Le Lamy droit du numérique

980 - Vie privée, données personnelles et réseaux sociaux

L'engouement pour les réseaux sociaux s'est accompagné, chez certains internautes, d'un dévoilement inédit et parfois inconscient de leur vie privée. Cette exposition d'une vie privée – très « *partagée* » – repose, le plus souvent, sur la fausse croyance en de la communication privée qui peut parfois s'avérer bien… publique ! Ce phénomène se manifeste tant par la mutation de la conception de l'espace privé dans ce monde virtuel que par la mutation de la conception même de la vie privée. La déclinaison de toute une rhétorique de l'amitié induit un sentiment de sécurité, de nature à troubler la perception du caractère public de cette forme de communication. Il faut bien reconnaître que tout conduit à brouiller les frontières, sur ce web communautaire, entre espace privé et espace public de même qu'entre correspondance privée et communication publique.

À cette confusion entre sphère privée et sphère publique s'ajoute un discours extrêmement volontariste sur la parfaite maîtrise de son « *identité numérique* » sur l'internet. Pour « *protéger son intimité* », il faudrait « *gérer son extimité* », et ce, « *en existant de manière active, sinon il n'y aura que ce que les autres ont dit sur vous* » (Lefebvre A., Les réseaux sociaux dans l'internet 2, sur le site <www.duperrin.com>). Enfin, on voit poindre, çà et là, et notamment de la part des responsables de réseaux sociaux, l'affirmation selon laquelle la norme sociale en matière de vie privée aurait changé (voir, par exemple, les propos de Marc Zuckerberg, PDG de Facebook sur le site <www.lemonde.fr> du 11 janvier 2010). Ce discours tendant à l'affadissement du concept de vie privée peut s'expliquer par une mutation des pratiques d'exposition de la vie privée et plus largement des pratiques d'exposition de soi, sur les réseaux sociaux, pratiques soumettant la norme à de fortes turbulences (voir Mallet-Poujol N., L'internet et le contrôle des individus, in Cahiers Français, n° 354, Liberté/Libertés, Doc. fr. janv.-févr. 2010, p. 75-80 et Réseaux sociaux et vie privée : exemple de (re)négociation de la norme, in Les pratiques, sources de normativité ? , sous la dir. de Fortier V. et Lebel-Grenier S., Les éditions Revue de Droit, Université de Sherbrooke, 2011, p. 185-207 ; voir aussi, Le Clainche J. et Le Métayer D., Données personnelles, vie privée et non-discrimination : des protections complémentaires, une convergence nécessaire, RLDI 2013/90, n° 3009 ; Lucas-Schloetter A., Droit à la vie privée et protection des données personnelles *versus* liberté d'expression, Légipresse 2011, n° 282, p. 217 ; Rochfeld J. La vie tracée ou le Code civil doit-il protéger la présence numérique des personnes ?, Mélanges Hauser, LexisNexis, Dalloz, 2012, p. 619).

Certes, la préoccupation de sécurité, de confidentialité et de protection de la vie privée est désormais affichée par les responsables de ces services, notamment par la promotion du paramétrage, par l'intéressé lui-même, des éléments de confidentialité de son profil. Toutefois cette préservation de la sphère privée n'est pas aussi accomplie qu'il y paraît et la notion de vie privée est très « *chahutée* » avec les réseaux sociaux. Prospère un discours sur l'avènement d'une « *vie privée en ligne* », qui s'inscrirait non dans la culture du secret mais dans celle du partage pour générer du lien social et favoriser la vie sociale des internautes (voir Manach J.-M., Vers une vie privée en réseau, posté le 18 mars 2010 sur le site <www.internetactu.net>, p. 6). Toute régulation juridique du traitement de ces informations partagées en ligne est alors vécue comme une entrave à la libre communication sur la toile. Or ce discours vise, en définitive, souvent le traitement de données personnelles, données de traçage électronique des internautes, données certes moins sensibles que les données relatives à la vie privée, mais dont on ne saurait minimiser la nécessaire protection (voir, Groupe art. 29, Avis n° 5/2009 sur les réseaux sociaux en ligne, adopté le 12 juin 2009, WP 163 ; Marino L., Notre vie privée : des little data aux big data, JCP 19 nov. 2012, supplément au n° 47, p. 14 ; voir Türk A., La vie privée en péril, Des citoyens sous contrôle, éd. Odile Jacob, 2011, p. 112 et s. ; Bloche P. et Verchère P, Les droits de l'individu dans la révolution numérique, Rapp. AN n° 3560/2011).

Cette situation ne manque pas d'affecter la réflexion « *Informatique et Libertés* », à travers notamment la revendication d'une forme de « *droit à l'oubli numérique* ». C'est à cet objectif délicat que s'était employée la proposition de loi du Sénat sur le droit à l'oubli, qui dépasse évidemment le seul problème de la vie privée, en introduisant, aux côtés du droit d'opposition à la collecte et aux traitement des données, un droit de suppression des données, dans certaines conditions, actuellement très discutées (voir Texte n° 81 adopté, en première lecture, par le Sénat, le 23 mars 2010). La réflexion a rebondi avec le règlement européen du 27 avril 2016 qui a, lui aussi, promu une telle prérogative de la personne concernée (voir aussi UE, Groupe de travail « *article 29* » sur la protection des données, Lignes directrices du 26 novembre 2014 pour la mise en œuvre du droit à l'oubli, WP 225 ; Résolution de l'ONU, n° 68/167 du 18 déc. 2013 sur « *Le droit à la vie privée à l'ère du numérique* » ; Conseil d'État, Etude annuelle, Le numérique et les droits fondamentaux, Doc. fr. 2014).

Partie 2 Numérique et libertés - Division 3 Les droits de la personne concernée - Chapitre 4 Le droit à la maîtrise de ses données - Section 3 Le droit à l'effacement

981 - Du règlement européen du 27 avril 2016 à l'ordonnance du 12 décembre 2018

Ainsi l'article 17 du RGPD, intitulé « *Droit à l'effacement (« droit à l'oubli »)* » énonce les conditions d'un droit à l'effacement, tandis que l'article 51.-I de la loi du 6 janvier 1978, tel qu'issu de l'ordonnance de 2018, dispose que « *le droit à l'effacement s'exerce dans les conditions prévues à l'article 17 du règlement (UE) 2016/679 du 27 avril 2016* », tout en prévoyant des mesures particulières pour les personnes mineures au moment de la collecte (art. 51.-II de la loi de 1978). La loi de 1978 comprend, par ailleurs, des dispositions spécifiques pour les personnes décédées (art. 85), pour les traitements d'infractions pénales (art. 97 et 106) ou bien encore pour les traitements intéressant la sûreté de l'État ou la défense (art. 118 et 119). Il convient donc d'examiner successivement les prescriptions du RGPD, celles de la loi française ainsi que l'alternative à l'effacement que constitue la solution du déréférencement.

Sur le droit à l'oubli numérique, voir Berguig M. et Thiérache C., L'oubli numérique est-il de droit face à une mémoire numérique illimitée ?, RLDI 2010/62, n° 2039 ; Drouard E., Internet et le droit à l'oubli numérique, Légipresse 2010, n° 272, p. 3 ; Mallet-Poujol N., Du droit à l'oubli numérique, Lettre « Recherche Droit et Justice », nov. 2011, n° 37, p. 9 et <www.gip-recherche-justice.fr> ; Mallet-Poujol N., Les virtualités du droit à l'oubli numérique, Juris art etc, Ed. Dalloz, mai 2013, n 2, p. 43 ; Padova Y. et Lebeau-Marianna, Entre droit des données personnelles et liberté d'expression, quelle place pour les

moteurs de recherche ?, RLDI 2013/90, n° 3008 ; Rapport Cyberlex, Contribution dans le cadre des travaux sur le droit à l'oubli numérique, 25 mai 2010, <www.cyberlex.org>.

Partie 2 Numérique et libertés - Division 3 Les droits de la personne concernée - Chapitre 4 Le droit à la maîtrise de ses données - Section 3 Le droit à l'effacement - § 1. Le RGPD

982 - Article 17 du RGPD

Le règlement instaure un droit à l'oubli numérique, en son article 17 intitulé « *Droit à l'effacement* (« *droit à l'oubli* ») », droit permettant aux individus d'obtenir la suppression de données les concernant si aucun motif légitime ne justifie leur conservation. Il développe et précise le droit d'effacement ainsi que l'obligation - faite au responsable du traitement ayant rendu publiques des données à caractère personnel - d'informer les tiers de la demande de la personne concernée d'effacer tout lien vers ces données ou les copies ou reproductions qui en ont été faites (art. 17.-2 RGPD). La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant, dans six hypothèses (art. 17.-1, a) à 17.-1, f) RGPD). Le droit à l'effacement est instauré aux fins de protéger l'individu. Il connaît des limites justifiées par la défense de l'intérêt général (art. 17.-3 RGPD).

Partie 2 Numérique et libertés - Division 3 Les droits de la personne concernée - Chapitre 4 Le droit à la maîtrise de ses données - Section 3 Le droit à l'effacement - § 1. Le RGPD - A. Le droit à l'effacement et la protection de l'individu

983 - Considérant 65 du RGPD

Évoquant, dans son considérant 65, le droit pour les personnes concernées de *« faire rectifier des données à caractère personnel les concernant »*, et de *« disposer d'un « droit à l'oubli » lorsque la conservation de ces données constitue une violation du présent règlement ou du droit de l'Union ou du droit d'un État membre auquel le responsable du traitement est soumis »*, le RGPD affirme, qu'en particulier, ces personnes *« devraient avoir le droit d'obtenir que leurs données à caractère personnel soient effacées et ne soient plus traitées, lorsque ces données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière, lorsque les personnes concernées ont retiré leur consentement au traitement ou lorsqu'elles s'opposent au traitement de données à caractère personnel les concernant, ou encore lorsque le traitement de leurs données à caractère personnel ne respecte pas d'une autre manière le présent règlement »*.

