Conseil d'État retient que le paramétrage d'un navigateur proposé à l'internaute par l'exploitant d'un site internet pour s'opposer au dépôt de cookies doit permettre de différencier les catégories de cookies et de savoir s'il est ensuite possible de naviguer sur le site : CE, 6 juin 2018, n° 412589.

17 –

Concernant les inquiétudes soulevées par le projet : Boulet L. et Frossard. L., « Un an de droit de la publicité », Comm. com. électr. 2018, chron. 9.

18 –

Une décision du 7 mars 2019 de l'autorité de protection des données des Pays-Bas a considéré que les cookie walls ne sont pas conformes au RGPD. Selon cette autorité, le dispositif n'est pas libre de consentir au traitement de données en raison des conséquences de son refus : https://autoriteitpersoonsgegevens.nl/nl/nieuws/websites-moeten-toegankelijk-blijven-bij-weigeren-tracking-cookies.

19 –

Dubois L. et Gaullier F., « Publicité ciblée en ligne, protection des données à caractère personnel et ePrivacy : un ménage à trois délicat », Legicom 2017/2, n° 59, p. 69.

20 –

En ce sens : G29, Guidelines on Automated individual decision-making and profiling, p. 21 et s.

21 –

RGPD, consid. 47.

22 –

Notant un recul du RGPD : Claret H., « Plates-formes numériques et protection des données personnelles du consommateur », Comm. com. électr. 2018, étude 10.

23 –

Rappelant qu'il faudra alors à la personne concernée démontrer l'atteinte à ses intérêts, droits et libertés fondamentaux : Claret H., « Plates-formes numériques et protection des données personnelles du consommateur », Comm. com. électr. 2018, étude 10.

24 –

Parmi une vague de mises en demeure, voir celle concernant une société spécialisée dans le ciblage publicitaire via des applications mobiles qui collectait des données sans recueillir le consentement des utilisateurs, notamment en les géolocalisant : Cnil, décision n° MED 2018-042 du 30 octobre 2018 : Comm. com. électr. 2018, comm. 91, note Metallinos N.

25 –

Bretonneau A., « Prospection commerciale : le consentement de l'utilisateur doit être exprès », AJDA 2015, n° 19, p. 1112.

26 –

Le consentement est défini comme « toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement » : RGPD, art. 4, 11).

27 –

La durée de conservation des données à caractère personnel doit être maitrisée par le responsable de traitement afin que cette durée n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées ou traitées : RGPD, art. 5, 1., e). La norme simplifiée NS-048 sur les fichiers clients-prospects et vente en ligne préconise un délai de trois ans pour l'utilisation des données à des fins de prospection commerciale de clients à compter de la fin de la relation commerciale, ou à compter de leur collecte pour des données d'une personne ciblée par la prospection sans être cliente.

28 –

Pour des décisions de condamnation sur le fondement du droit des clauses abusives : déclarant abusives et illicites 430 clauses des conditions générales d'utilisation de Facebook, v. TGI Paris, 9 avr. 2019 : www.legalis.net. V. aussi TGI Paris, 12 févr. 2019 : Comm. com. électr. 2019, comm. 23, note Loiseau G. : 38 clauses des conditions d'utilisation et des règles de confidentialité de Google ont été déclarées abusives et illicites, pour non-respect des obligations en matière de protection des données personnelles, en particulier s'agissant du consentement. V. aussi déclarant illicites 265 clauses des conditions d'utilisation, de politique de confidentialité et de règles de Twitter en raison de multiples

atteintes au droit des données personnelles : TGI Paris, 7 août 2018 : Comm. com. électr. 2018, comm. 74, note Loiseau G.

29 –

Rappelant que selon le G29, le profilage peut être autorisé sur le fondement de l'intérêt légitime poursuivi : Dary M. et Lichet V., « Prospection commerciale et données personnelles : le RGPD bouleverse-t-il les pratiques ? », RLDA 2018, n° 6, n° 138.

30 –

CJUE, 13 mai 2014, n° C-131/12, Google Spain ; Cass. 1re civ., 14 févr. 2018, n° 17-10499 : JurisData n° 2018-001901.

31 –

RGPD, art. 20.

32 –

Les articles 13 et 14 du RGPD énumèrent les informations que le responsable de traitement doit fournir lors de la collecte à la personne concernée et distinguent selon que la collecte a été effectuée ou non auprès d'elle.

33 –

Douville T., « Les droits des personnes concernées en cas de transmission de leurs données à caractère personnel », RLDI 2018, n° 11, n° 153 ; Martial-Braz N., « Les nouveaux droits des individus consacrés par la loi pour une République numérique. Quelles innovations ? Quelle articulation avec le Règlement européen ? », Dalloz IP/IT, 2016, p. 525.

34 –

G 29, Guidelines on transparency under Regulation 2016/679 (wp 260), pt 30. Évoquant le « click fatigue » : Metallinos N., « Le RGPD apporte-t-il de réels changements sur la place du consentement ? », Comm. com. électr. 2018, comm. 58.

35 –

Par une délibération du 21 janvier 2019, la Cnil a infligé une sanction de 50 millions d'euros à Google pour ne pas avoir respecté ses obligations en matière de transparence des informations fournies aux utilisateurs de smartphones, ainsi qu'en matière de recueil de consentement. S'agissant de son montant, la sanction qualifiée d'exemplaire est conforme aux prescriptions du RGPD qui précise que « chaque autorité de contrôle veille à ce que les amendes administratives (…) soient, dans chaque cas, effectives, proportionnées et dissuasives » : délib. Cnil n° SAN-2019-001 du 21 janvier 2019 : JCP G 2019, 67, note Deroulez J.

36 –

Exigeant l'effacement de données d'un client transférées par erreur aux États-Unis : CA Grenoble, 12 mars 2019 : www.legalis.net.

37 –

RGPD, art. 82.

38 –

Concernant la répartition des obligations et les règles en matière de responsabilité : Bounedjoum A. et Simon F.-L., « RGPD : quelles nouvelles règles en matière de responsabilité et quels impacts sur les contrats ? », AJ contrat 2018, p. 172.

39 –

V. RGPD, art. 28 mais aussi art. 32 et 33.

40 –

RGPD, consid. 81.