Partie 2 Numérique et libertés - Division 3 Les droits de la personne concernée - Chapitre 4 Le droit à la maîtrise de ses données - Section 3 Le droit à l'effacement - § 1. Le RGPD - A. Le droit à l'effacement et la protection de l'individu

984 - Information de l'ensemble des responsables de traitements

Le règlement a également étendu le droit à l'effacement à l'ensemble des responsables de traitement de sorte que le responsable du traitement qui a rendu publiques les données *« soit tenu d'informer les responsables du traitement qui traitent ces données à caractère personnel qu'il convient d'effacer tout lien vers ces données, ou toute copie ou reproduction de celles-ci »* (consid. 66). L'idée du législateur européen est de *« renforcer le "droit à l'oubli" numérique »*, par l'amélioration de son effectivité (consid. 66). Aussi, aux termes de l'article 17.-2 du RGPD, *« lorsqu'il a rendu publiques les données à caractère personnel et qu'il est tenu de les effacer en vertu du paragraphe 1, le responsable du traitement, compte tenu des technologies disponibles et des coûts de mise en œuvre, prend des mesures raisonnables, y compris d'ordre technique, pour informer les responsables du traitement qui traitent ces données à caractère personnel que la personne concernée a demandé l'effacement par ces responsables du traitement de tout lien vers ces données à caractère personnel, ou de toute copie ou reproduction de celles-ci »*.

Aux termes de l'article 17.-1 du RGPD, la personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, lorsque l'un des motifs suivants s'applique :

« a) les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ;

b) la personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'article 6, paragraphe 1, point a), ou à l'article 9, paragraphe 2, point a), et il n'existe pas d'autre fondement juridique au traitement ;

c) la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 1, et il n'existe pas de motif légitime impérieux pour le traitement, ou la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 2 ;

d) les données à caractère personnel ont fait l'objet d'un traitement illicite ;

e) les données à caractère personnel doivent être effacées pour respecter une obligation légale qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis ;

f) les données à caractère personnel ont été collectées dans le cadre de l'offre de services de la société de l'information visée à l'article 8, paragraphe 1 ».

Ainsi, la personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, des données la concernant et ce, dans six hypothèses (art. 17.-1, a) à 17.-1, f) RGPD). Dans l'esprit de la protection des données personnelles, ce droit à l'effacement a deux ressorts. Le

premier ressort, que l'on peut qualifier « *d'externe* », est lié au principe de finalité tandis que le second ressort, « *interne* », procède de la volonté même de l'individu.

Partie 2 Numérique et libertés - Division 3 Les droits de la personne concernée - Chapitre 4 Le droit à la maîtrise de ses données - Section 3 Le droit à l'effacement - § 1. Le RGPD - A. Le droit à l'effacement et la protection de l'individu

985 - Droit à l'effacement et principe de finalité

Le règlement adosse clairement le droit à l'effacement au principe de finalité qui parcourt le dispositif « *Informatique et Libertés* », qu'il s'agisse des traitements inutiles ou des traitements prohibés.

a) Les traitements inutiles

Le principe de finalité est une des pierres angulaires de la protection des données personnelles. Il postule que les données doivent être « *2° Collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités (...)* » (art. 4.-2° de la loi de 1978), des exceptions étant prévues pour les traitements statistiques ou de recherche scientifique et historique. Il a pour corollaire le principe de proportionnalité selon lequel les données doivent être « *3° Adéquates, pertinentes et, au regard des finalités pour lesquelles elles sont traitées, limitées à ce qui est nécessaire ou, pour les traitements relevant des titres III et IV, non excessives* » (art. 4.-3° de la loi de 1978).

Dans cet esprit, l'article 17.-1, a) du RGPD affirme logiquement que la personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et que le responsable du traitement a l'obligation d'effacer ces données dans les meilleurs délais, lorsque l'un des motifs suivants s'applique : (...) « *a) les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière* ». Cela signifie *a contrario* qu'il ne joue pas quand les données sont encore nécessaires au traitement.

b) Principe de finalité et durée de conservation

Le principe de finalité guide, par exemple, la détermination de la durée de conservation des données. Cette limitation temporelle est un des éléments centraux de la protection, en ce qu'elle garantit à l'individu une forme de droit à l'oubli de données, à la collecte desquelles il n'a pas été en mesure de s'opposer. Face à des traitements obligatoires ou indispensables, la fixation de limites à la durée de mise en mémoire constitue une dernière soupape de sécurité pour la personne concernée. Ainsi cette cause d'effacement peut provenir tant de l'arrivée à son échéance de la durée de conservation autorisée pour le traitement que de l'absence de nécessité, avant cette échéance, de conserver les données.

c) Réseaux sociaux, droit à l'oubli et durée de conservation des données

Au plan européen, le groupe de « l'article 29 » a émis très tôt un certain nombre de préconisations à l'attention des services de réseautage social ou SRS. Ainsi l'article 3.8 de l'avis du 12 juin 2009 suggère notamment, à propos de la conservation des données, que :

« *Les données personnelles fournies par un utilisateur lors de son inscription au SRS devraient être effacées dès que l'utilisateur ou le fournisseur de SRS décide de supprimer le compte. De même, les informations supprimées par l'utilisateur lors de la mise à jour de son compte ne devraient pas être conservées. Les SRS devraient avertir les utilisateurs avant de procéder à ces formalités avec les moyens dont ils disposent pour les informer de ces périodes de rétention. Dans certains cas spécifiques, à des fins légales et sécuritaires, il pourrait être justifié de conserver pour une durée déterminée des données qui ont été mises à jour ou effacées et des comptes afin d'empêcher les opérations malveillantes résultant de l'usurpation d'identité et d'autres délits.Lorsqu'un utilisateur n'utilise plus le service pendant un certain laps de temps, le profil devrait devenir inactif, c'est-à-dire qu'il ne devrait plus être visible pour les autres utilisateurs ou pour le monde extérieur et quelque temps après, les données du compte abandonné devraient être effacées. Les SRS devraient avertir les utilisateurs par tous les moyens disponibles avant de procéder à ces formalités* » (UE, Groupe de travail "article 29" sur la protection des données, Avis 5/2009 sur les réseaux sociaux en ligne, adopté le 12 juin 2009, WP 163 ; voir aussi Groupe « article 29 », Lignes directrices du 26 novembre 2014 pour la mise en œuvre du droit à l'oubli, WP 225).

De même, la Charte du droit à l'oubli dans les sites collaboratifs et les moteurs de recherche, établie en octobre 2010 par le Secrétariat d'État à la prospective et au développement de l'économie numérique, a notamment prévu, en son article 1.3 de donner aux internautes, dès la collecte des données, une information « *claire, transparente, complète et facile à retrouver sur le site* » sur la durée de conservation des données à caractère personnel (voir Costes L., Une charte sur le « droit à l'oubli numérique », RLDI 2010/65, éditorial, p. 3).

d) Les traitements prohibés

Le règlement européen prévoit deux motifs de prohibition justifiant l'effacement des données personnelles. Premier motif, le droit à l'effacement intervient lorsque les données « *ont fait l'objet d'un traitement illicite* » (art. 17.-1, d). La suppression est, par exemple, la conséquence de l'illicéité de la publication.

Second motif, les données doivent être effacées « *pour respecter une obligation légale quiest prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis* » (art. 17.-1, e). L'on pourrait songer, par exemple, à des obligations d'effacement de mentions de condamnations, accompagnant des mesures d'amnistie.

Partie 2 Numérique et libertés - Division 3 Les droits de la personne concernée - Chapitre 4 Le droit à la maîtrise de ses données - Section 3 Le droit à l'effacement - § 1. Le RGPD - A. Le droit à l'effacement et la protection de l'individu

986 - Droit à l'effacement et volonté individuelle

Outre le principe de finalité, le RGPD adosse le droit à l'effacement à la volonté individuelle. Ce primat de la volonté de la personne concernée s'exprime, dans la loi de 1978 ainsi que dans le règlement de 2016, au travers de l'exigence d'un consentement à certains traitements des données ou du recours à la

faculté d'opposition.

a) Le consentement au traitement des données

Le règlement conçoit un droit à l'effacement lorsque « *la personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'article 6, paragraphe 1, point a), ou à l'article 9, paragraphe 2, point a* » et qu'il « *n'existe pas d'autre fondement juridique au traitement* » (art. 17.-1,b). Ce faisant, il met en œuvre le principe d'autodétermination de l'individu, principe renforcé quand celui-ci était mineur au moment de l'exposition de ses données personnelles.

Le retrait du consentement participe du pouvoir d'autodétermination de la personne concernée, lorsque l'accord pour la collecte des données est discrétionnaire, leur traitement n'ayant aucun caractère obligatoire. La personne peut alors librement retirer son consentement au traitement de ses données. Il s'agit principalement des hypothèses de consentement au traitement des données « *pour une ou plusieurs finalités spécifiques* » (art. 6.-1, a) du RGPD) et de consentement explicite au traitement de données sensibles, c'est-à-dire de traitement de données qui révèlent « *l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale* », ainsi que le traitement des « *données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique* » (art. 9.-2, a) du RGPD).

b) La faculté d'opposition au traitement des données

Le moyen le plus évident de lutter contre la publication d'informations personnelles sur l'internet est assurément de s'y opposer. La loi « *Informatique et libertés* » a, dès l'origine, promu, à titre préventif, – outre la limitation de la durée de conservation des données – le droit d'opposition de la personne concernée à certains traitements portant sur des données personnelles, droit dont la violation est assortie de sanctions pénales (voir art. 226-18-1 C. pén.).

Partie 2 Numérique et libertés - Division 3 Les droits de la personne concernée - Chapitre 4 Le droit à la maîtrise de ses données - Section 3 Le droit à l'effacement - § 1. Le RGPD - A. Le droit à l'effacement et la protection de l'individu

987 - La réflexion sur le droit à l'oubli et la faculté d'opposition à partir des années 2000

Face à l'exposition croissante de l'individu sur l'internet – et notamment à travers les réseaux sociaux, sur l'initiative de tiers « *amis sur la toile* » – le droit d'opposition a été promu comme un des moyens juridiques d'assurer une forme de droit à l'oubli numérique, aux côtés de dispositions relatives à la durée de conservation des données. Par exemple, dans leur proposition de loi n° 93 visant à mieux garantir le droit à la vie privée à l'heure du numérique, présentée le 6 novembre 2009, les sénateurs Yves Détraigne et Anne-Marie Escoffier, entendaient faciliter l'exercice du droit d'opposition, notamment en réécrivant l'ancien article 38 de la loi de 1978, pour « *bien distinguer le droit d'opposition commerciale, qui s'exerce avant tout traitement ou, en cas de collecte indirecte, avant toute communication des données, et le droit de suppression des données qui s'exerce, par définition, après* » (voir aussi le Rapport d'information du Sénat n° 441 sur « *La vie privée à l'heure des mémoires numériques, Pour une confiance renforcée entre citoyens et société de l'information* », déposé par Yves Détraigne et Anne-Marie Escoffier, le 27 mai 2009).

À cet égard, en termes d'autorégulation, la Charte du droit à l'oubli dans les sites collaboratifs et les moteurs de recherché, établie en octobre 2010 par le Secrétariat d'État à la prospective et au développement de l'économie numérique, affirme, en son article 3, qu'il convient de faciliter la mise en œuvre du droit d'opposition, pour les données publiées par l'internaute. À ce sujet, les signataires considèrent que « *toute demande d'opposition portant sur une telle donnée est légitime* » (voir Costes L., Une charte sur le « droit à l'oubli numérique », RLDI 2010/65, éditorial, p. 3).

La discussion avait été portée au plan communautaire avec la proposition de règlement du Parlement européen et du Conseil 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, (COM(2012)11 final du 25 janvier 2012). La Commission européenne évoquait, en effet, dès 2012, la possibilité, pour toute personne, de disposer d'un « *droit à l'oubli numérique* » lorsque la conservation de ses données n'était pas conforme au présent règlement. Parmi les motifs du droit d'obtenir que les données soient effacées et ne soient plus traitées, était mentionné – outre les hypothèses de données n'étant plus nécessaires au regard des finalités pour lesquelles elles ont été recueillies ou traitées, de personnes concernées ayant retiré leur consentement au traitement ou encore de traitement de données non conforme au règlement – le fait que les personnes concernées s'opposent au traitement de données à caractère personnel les concernant.

Cette question de l'oubli numérique a également été traitée par la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique (art. 63), pour ce qui concerne les données des mineurs et celles des personnes décédées.

Partie 2 Numérique et libertés - Division 3 Les droits de la personne concernée - Chapitre 4 Le droit à la maîtrise de ses données - Section 3 Le droit à l'effacement - § 1. Le RGPD - A. Le droit à l'effacement et la protection de l'individu

988 - La position de la CNIL dans les années 2010

Du côté de la CNIL, la formation restreinte de la Commission a prononcé, à l'encontre de l'éditeur d'un site mettant en ligne une banque de données de décisions de jurisprudence, une sanction pécuniaire de dix mille euros ainsi que l'injonction de cesser la mise en œuvre du traitement, pour n'avoir pas donné suite à sa mise en demeure de procéder à l'anonymisation des décisions ayant fait l'objet d'opposition de la part des personnes concernées (CNIL, délib. n° 2011-238, 12 juill. 2011, Com. com. élec. 2011, n° 12, comm. 115, note Lepage A. ; voir, dans la même affaire, CE, 23 mars 2015, n° 353717, Rec. CE tables, Com. com. élec. 2015, n° 6, n° 52, note Debet A.). L'instruction des plaintes a révélé que le président de l'association mise en cause « *n'avait pas répondu aux demandes formées par ces personnes afin que soit respecté leur droit d'opposition à figurer dans ce traitement, et que cette diffusion leur causait, ou était susceptible de leur causer de graves préjudices* ». Pour la CNIL, l'association gérant le site a notamment « *manqué à son obligation de respecter le droit d'opposition formulé par les différents plaignants, tel que garanti par* l'article 38 de la loi du 6 janvier 1978 *modifiée* ».

De même, à propos d'une procédure d'opposition automatique mise en place par une société agrégeant les données issues de profils publics d'internautes sur les réseaux sociaux, mais qui s'est révélée défaillante, la CNIL a affirmé qu'il est « *parfaitement légitime que les personnes s'opposent à la diffusion de*

données qu'elles ont, certes, elles-mêmes divulguées, mais dont elles peuvent parfaitement ne pas pour autant souhaiter qu'elles soient agrégées sous une forme telle que celle retenue par la société » (CNIL, délib. n° 2012-156 du 1er juin 2012 portant avertissement, Com. com. élec. 2012, n° 9, comm. 94, note Loiseau G.). Le service développé par cette société consistait à rechercher des informations sur les personnes physiques rendues publiques sur les réseaux sociaux, pour les agréger dans des fiches nominatives. En l'espèce, étaient diffusées des informations sous la forme d'un curriculum vitae, de l'association de photos de personnes tierces présentées comme étant en relation avec l'intéressé ou de graphique reliant de manière visuelle ces personnes entre elles. C'est à raison que la CNIL a prononcé un avertissement à l'encontre de la société pour avoir notamment manqué aux obligations prescrites par l'ancien article 38 de la loi de 1978, dès lors que la procédure d'opposition proposée par la société imposait aux personnes refusant qu'un profil à leur nom figure sur le site d'accepter, au préalable, la prise en main de leur profil, afin d'exprimer ensuite leur refus !

Partie 2 Numérique et libertés - Division 3 Les droits de la personne concernée - Chapitre 4 Le droit à la maîtrise de ses données - Section 3 Le droit à l'effacement - § 1. Le RGPD - A. Le droit à l'effacement et la protection de l'individu

989 - La position des tribunaux dans les années 2010

Au plan judiciaire, les justiciables ont fondé, avec plus ou moins de succès, des demandes de suppressions de données ou de déréférencement sur l'ancien article 38 de la loi de 1978. Ainsi, un internaute ayant eu à déplorer – alors qu'il participait régulièrement, sous un pseudonyme, à un forum de discussion sur un blog – la publication, sur ce site, d'articles associant ses nom et prénom à son pseudonyme et révélant des éléments vrais ou supposés de sa vie privée, a formulé une demande d'injonction à l'hébergeur du blog, de supprimer toute mention de ses nom et prénom sur le blog, sur le fondement de l'article 6.-I, 8° LCEN, mais aussi sur le fondement de l'ancien article 38. La Cour d'appel y a fait droit au motif que l'hébergeur pouvait être qualifié de responsable du traitement, au sens de l'article 3 de la loi de 1978, dès lors que, dans le cadre de la prestation offerte aux responsables de blogs, il « *collecte les informations contenues dans les billets, les conserve tout en organisant à la fois de façon ante-chronologique (…) et de façon à les regrouper ou agglomérer au fil du temps sur un thème donné* », tout en se réservant la faculté d'en « *suspendre la transmission ou diffusion, en cas d'abus de la part des utilisateurs* » (CA Montpellier, 15 déc. 2011, Com. com. élec. 2012, n° 4, comm. 41, note Debet A., RLDI 2012/79, n° 2644). La solution est légitime sur le droit d'opposition. Elle est plus contestable sur la qualification du responsable de traitement, plus raisonnablement attribuable au responsable du blog, qui détermine les finalités et les moyens du traitement, en l'espèce le blog, qu'à l'hébergeur, sauf à accepter un cumul de qualification pour des traitements distincts…

De même, c'est sur le fondement du droit d'opposition que le TGI de Paris a fait droit à une demande de suppression de suggestions de recherche, associant au nom d'un internaute des termes se référant à une orientation sexuelle (TGI Paris, 22 juin 2011, M.G. c/ Sté Google, Légipresse 2011, n° 287, p. 529). Le tribunal évoque, à raison, le droit d'opposition de l'ancien article 38 de la loi de 1978, mais la question de la qualification de responsable de traitement est, là encore, éclipsée.

Sur le rejet d'une demande d'effacement de la mention de baptême sur un registre paroissial, voir Cass. 1re civ., 19 nov. 2014, n° 13-25156

Partie 2 Numérique et libertés - Division 3 Les droits de la personne concernée - Chapitre 4 Le droit à la maîtrise de ses données - Section 3 Le droit à l'effacement - § 1. Le RGPD - A. Le droit à l'effacement et la protection de l'individu

990 - Le règlement européen de 2016

Aux termes de l'article 17.-1, c) du RGPD, le droit à l'effacement s'applique lorsque « *la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 1, et il n'existe pas de motif légitime impérieux pour le traitement, ou la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 2* ». Le droit à l'effacement intervient ainsi sur des oppositions au traitement de données personnelles, supposant l'absence de motif légitime impérieux pour le traitement, ou sur des oppositions discrétionnaires.

Partie 2 Numérique et libertés - Division 3 Les droits de la personne concernée - Chapitre 4 Le droit à la maîtrise de ses données - Section 3 Le droit à l'effacement - § 1. Le RGPD - A. Le droit à l'effacement et la protection de l'individu

991 - Opposition hors motifs impérieux de traitement

Dans cette première hypothèse (art. 21.-1 du RGPD), la personne est confrontée à un traitement nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement (art. 6.-1, e) du RGPD). Ou bien encore, elle est confrontée à un traitement nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant (art. 6.-1, f) du RGPD).

Cette opposition vaut y compris pour un profilage fondé sur ces dispositions. Dans ces deux cas, l'opposition est recevable s'il n'existe pas de motif légitime impérieux pour le traitement. Autrement dit, le responsable du traitement ne doit plus traiter les données, « *à moins qu'il ne démontre qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice* » (art. 21.-1, *in fine* du RGPD). Ainsi le règlement opère un renversement de la charge de la preuve par rapport à la loi française. Le responsable de traitement doit démontrer les motifs légitimes et impérieux pour le traitement, là où la personne concernée devait démontrer les motifs légitimes d'opposition.

992 - Opposition discrétionnaire

Dans cette seconde hypothèse (art. 21.-2 du RGPD), lorsque les données sont traitées à des fins de prospection, la personne concernée a le droit de s'opposer à tout moment à leur traitement à de telles fins, y compris au profilage dans la mesure où il est lié à une prospection. Le considérant 70 du règlement indique que la personne concernée devrait avoir le droit « *à tout moment et sans frais* » de s'opposer à ce traitement. Il précise, en outre, que ce droit « *devrait être explicitement porté à l'attention de la personne concernée et présenté clairement et séparément de toute information* ».

Il convient donc de considérer que le droit à l'effacement intervient également lorsqu'il est outrepassé à l'opposition formulée par l'intéressé ou lorsque celui-ci a été dans l'incapacité de s'y opposer. Ce droit à l'effacement ne doit pas être confondu avec le droit de rectification, car il est plus large. Il a vocation à être appliqué, même si les informations sont exactes et licites, sous réserve de l'appréciation des motifs impérieux de traitement.

993 - Article 17.-3 du RGPD

Après l'affirmation du droit à l'effacement, le règlement européen, dans son considérant 65, explique que « *toutefois, la conservation ultérieure des données à caractère personnel devrait être licite lorsqu'elle est nécessaire à l'exercice du droit à la liberté d'expression et d'information, au respect d'une obligation légale, à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, pour des motifs d'intérêt public dans le domaine de la santé publique, à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, ou à la constatation, à l'exercice ou à la défense de droits en justice* ».

À cet effet, l'article 17.-3 du RGPD dispose que :

« *3. Les paragraphes 1 et 2 ne s'appliquent pas dans la mesure où ce traitement est nécessaire :*

a) *à l'exercice du droit à la liberté d'expression et d'information ;*
b) *pour respecter une obligation légale qui requiert le traitement prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis, ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;*
c) *pour des motifs d'intérêt public dans le domaine de la santé publique, conformément à l'article 9, paragraphe 2, points h) et i), ainsi qu'à l'article 9, paragraphe 3 ;*
d) *à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, dans la mesure où le droit visé au paragraphe 1 est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement ; ou*
e) *à la constatation, à l'exercice ou à la défense de droits en justice* ».

Le droit à l'effacement comprend ainsi deux puissants verrous d'intérêt général. Le premier verrou impose une protection des fonds informationnels, au fur et à mesure de leur constitution, au nom du droit à l'information, tandis que le second verrou l'impose au nom d'autres intérêts publics.

994 - Protection des fonds informationnels et droit à l'information

Il n'est pas possible, au regard du droit à l'information, d'effacer des données sur les fonds informationnels appelant une grande stabilité. Certains corpus de données ne sauraient, en effet, se transformer en palimpsestes au gré de la volonté de l'individu et au mépris de la liberté d'expression, des droits de l'histoire ou des droits de la recherche scientifique et statistique.

a) Les organes de presse et la liberté d'expression et d'information

Logiquement, la première exception au droit à l'effacement est liée à la liberté d'expression et d'information. Ainsi, les dispositions du règlement européen relatives au droit de suppression « *ne s'appliquent pas dans la mesure où ce traitement est nécessaire : a) à l'exercice du droit à la liberté d'expression et d'information ; (...)* » (art. 17.-3, a) du RGPD). Cette exception est à rapprocher du régime spécifique applicable aux traitements de données à caractère personnel aux fins de journalisme et d'expression littéraire et artistique, dans le dispositif « *Informatique et Libertés* » français (art. 80 de la loi de 1978, ancien art. 67), ainsi que dans le règlement européen (art. 85 du RGPD).

Il est évidemment hors de question de conférer à l'individu la possibilité d'obtenir des sites de presse électroniques l'effacement de données le concernant, même si elles mettent, par exemple, en cause son honneur. L'article peut certes être diffamatoire mais bénéficier du fait justificatif de l'exception de vérité ou de la bonne foi. En tout état de cause, si la diffamation est sanctionnée, outre les condamnations pénales et/ou l'indemnisation civile, au nom de la liberté d'expression, le juge aura plutôt tendance à ordonner, soit l'insertion d'un communiqué judiciaire et d'un lien hypertexte de l'article vers ce communiqué, soit le déréférencement des moteurs de recherche (voir, N. Mallet-Poujol, Les traitements de données personnelles aux fins de journalisme : Légicom, n° 43, 2009/2, p. 69 ; N. Mallet-Poujol, Presse en ligne et droit à l'oubli numérique : nouvelles responsabilités, Ed. LexisNexis,

Coll. « Colloques & Débats », sept. 2011, p. 283 et s. ; J. Boyer, Droit à l'oubli, droit de suppression, droit de suite : la loi Informatique et liberté doit-elle arbitrer la liberté d'expression ? : Légicom, n° 46, 2011/1, p. 77).

La demande d'effacement peut ne porter que sur les noms et prénoms de personnes souhaitant bénéficier d'une forme de droit à l'oubli. Autrement dit, elle peut consister en une demande d'anonymisation du corpus litigieux. Tel était la requête de deux ressortissants allemands condamnés pour meurtre, vingt-cinq ans auparavant, ayant purgé leur peine et souhaitant que leurs noms soient supprimés d'archives de presse en ligne. Ils s'étaient heurtés au refus de la Cour fédérale de justice, au nom de l'intérêt du public à être informé sur un événement d'actualité, mais aussi à pouvoir faire des recherches sur des événements passés, les médias ayant pour mission de participer à la formation de l'opinion démocratique en mettant à la disposition du public des informations anciennes conservées dans leurs archives. Approuvant cette analyse, la CEDH a considéré qu'il n'y avait pas eu violation de l'article 8 Conv. EDH dans le rejet, par les tribunaux allemands, d'une demande d'anonymisation d'un reportage sur un procès pénal, mis en ligne sur le site internet d'une radio.

Pour la Cour, en effet « *l'anonymisation d'un reportage constitue certes une mesure moins attentatoire à la liberté d'expression qu'une suppression du reportage tout entier* ». Elle relève toutefois que « *l'inclusion dans un reportage d'éléments individualisés, tel le nom complet de la personne visée, constitue un aspect important du travail de la presse* » et ce d'autant plus lorsqu'il s'agit de « *reportages sur des procédures pénales ayant suscité un intérêt considérable* ». Elle en conclut que « *la disponibilité des reportages litigieux sur les sites web des médias au moment de l'introduction des demandes des requérants contribuait toujours à un débat d'intérêt général que l'écoulement d'un laps de temps de quelques années n'a pas fait disparaître* » (CEDH, 28 juin 2018, n° 60798/10 et 65599/10, M.L. et W.W. c. Allemagne, pt. 105, LP, sept. 2018, n° 363, p. 433, note R. Le Gunehec et J. Prévost). La CEDH observe, à cet égard, que les requérants « *n'ont pas fait part des tentatives qu'ils auraient faites de s'adresser aux exploitants des moteurs de recherche pour réduire la détectabilité des informations sur leurs personnes* » (pt. 114). Le déréférencement, en revanche, semble bien pressenti comme une solution acceptable !

b) Les archives et les droits de l'histoire

Dans le même esprit, le droit à l'effacement ne s'applique pas lorsque ce traitement est nécessaire « *à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques (...)* », dans la mesure où ce droit est « *susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement* » (art. 17.-3, d) RGPD). Là encore, cette exception est à rapprocher du régime particulier des traitements d'archives et des traitements de recherche historique et statistiques dans le dispositif « *Informatique et Libertés* », français et européen.

Au plan français, par exemple, outre des allègements de procédure auprès de la CNIL, ces traitements bénéficient évidemment d'une exception au principe de limitation de la durée de conservation des données (voir art. 4.-5° de la loi de 1978, ancien art. 36), avec, pour les archives publiques, un tri des données conforme à la loi sur les archives (voir art. L. 212-3 du Code du patrimoine).

Le principe de finalité connait également, une exception dite « *d'extension de finalité* », un traitement ultérieur de données à des fins statistiques ou à des fins de recherche scientifique ou historique pouvant être considéré comme compatible avec les finalités initiales de la collecte des données, s'il est réalisé dans le respect de certains principes et procédures de la loi de 1978 et s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées. L'article 4.-2° *in fine* de la loi de 1978 (ancien art. 6.2°), dispose que « *Toutefois, un traitement ultérieur de données à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques est considéré comme compatible avec les finalités initiales de la collecte des données, s'il est réalisé dans le respect des dispositions du règlement (UE) 2016/679 du 27 avril 2016 et de la présente loi, applicables à de tels traitements et s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées* ».

S'agissant de la mort numérique enfin, la loi de 1978 prévoit que le respect des directives générales et particulières, définies par la personne concernée - afin de régir la conservation, l'effacement et la communication de ses données après son décès - est sans préjudice des dispositions applicables aux archives publiques comportant des données à caractère personnel (voir art. 85.-I de la loi de 1978, ancien art. 40-1, al. 6).

Quant au règlement européen, il prévoit, en son article 89 intitulé « *Garanties et dérogations applicables au traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques* », que le droit de l'Union ou le droit d'un État membre peut prévoir des dérogations à un certain nombre de droits, sous réserve des garanties appropriées pour les droits et libertés de la personne concernée, dans la mesure où ces droits risqueraient de rendre impossible ou d'entraver sérieusement la réalisation des finalités spécifiques et où de telles dérogations sont nécessaires pour atteindre ces finalités (voir notamment, sur le régime juridique de ces traitements, l'art. 5.-1, b) (limitation des finalités), l'art. 5.-1, e) (limitation de la conservation), l'art. 9.-2, j) sur les données sensibles et les considérants 156 et 158 du RGPD).

Ainsi ne faut-il pas se méprendre sur la portée du droit à l'oubli, lequel ne saurait en aucun cas – ce qu'ont redouté les archivistes et les historiens, lors de la négociation du règlement – conduire à l'effacement de données contenues dans des archives, au mépris de la rigueur historique, ni à la soustraction de données de traitements de recherche, au mépris de la rigueur scientifique (voir notamment la pétition « *Citoyens contre le projet de règlement européen sur les données personnelles* », initiée par l'AAF – Association des archivistes français – en mars 2013).

Partie 2 Numérique et libertés - Division 3 Les droits de la personne concernée - Chapitre 4 Le droit à la maîtrise de ses données - Section 3 Le droit à l'effacement - § 1. Le RGPD - B. Les exceptions au droit à l'effacement et l'intérêt général

995 - Protection des fonds informationnels et intérêts publics

La stabilité de certains fonds informationnels obéit également à d'autres motifs d'intérêt public. Le règlement européen a, d'une part, envisagé toutes les formes de traitements numériques d'intérêt public et, d'autre part, évoqué les impératifs particuliers de santé et de justice.

Partie 2 Numérique et libertés - Division 3 Les droits de la personne concernée - Chapitre 4 Le droit à la maîtrise de ses données - Section 3 Le droit à l'effacement - § 1. Le RGPD - B. Les exceptions au droit à l'effacement et l'intérêt général

996 - Les traitements d'intérêt public

Le régime des traitements publics est toujours sensible et nécessite parfois des dérogations au droit commun. À propos du droit à l'effacement, deux techniques juridiques sont employées : l'exception pure et simple au droit à l'effacement ou l'effacement indirect

a) L'exception au droit à l'effacement

Aux termes de l'article 17.-3, b) du RGPD, le droit à l'effacement ne s'applique pas dans la mesure où ce traitement est nécessaire « *pour respecter une obligation légale qui requiert le traitement prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis, ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement* ». Cette exception très classique permet le fonctionnement normal de toute activité numérique procédant d'un intérêt public, au premier rang de laquelle figure l'administration numérique.

Ces types de fichiers publics ou d'intérêt public ne sauraient être modifiés selon la volonté de l'individu, même s'ils contiennent des données sensibles. Le principe en est évidemment la stabilité et l'exhaustivité, pendant la durée de conservation des données prévue pour le traitement, en fonction de la finalité de tels fichiers.

b) Le droit à l'effacement indirect

La loi française a rajouté deux hypothèses d'effacement indirect : pour les traitements relatifs aux impositions et pour les traitements relatifs à la sécurité publique..

Partie 2 Numérique et libertés - Division 3 Les droits de la personne concernée - Chapitre 4 Le droit à la maîtrise de ses données - Section 3 Le droit à l'effacement - § 1. Le RGPD - B. Les exceptions au droit à l'effacement et l'intérêt général

997 - Les impératifs de santé et de justice

Parmi les traitements d'intérêt public, le règlement a identifié ceux relatifs à la santé et à la justice. Le droit à l'effacement ne s'applique pas lorsque le traitement est nécessaire « *pour des motifs d'intérêt public dans le domaine de la santé publique* » (art. 17.-3, c) RGPD). Il s'agit des traitements nécessaires « *aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale sur la base du droit de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé (...)* » (art. 9.-2, h) RGPD).

Il s'agit également des traitements nécessaires « *pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, sur la base du droit de l'Union ou du droit de l'État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel* » (art. 9.-2, i RGPD ; voir aussi art. 9.-3 RGPD).

Enfin, le droit à l'effacement ne s'applique pas lorsque le traitement est nécessaire « *à la constatation, à l'exercice ou à la défense de droits en justice* » (art. 17.-3, e) RGPD). Là encore, dans ces deux hypothèses, un intérêt public majeur s'attache à la protection de ces fonds informationnels.

Partie 2 Numérique et libertés - Division 3 Les droits de la personne concernée - Chapitre 4 Le droit à la maîtrise de ses données - Section 3 Le droit à l'effacement - § 2. La loi française

998 - Dispositions applicables

La loi du 6 janvier 1978, telle qu'issue de l'ordonnance de 2018, vient préciser les modalités du droit d'effacement indirect et de l'obligation de notification de l'effacement. Elle comprend également un certain nombre de dispositions relatives au droit à l'effacement des données des personnes mineures ou des personnes décédées ou bien encore des conditions d'effacement des données figurant dans les traitements d'infractions pénales ou dans les traitements intéressant la sûreté de l'État ou la défense. Mais il convient également de mentionner des dispositions du code de procédure pénale relatives à l'effacement des données ainsi que la disposition du code pénal, instaurant l'effacement de données comme peine complémentaire, pour certaines atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques (art. 226-23 du code pénal).

Partie 2 Numérique et libertés - Division 3 Les droits de la personne concernée - Chapitre 4 Le droit à la maîtrise de ses données - Section 3 Le droit à l'effacement - § 2. La loi française

999 - Le droit d'effacement indirect

La loi de 1978 prévoit des hypothèses d'effacement indirect pour certains traitements relatifs aux impositions ou à la sécurité publique. Les demandes tendant à l'exercice du droit d'effacement sont alors adressées à la CNIL qui désigne l'un de ses membres appartenant ou ayant appartenu au Conseil d'État, à la Cour de cassation ou à la Cour des comptes pour mener les investigations utiles et faire procéder aux modifications nécessaires, lequel membre peut se faire assister d'un agent de la commission. La CNIL informe la personne concernée qu'il a été procédé aux vérifications nécessaires et de son droit de former un recours juridictionnel. Cette procédure est précisée par l'article 118 de la loi de 1978.

a) Traitements relatifs aux impositions

Aux termes de l'article 52, alinéa 1er, de la loi de 1978, tel qu'issu de l'ordonnance de 2018, « *par dérogation aux articles 49 à 51, pour les traitements mis en œuvre par les administrations publiques et les personnes privées chargées d'une mission de service public qui ont pour mission de contrôler ou recouvrer des impositions, les droit d'accès, de rectification et d'effacement s'exercent dans les conditions prévues à l'article 118, si de telles restrictions ont été prévues par l'acte instaurant le traitement* ». La loi nouvelle entend ainsi appliquer aux traitements relatifs au contrôle ou au recouvrement des impositions, les dispositions visant les traitements intéressant la sûreté de l'Etat ou la défense, si cela a été prévu par l'acte instaurant le traitement.

Une option est donc offerte au moment de la création du traitement, instaurant *de facto* un régime mixte d'effacement, direct ou indirect. Dans son avis sur le projet d'ordonnance prise en application de l'article 32 de la loi du 20 juin 2018, la CNIL avait d'ailleurs relevé que le projet d'article 52 de la loi, en prévoyant l'exercice indirect des droits pour l'ensemble des informations contenues dans le traitement, ne semblait « *pas répondre à l'exigence de proportionnalité fixée par l'article 23 du Règlement car il paraît exclure, en toute hypothèse, la faculté que les droits puissent s'exercer directement pour certaines catégories de données du traitement, comme cela est d'ailleurs actuellement le cas pour le fichier FICOBA de l'administration fiscale, concerné par cette disposition* ». Elle avait estimé que cette possibilité de régime mixte en termes d'accès, de rectification et d'effacement, qui est d'ailleurs ménagée pour les traitements intéressant la sûreté de l'État et la défense, devrait être prévue (CNIL, délib. n° 2018-349 du 15 nov. 2018).

b) Traitements relatifs à la sécurité publique

La loi du 6 janvier 1978 prévoit, pour les traitements intéressant la sécurité publique, la même procédure d'effacement indirect que pour les traitements relatifs à l'imposition. Ainsi, aux termes de l'article 52, alinéa 2, de la loi de 1978, « *il est fait application des mêmes dispositions lorsque le traitement intéresse la sécurité publique, sous réserve de l'application des dispositions du titre III* ».

Les dispositions du titre III concernent les traitements de données à caractère personnel mis en œuvre, à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, traitements relevant de la Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016. Cette coordination entre les dispositions de l'article 52, alinéa 2, de la loi de 1978, et le Titre III de la même loi était nécessaire pour les traitements intéressant la sécurité publique, la directive prévoyant par principe l'exercice direct de ces droits par la personne concernée auprès du responsable du traitement.

Partie 2 Numérique et libertés - Division 3 Les droits de la personne concernée - Chapitre 4 Le droit à la maîtrise de ses données - Section 3 Le droit à l'effacement - § 2. La loi française

1000 - Donnée transmise à un tiers et obligation de notification

Pour que l'effacement ait plein effet, le RGPD, prévoit, selon l'intitulé de son article 19, une « *obligation de notification en ce qui concerne la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement* ». L'article 19 dispose, en effet, que « *le responsable du traitement notifie à chaque destinataire auquel les données à caractère personnel ont été communiquées toute rectification ou tout effacement de données à caractère personnel ou toute limitation du traitement effectué conformément à l'article 16, à l'article 17, paragraphe 1, et à l'article 18, à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés. Le responsable du traitement fournit à la personne concernée des informations sur ces destinataires si celle-ci en fait la demande* ».

L'article 54 de la loi de 1978, tel qu'issu de l'ordonnance de 2018, dispose, quant à lui, que « *l'obligation de notification en cas de rectification ou d'effacement de données à caractère personnel ou la limitation du traitement s'exerce dans les conditions prévues à l'article 19 du règlement (UE) 2016/679 du 27 avril 2016* ».

La disposition de l'article 19 du RGPD rappelle celle de l'ancien article 40, alinéa 5, de la loi de 1978, précisant que : « *si une donnée a été transmise à un tiers, le responsable du traitement doit accomplir les diligences utiles afin de lui notifier les opérations qu'il a effectuées conformément au premier alinéa* ». Il ne s'agissait que d'une obligation de moyens, la directive ne prévoyant cette mesure que si elle ne s'avère pas impossible ou ne suppose pas un effort disproportionné (Türk A., Rapport Sénat, Examen des articles, précité, nos 218 et s.).

Partie 2 Numérique et libertés - Division 3 Les droits de la personne concernée - Chapitre 4 Le droit à la maîtrise de ses données - Section 3 Le droit à l'effacement - § 2. La loi française

1001 - L'effacement des données des personnes mineures

La loi française met en place un droit à l'effacement quand les données ont été collectées alors que la personne concernée était mineure. Ce droit est, en principe, exercé par la personne concernée. Il peut également être exercé par le titulaire de l'autorité parentale quand les données ont été collectées alors que l'enfant ne pouvait pas consentir seul au traitement, en raison de sa « *minorité numérique* ».

Partie 2 Numérique et libertés - Division 3 Les droits de la personne concernée - Chapitre 4 Le droit à la maîtrise de ses données - Section 3 Le droit à l'effacement - § 2. La loi française

1002 - L'effacement sollicité par la personne concernée

a) La minorité de l'individu, le droit de repentir et le RGPD

Le droit à l'effacement revêt une acuité particulière lorsque les données personnelles ont été exposées par des mineurs. Cette préoccupation est présente dans le règlement européen, dont le considérant 65 explique notamment que ce droit est « *pertinent, en particulier, lorsque la personne concernée a donné son consentement à l'époque où elle était enfant et n'était pas pleinement consciente des risques inhérents au traitement, et qu'elle souhaite par la suite supprimer ces données à caractère personnel, en particulier sur l'internet* ».

Il précise que la personne devrait pouvoir exercer ce droit « *nonobstant le fait qu'elle n'est plus un enfant* ».

Le règlement prévoit un droit à l'effacement de données collectées dans le cadre de « *l'offre directe de services de la société de l'information aux enfants* ». Sont visés les réseaux sociaux ouverts aux enfants.

Ainsi, l'article 17.-1, f) du RGPD dispose que la personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, lorsque l'un des motifs suivants s'applique : « *f) les données à caractère personnel ont été collectées dans le cadre de l'offre de services de la société de l'information visée à l'article 8, paragraphe 1* ».

b) Loi « pour une République numérique »

Participant de la volonté de faciliter une forme de droit à l'oubli numérique, la loi du 7 octobre 2016 pour une République numérique (art. 63) a complété la loi du 6 janvier 1978, en insérant à l'article 40 des dispositions relatives au droit à l'effacement des personnes mineures. Il s'agissait, selon l'exposé des motifs, pour des données collectées alors que la personne concernée était mineure au moment de la collecte, de mettre en place « *une procédure accélérée spécifique avec des délais réduits et une intervention plus rapide de la CNIL* ».

L'ancien article 40. II, al. 1 de la loi de 1978 disposait que, « *sur demande de la personne concernée, le responsable du traitement est tenu d'effacer dans les meilleurs délais les données à caractère personnel qui ont été collectées dans le cadre de l'offre de services de la société de l'information lorsque la personne concernée était mineure au moment de la collecte* ». Ce droit était assorti d'exceptions, principalement liées à la liberté d'expression et d'information ainsi qu'à des considérations d'intérêt public.

c) Ordonnance du 12 décembre 2018

Cette formulation de l'ancien article 40 de la loi de 1978 a été, en partie, reprise par l'ordonnance de 2018. Désormais l'article 51.-II, alinéa 1er, de la loi de 1978 dispose que :

« *En particulier, sur demande de la personne concernée, le responsable du traitement est tenu d'effacer dans les meilleurs délais les données à caractère personnel qui ont été collectées dans le cadre de l'offre de services de la société de l'information lorsque la personne concernée était mineure au moment de la collecte. Lorsqu'il a transmis les données en cause à un tiers lui-même responsable de traitement, il prend des mesures raisonnables, y compris d'ordre technique, compte tenu des technologies disponibles et des coûts de mise en œuvre, pour informer le tiers qui traite ces données que la personne concernée a demandé l'effacement de tout lien vers celles-ci, ou de toute copie ou de toute reproduction de celles-ci* ».

En cas de non effacement, une saisine de la CNIL est prévue par l'article 51.-II, alinéa 2, de la loi de 1978, lequel dispose qu'en « *cas de non-exécution de l'effacement des données à caractère personnel ou en cas d'absence de réponse du responsable du traitement dans un délai d'un mois à compter de la demande, la personne concernée peut saisir la Commission nationale de l'informatique et des libertés, qui se prononce sur cette demande dans un délai de trois semaines à compter de la date de réception de la réclamation* ».

En revanche, les exceptions de l'ancien article 40, *in fine*, calquée sur le RGPD, n'ont pas été reprises, car elles figurent à l'article 17.-3 du règlement, que la personne soit majeure ou mineure. Dans ces deux hypothèses, européenne et française, la demande de suppression émane de la personne mineure ou devenue majeure, pour des informations livrées durant sa minorité.

Dans son avis sur le projet d'ordonnance prise en application de l'article 32 de la loi du 20 juin 2018, la CNIL s'était interrogée sur la compatibilité des dispositions prévues au II du projet d'article 51 de la loi avec celles de l'article 17 du RGPD, qui « *prévoient déjà l'effacement de données relatives à des personnes mineures collectées dans le cadre de l'offre de services de la société de l'information, dans des conditions distinctes de celles prévues par le projet d'ordonnance* ». Elle avait relevé, en revanche que le second alinéa de l'article 51. II, relatif aux aspects procéduraux des actions de la Commission en la matière, pouvait être maintenu en l'état (Délib. CNIL n° 2018-349 du 15 nov. 2018).

1003 - L'effacement sollicité par le titulaire de l'autorité parentale

a) RGPD, contrat et minorité numérique

La suppression de données peut évidemment avoir pour fondement l'exercice de l'autorité parentale. À cet égard, l'article 8.-1 du RGPD, intitulé « *Conditions applicables au consentement des enfants en ce qui concerne les services de la société de l'information* », prévoit que « *lorsque l'enfant est âgé de moins de 16 ans, ce traitement n'est licite que si, et dans la mesure où, le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant* ». Les États membres peuvent prévoir par la loi « *un âge inférieur pour ces finalités pour autant que cet âge inférieur ne soit pas en-dessous de 13 ans* ». Le règlement précise, en son article 8.-2, que le responsable du traitement « *s'efforce raisonnablement de vérifier, en pareil cas, que le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant, compte tenu des moyens technologiques disponibles* ». L'article 8.-3 du RGPD ajoute fort logiquement que l'article 8.-1 « *ne porte pas atteinte au droit général des contrats des États membres, notamment aux règles concernant la validité, la formation ou les effets d'un contrat à l'égard d'un enfant* ».

b) Loi française et minorité de quinze ans

L'ordonnance du 12 décembre 2018 a repris l'ancien article 7-1 de la loi du 6 janvier 1978, introduit par la loi du 20 juin 2018, relatif à l'âge du consentement des mineurs concernant l'offre directe de services de la société de l'information. Le législateur français a donc choisi le seuil des quinze ans.

Ainsi, aux termes de l'article 45 de la loi de 1978, tel qu'issu de l'ordonnance de 2018, « *en application du 1 de l'article 8 du règlement (UE) 2016/679 du 27 avril 2016, un mineur peut consentir seul à un traitement de données à caractère personnel en ce qui concerne l'offre directe de services de la société de l'information à compter de l'âge de quinze ans.*

Lorsque le mineur est âgé de moins de quinze ans, le traitement n'est licite que si le consentement est donné conjointement par le mineur concerné et le ou les titulaires de l'autorité parentale à l'égard de ce mineur.

Le responsable de traitement rédige en des termes clairs et simples, aisément compréhensibles par le mineur, les informations et communications relatives au traitement qui le concerne ».

Lors de l'élaboration du projet de loi, le Gouvernement, suivant l'avis de la CNIL, avait fait le choix de ne pas utiliser, pour la France, cette marge de manœuvre. L'âge de 16 ans avait vocation à s'appliquer, position défendue par la France lors des négociations européennes. C'est l'Assemblée nationale qui a pris l'initiative d'abaisser le seuil, le Sénat y étant opposé. L'idée était notamment de prendre en compte les seuils de 15 ans établis dans d'autres domaines comme, par exemple, en matière d'opposition à l'accès des parents aux données de santé ou en matière de majorité sexuelle (sur ce débat, voir notamment, S. Joissains, Rapport Sénat, nº 350, enregistré le 14 mars 2018, p. 103 et s.)

Partie 2 Numérique et libertés - Division 3 Les droits de la personne concernée - Chapitre 4 Le droit à la maîtrise de ses données - Section 3 Le droit à l'effacement - § 2. La loi française

1004 - L'effacement des données des personnes décédées

La question du droit à l'effacement des données des personnes décédées a toujours préoccupé le législateur. Le texte de la loi du 6 janvier 1978 a substantiellement évolué en 2004, puis en 2016, avant d'être remanié en 2018, à la lumière de la réflexion sur la mort numérique sur les réseaux sociaux (voir notamment Favreau A., L'accès des proches aux données à caractère personnel du défunt : Numérique, Nouveaux droits, nouveaux usages, sous la dir. Chatry S. et Gobert Th., mare & martin, 2017, p. 65).

Aux termes de l'ancien article 40, alinéa 6, de la loi de 1978, tel que modifiée par la loi du 6 août 2004, "« les héritiers d'une personne décédée justifiant de leur identité peuvent, si des éléments portés à leur connaissance leur laissent présumer que les données à caractère personnel la concernant faisant l'objet d'un traitement n'ont pas été actualisées, exiger du responsable de ce traitement qu'il prenne en considération le décès et procède aux mises à jour qui doivent en être la conséquence »". Par ailleurs, "« lorsque les héritiers en font la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en vertu de l'alinéa précédent »" (L. nº 78-17, 6 janv. 1978 modifiée, art. 40, al. 7). Selon les travaux préparatoires de la loi de 2004, cette faculté avait des limites et "« les héritiers ne pourront effacer des précisions que, de son vivant, la personne décédée avait laissé figurer dans un fichier »" (Türk A., Rapport Sénat, Examen des articles, précité, nº 218).

Ces dispositions ont été grandement remaniées par la loi nº 2016-1321 du 7 octobre 2016 pour une République numérique (art. 63). En effet, le législateur a entendu organiser la délicate question de la « *mort numérique* », c'est-à-dire de la gestion des données numériques des personnes décédées, « *les héritiers n'en ayant pas nécessairement connaissance et ne pouvant y avoir accès* » (Exposé des motifs). En outre, la loi a entendu « *permettre à toute personne, de son vivant, d'organiser les conditions de conservation et de communication de ses données à caractère personnel après son décès* », par la transmission de directives en ce sens (Exposé des motifs). Ainsi, les alinéas 6 et 7 de l'article 40 ont été supprimés. Ils ont été remplacés, en 2016 par un article 40-1, largement repris, en 2018, à l'article 85 de la loi de 1978

Partie 2 Numérique et libertés - Division 3 Les droits de la personne concernée - Chapitre 4 Le droit à la maîtrise de ses données - Section 3 Le droit à l'effacement - § 2. La loi française

1005 - Mort numérique et droit à l'oubli

La loi du 6 janvier 1978, telle qu'issue de l'ordonnance du 12 décembre 2018, comprend désormais, en son titre II, un chapitre V, consacré aux « *Dispositions régissant les traitements de données à caractère personnel relatives aux personnes décédées* », composé des articles 84 à 86. Comme le souligne le rapport au Président de la République relatif à l'ordonnance (JO 13 déc. 2018), il s'agit d'une reprise des dispositions de la loi du 6 janvier 1978 qui n'ont pas été modifiées sur ce point par la loi du 20 juin 2018 « *dans la mesure où ces traitements ne sont pas régis par le règlement (UE) 2016/679 (considérant 27), ni, de façon générale, par le droit de l'Union européenne* ». Sont ainsi précisés le principe d'extinction des droits sauf maintien prévu par la loi, le régime des directives anticipées, les droits des héritiers en l'absence de directive et les modalités de gestion des informations concernant les personnes décédées, dans les traitements à des fins de recherche dans le domaine de la santé.

a) Principe d'extinction des droits sauf maintien prévu par la loi

L'article 84 de la loi de 1978 dispose que « *les traitements de données à caractère personnel relatives aux personnes décédées sont régis par les dispositions du présent chapitre. Les droits mentionnés au chapitre II s'éteignent au décès de la personne concernée. Toutefois, ils peuvent être provisoirement maintenus dans les conditions fixées à l'article 85* ». Est ainsi rappelé le principe selon lequel les droits de la personne concernée s'éteignent au décès de celle-ci, mais peuvent être provisoirement maintenus en fonction des directives de la personne.

b) Directives anticipées

L'article 85 de la loi de 1978 reprend les dispositions de l'ancien article 40.-1 de la loi de 1978. Sont ainsi précisées les conditions dans lesquelles la personne peut définir des directives relatives à la conservation, à l'effacement et à la communication de ses données à caractère personnel après son décès. L'article 85.-I, alinéa 1er, dispose, en effet que : « *toute personne peut définir des directives relatives à la conservation, à l'effacement et à la communication de ses données à caractère personnel après son décès. Ces directives sont générales ou particulières* ».

c) Directives générales

Aux termes de l'article 85.-I, alinéa 2, de la loi de 1978, les directives générales « *concernent l'ensemble des données à caractère personnel se rapportant à la personne concernée et peuvent être enregistrées auprès d'un tiers de confiance numérique certifié par la Commission nationale de l'informatique et des libertés* ».

d) Registre unique

Aux termes de l'article 85.-I, alinéa 3, de la loi de 1978, les références des directives générales et le tiers de confiance auprès duquel elles sont enregistrées sont « *inscrites dans un registre unique dont les modalités et l'accès sont fixés par décret en Conseil d'Etat, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés* ».

e) Directives particulières

Aux termes de l'article 85.-I, alinéa 4, de la loi de 1978, « *les directives particulières concernent les traitements de données à caractère personnel mentionnées par ces directives. Elles sont enregistrées auprès des responsables de traitement concernés. Elles font l'objet du consentement spécifique de la personne concernée et ne peuvent résulter de la seule approbation par celle-ci des conditions générales d'utilisation* ».

f) Objet des directives

Aux termes de l'article 85.-I, alinéa 5, de la loi de 1978, « *les directives générales et particulières définissent la manière dont la personne entend que soient exercés, après son décès, les droits mentionnés au chapitre II du présent titre. Le respect de ces directives est sans préjudice des dispositions applicables aux archives publiques comportant des données à caractère personnel* ».

Aux termes de l'article 85.-I, alinéa 6, « *lorsque les directives prévoient la communication de données qui comportent également des données à caractère personnel relatives à des tiers, cette communication s'effectue dans le respect de la présente loi* ».

g) Révocation des directives

Aux termes de l'article 85.-I, alinéa 7, « *la personne peut modifier ou révoquer ses directives à tout moment* ».

h) Personne désignée par la directive

Aux termes de l'article 85.-I, alinéa 8, de la loi de 1978, « *les directives mentionnées au premier alinéa du présent I peuvent désigner une personne chargée de leur exécution. Celle-ci a alors qualité, lorsque la personne est décédée, pour prendre connaissance des directives et demander leur mise en œuvre aux responsables de traitement concernés. A défaut de désignation ou, sauf directive contraire, en cas de décès de la personne désignée, ses héritiers ont qualité pour prendre connaissance des directives au décès de leur auteur et demander leur mise en œuvre aux responsables de traitement concernés* ».

i) Clause contractuelle réputée non écrite

Aux termes de l'article 85.-I, alinéa 9, de la loi de 1978, « *toute clause contractuelle des conditions générales d'utilisation d'un traitement portant sur des données à caractère personnel limitant les prérogatives reconnues à la personne en vertu du présent article est réputée non écrite* ».

Partie 2 Numérique et libertés - Division 3 Les droits de la personne concernée - Chapitre 4 Le droit à la maîtrise de ses données - Section 3 Le droit à l'effacement - § 2. La loi française

1006 - Absence de directives et droits des héritiers

Aux termes de l'article 85.-II de la loi de 1978, en l'absence de directives ou de mention contraire dans ces directives, les héritiers de la personne concernée peuvent exercer, après son décès, les droits mentionnés au chapitre II du présent titre II dans la mesure nécessaire à l'organisation et au règlement de la succession du défunt ou à la prise en compte, par les responsables de traitement, de son décès.

a) Organisation et règlement de la succession du défunt

A ce titre, « *les héritiers peuvent accéder aux traitements de données à caractère personnel qui le concernent afin d'identifier et d'obtenir communication des informations utiles à la liquidation et au partage de la succession. Ils peuvent aussi recevoir communication des biens numériques ou des données s'apparentant à des souvenirs de famille, transmissibles aux héritiers* » (art. 85.-II, 1° de la loi de 1978).

b) Prise en compte du décès par les responsables de traitement

À ce titre, « *les héritiers peuvent faire procéder à la clôture des comptes utilisateurs du défunt, s'opposer à la poursuite des traitements de données à caractère personnel le concernant ou faire procéder à leur mise à jour* » (art. 85.-II, 2° de la loi de 1978). Il est précisé que « *lorsque les héritiers en font la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en application du précédent alinéa* » (art. 85.-II, 2° de la loi de 1978).

c) Tribunal compétent

Aux termes de l'article 85.-II, dernier alinéa, de la loi de 1978, « *les désaccords entre héritiers sur l'exercice des droits prévus au présent II sont portés devant le tribunal de grande instance compétent* ».

d) Information délivrée par le prestataire d'un service de communication au public en ligne

Aux termes de l'article 85.-III de la loi de 1978, tout prestataire d'un service de communication au public en ligne « *informe l'utilisateur du sort des données qui le concernent à son décès et lui permet de choisir de communiquer ou non ses données à un tiers qu'il désigne* ».

Partie 2 Numérique et libertés - Division 3 Les droits de la personne concernée - Chapitre 4 Le droit à la maîtrise de ses données - Section 3 Le droit à l'effacement - § 2. La loi française

1007 - Traitements dans le domaine de la santé et informations sur les personnes décédées

a) Certificats des causes de décès

L'article 86 de la loi de 1978 dispose que « *les informations concernant les personnes décédées, y compris celles qui figurent sur les certificats des causes de décès, peuvent faire l'objet d'un traitement à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé, sauf si l'intéressé a, de son vivant, exprimé son refus par écrit* ». Est ainsi précisé que la possibilité que les informations concernant les personnes décédées, y compris celles qui figurent sur les certificats des causes de décès, fassent l'objet d'un traitement sauf si l'intéressé a, de son vivant, exprimé son refus par écrit, s'applique dans le cadre des finalités de recherche, d'étude ou d'évaluation dans le domaine de la santé.

b) Leffacement de données de traitements d'infractions pénales

Le droit d'effacement des traitements d'infractions pénales est strictement régi par les articles 97, 106 et 111 de la loi du 6 janvier 1978, lesquels résultent de la transposition de la 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 de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données. Sont ainsi précisés la teneur du droit à l'effacement, la procédure d'effacement, les restrictions à ce droit et les modalités de saisine de la CNIL, en cas de litige.

Partie 2 Numérique et libertés - Division 3 Les droits de la personne concernée - Chapitre 4 Le droit à la maîtrise de ses données - Section 3 Le droit à l'effacement - § 2. La loi française

1008 - Droit à l'effacement

S'agissant des traitements d'infractions pénales relevant de la directive 2016/680, l'article 97, alinéa 1er, de la loi de 1978 dispose que « *les autorités compétentes prennent toutes les mesures raisonnables pour garantir que les données à caractère personnel qui sont inexactes, incomplètes ou ne sont plus à jour soient effacées ou rectifiées sans tarder ou ne soient pas transmises ou mises à disposition. A cette fin, chaque autorité compétente vérifie, dans la mesure du possible, la qualité des données à caractère personnel avant leur transmission ou mise à disposition* ».

a) Transmission des informations et vérification de leur qualité

Chaque autorité compétente doit vérifier, dans la mesure du possible, la qualité des données à caractère personnel avant leur transmission ou mise à disposition. Il est prévu, à cet effet, de délivrer des informations additionnelles. Ainsi, aux termes de l'article 97, alinéa 2, de la loi de 1978, « *dans la mesure du possible, lors de toute transmission de données à caractère personnel, sont ajoutées des informations permettant à l'autorité compétente destinataire de juger de l'exactitude, de l'exhaustivité et de la fiabilité des données à caractère personnel et de leur niveau de mise à jour* ».

b) Données inexactes ou transmises illicitement

Aux termes de l'article 97, alinéa 3, de la loi de 1978, « *s'il s'avère que des données à caractère personnel inexactes ont été transmises ou que des données à caractère personnel ont été transmises de manière illicite, le destinataire en est informé sans retard. Dans ce cas, les données à caractère personnel sont rectifiées ou effacées ou leur traitement est limité conformément à l'article 106* ».

Partie 2 Numérique et libertés - Division 3 Les droits de la personne concernée - Chapitre 4 Le droit à la maîtrise de ses données - Section 3 Le droit à l'effacement - § 2. La loi française

1009 - Procédure d'effacement

S'agissant des traitements d'infractions pénales relevant de la directive 2016/680, la procédure d'effacement est précisée à l'article 106 de la loi de 1978. Cet article vise tant la rectification, la complémentation ou l'effacement des données que la limitation du traitement.

a) Droit de la personne concernée

Aux termes de l'article 106.-I de la loi de 1978, la personne concernée a le droit d'obtenir du responsable de traitement :

« *1° Que soient rectifiées dans les meilleurs délais des données à caractère personnel la concernant qui sont inexactes ;*

2° Que soient complétées des données à caractère personnel la concernant incomplètes, y compris en fournissant à cet effet une déclaration complémentaire ;

3°Que soient effacées dans les meilleurs délais des données à caractère personnel la concernant lorsque le traitement est réalisé en violation des dispositions de la présente loi ou lorsque ces données doivent être effacées pour respecter une obligation légale à laquelle est soumis le responsable de traitement ;

4° Que le traitement soit limité dans les cas prévus au III du présent article ».

b) Justification de l'effacement

Aux termes de l'article 106.-II de la loi de 1978, « *lorsque l'intéressé en fait la demande, le responsable de traitement doit justifier qu'il a procédé aux opérations exigées en application du I* ».

c) Alternative à l'effacement : la limitation du traitement

Aux termes de l'article 106.-III de la loi de 1978, au lieu de procéder à l'effacement, le responsable de traitement limite le traitement :

« *1° Soit lorsque l'exactitude des données à caractère personnel est contestée par la personne concernée sans qu'il soit possible de déterminer si les données sont exactes ou non ;*

2° Soit lorsque les données à caractère personnel doivent être conservées à des fins probatoires.

Lorsque le traitement est limité en application du 1o du présent III, le responsable de traitement informe la personne concernée avant de mettre fin à la limitation du traitement ».

d) Information sur le refus d'effacement

Aux termes de l'article 106.-IV de la loi de 1978, « *le responsable de traitement informe la personne concernée de tout refus de rectifier ou d'effacer des données à caractère personnel ou de limiter le traitement de ces données, ainsi que des motifs du refus* ».

e) Notification de l'effacement

Aux termes de l'article 106.-VI de la loi de 1978, « *lorsque des données à caractère personnel ont été rectifiées ou effacées ou que le traitement a été limité au titre des I et III, le responsable de traitement le notifie aux destinataires afin que ceux-ci rectifient ou effacent les données ou limitent le traitement des données sous leur responsabilité* ».

Partie 2 Numérique et libertés - Division 3 Les droits de la personne concernée - Chapitre 4 Le droit à la maîtrise de ses données - Section 3 Le droit à l'effacement - § 2. La loi française

1010 - Restrictions au droit d'effacement de la personne concernée

S'agissant des traitements d'infractions pénales relevant de la directive 2016/680, l'article 107 de la loi de 1978 dispose que :

« *- I. - Les droits de la personne physique concernée peuvent faire l'objet de restrictions selon les modalités prévues au II du présent article dès lors et aussi longtemps qu'une telle restriction constitue une mesure nécessaire et proportionnée dans une société démocratique en tenant compte des droits fondamentaux et des intérêts légitimes de la personne pour :*

1° Eviter de gêner des enquêtes, des recherches ou des procédures administratives ou judiciaires ;
2° Eviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales ;
3° Protéger la sécurité publique ;
4°Protéger la sécurité nationale ;
5° Protéger les droits et libertés d'autrui.

Ces restrictions sont prévues par l'acte instaurant le traitement.

II. - Lorsque les conditions prévues au I sont remplies, le responsable de traitement peut :

1° Retarder ou limiter la communication à la personne concernée des informations mentionnées au II de l'article 104 ou ne pas communiquer ces informations ;
2° Refuser ou limiter le droit d'accès de la personne concernée prévu à l'article 105 ;
3° Ne pas informer la personne du refus de rectifier ou d'effacer des données à caractère personnel ou de limiter le traitement de ces données, ni des motifs de cette décision, par dérogation au IV de l'article 106.

III. - Dans les cas mentionnés au 2° du II du présent article, le responsable de traitement informe la personne concernée, dans les meilleurs délais, de tout refus ou de toute limitation d'accès ainsi que des motifs du refus ou de la limitation. Ces informations peuvent ne pas être fournies lorsque leur communication risque de compromettre l'un des objectifs énoncés au I. Le responsable de traitement consigne les motifs de fait ou de droit sur lesquels se fonde la décision et met ces informations à la disposition de la Commission nationale de l'informatique et des libertés.

IV. - En cas de restriction des droits de la personne concernée intervenue en application des II ou III, le responsable de traitement informe la personne concernée de la possibilité, prévue à l'article 108, d'exercer ses droits par l'intermédiaire de la Commission nationale de l'informatique et des libertés. Hors le cas prévu au 1° du II, il l'informe également de la possibilité de former un recours juridictionnel ».

Partie 2 Numérique et libertés - Division 3 Les droits de la personne concernée - Chapitre 4 Le droit à la maîtrise de ses données - Section 3 Le droit à l'effacement - § 2. La loi française

1011 - Saisine de la CNIL par la personne concernée

S'agissant des traitements d'infractions pénales relevant de la directive 2016/680, l'article 108 de la loi de 1978 dispose que :

« *En cas de restriction des droits de la personne concernée intervenue en application des II ou III de l'article 107, la personne concernée peut saisir la Commission nationale de l'informatique et des libertés.*

La commission désigne l'un de ses membres appartenant ou ayant appartenu au Conseil d'Etat, à la Cour de cassation ou à la Cour des comptes pour mener les investigations utiles et faire procéder aux modifications nécessaires. Celui-ci peut se faire assister d'un agent de la commission. La commission informe la personne concernée qu'il a été procédé aux vérifications nécessaires et de son droit de former un recours juridictionnel.

Lorsque la commission constate, en accord avec le responsable du traitement, que la communication des données qui y sont contenues ne met pas en cause ses finalités, la sûreté de l'Etat, la défense ou la sécurité publique, ces données peuvent être communiquées au requérant ».

Partie 2 Numérique et libertés - Division 3 Les droits de la personne concernée - Chapitre 4 Le droit à la maîtrise de ses données - Section 3 Le droit à

1012 - Décision ou dossier judiciaire et code de procédure pénale

Aux termes de l'article 111 de la loi de 1978, les dispositions du présent chapitre « *ne s'appliquent pas lorsque les données à caractère personnel figurent soit dans une décision judiciaire, soit dans un dossier judiciaire faisant l'objet d'un traitement lors d'une procédure pénale. Dans ces cas, l'accès à ces données et les conditions de rectification ou d'effacement de ces données ne peuvent être régis que par les dispositions du code de procédure pénale* ».

1013 - L'effacement de données de traitements intéressant la sûreté de l'État ou la défense

Un titre IV spécifique de la loi du 6 janvier 1978 est désormais dédié aux traitements intéressant la sûreté de l'État ou la défense. Un principe d'effacement indirect, *via* la saisine de la CNIL, est énoncé à l'article 118 de la loi de 1978, principe qui souffre néanmoins certaines exceptions.

1014 - Le principe d'effacement indirect

L'effacement de données figurant dans des traitements intéressant la sûreté de l'État ou la défense ne peut s'effectuer que par la médiation d'un membre de la CNIL.

a) Médiation de la CNIL

Ainsi, aux termes de l'article 118.-I, alinéa 1er, de la loi de 1978, tel qu'issu de l'ordonnance de 2018 :

« *Les demandes tendant à l'exercice du droit d'accès, de rectification et d'effacement sont adressées à la Commission nationale de l'informatique et des libertés qui désigne l'un de ses membres appartenant ou ayant appartenu au Conseil d'Etat, à la Cour de cassation ou à la Cour des comptes pour mener les investigations utiles et faire procéder aux modifications nécessaires. Celui-ci peut se faire assister d'un agent de la commission. La commission informe la personne concernée qu'il a été procédé aux vérifications nécessaires et de son droit de former un recours juridictionnel* ».

b) Communication directe au requérant

L'article 118.-I, alinéa 2, précise toutefois que « *lorsque la commission constate, en accord avec le responsable du traitement, que la communication des données qui y sont contenues ne met pas en cause ses finalités, la sûreté de l'Etat, la défense ou la sécurité publique, ces données peuvent être communiquées au requérant* ».

1015 - L'exception d'effacement direct

a) Traitements dont la communication des données ne met pas en cause ses finalités

Aux termes de l'article 119.-I de la loi de 1978, « *par dérogation à l'article 118, lorsque le traitement est susceptible de comprendre des informations dont la communication ne mettrait pas en cause les fins qui lui sont assignées, l'acte réglementaire autorisant le traitement peut prévoir que les droits d'accès, de rectification et d'effacement peuvent être exercés par la personne concernée auprès du responsable de traitement directement saisi dans les conditions prévues aux II à III du présent article* ».

b) Droits de la personne concernée

Aux termes de l'article 119.-II de la loi de 1978, dans cette hypothèse de traitements dont la communication des données ne mettrait pas en cause les fins qui lui sont assignées, la personne concernée justifiant de son identité a le droit d'obtenir :

« *1° La confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de ce traitement ;*

2° Des informations relatives aux finalités du traitement, aux catégories de données à caractère personnel traitées et aux destinataires ou aux catégories de destinataires auxquels les données sont communiquées ;

3° Le cas échéant, des informations relatives aux transferts de données à caractère personnel envisagés à destination d'un Etat non membre de l'Union européenne ;

4° La communication, sous une forme accessible, des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci ;

5° Les informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé ».

c) Hypothèse des demandes abusives

Aux termes de l'article 119.-II *in fine* de la loi de 1978, « *les demandes manifestement abusives, notamment par leur nombre, leur caractère répétitif ou systématique peuvent être rejetées* ».

d) Droit d'effacement de la personne concernée

Aux termes de l'article 119.-III de la loi de 1978, la personne concernée justifiant de son identité « *peut également exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite* ».

e) Justification des effacements par le responsable du traitement

Aux termes de l'article 119.-III de la loi de 1978, « *lorsque l'intéressé en fait la demande, le responsable de traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées* ».

f) Charge de la preuve

Aux termes de l'article 119.-III de la loi de 1978, « *en cas de contestation, la charge de la preuve incombe au responsable de traitement auprès duquel est exercé le droit d'accès sauf lorsqu'il est établi que les données contestées ont été communiquées par l'intéressé ou avec son accord* ».

g) Donnée transmise à un tiers

Aux termes de l'article 119.-III de la loi de 1978, « *si une donnée a été transmise à un tiers, le responsable du traitement doit accomplir les diligences utiles afin de lui notifier les opérations qu'il a effectuées conformément au premier alinéa du III* ».

Partie 2 Numérique et libertés - Division 3 Les droits de la personne concernée - Chapitre 4 Le droit à la maîtrise de ses données - Section 3 Le droit à l'effacement - § 2. La loi française

1016 - Droit d'effacement et code de procédure pénale

Aux termes de l'article 111 de la loi de 1978, les dispositions du présent chapitre « *ne s'appliquent pas lorsque les données à caractère personnel figurent soit dans une décision judiciaire, soit dans un dossier judiciaire faisant l'objet d'un traitement lors d'une procédure pénale. Dans ces cas, l'accès à ces données et les conditions de rectification ou d'effacement de ces données ne peuvent être régis que par les dispositions du code de procédure pénale* ».

Le droit d'effacement de certains fichiers peut, en effet, résulter d'autres dispositions légales. Plusieurs articles du code de procédure pénale prévoient des procédures spécifiques d'effacement de données de fichiers de police ou de justice.

Partie 2 Numérique et libertés - Division 3 Les droits de la personne concernée - Chapitre 4 Le droit à la maîtrise de ses données - Section 3 Le droit à l'effacement - § 2. La loi française

1017 - Le traitement d'antécédents judiciaires - TAJ -

Aux termes de l'article 230-8 du code de procédure pénale, relatif aux fichiers d'antécédents, « *le traitement des données à caractère personnel est opéré sous le contrôle du procureur de la République territorialement compétent, qui, d'office ou à la demande de la personne concernée, ordonne qu'elles soient effacées, complétées ou rectifiées, notamment en cas de requalification judiciaire, ou qu'elles fassent l'objet d'une mention. La rectification pour requalification judiciaire est de droit* (...) ».

Dans une affaire, où le droit de rectification pour « *requalification judiciaire* » découlait de l'article 21 de la loi du 18 mars 2003 pour la sécurité intérieure, alors en vigueur, le Conseil d'État a été amené à trancher une question de compétence d'attribution, entre la juridiction judiciaire ou administrative, dans le cadre d'un litige né du refus du procureur de la République d'ordonner l'effacement des mentions d'une personne dans le « *système de traitement des infractions constatées* » - STIC - (remplacé en 2014 par le traitement d'antécédents judiciaires - TAJ -). Il a ainsi jugé que - si les données nominatives figurant dans le STIC portent sur des informations recueillies au cours d'enquêtes préliminaires ou de flagrance ou d'investigations exécutées sur commission rogatoire et concernant tout crime ou délit ainsi que certaines contraventions de cinquième classe - les décisions en matière d'effacement ou de rectification, qui ont pour objet la tenue à jour de ce fichier et sont détachables d'une procédure judiciaire, constituent des « *actes de gestion administrative du fichier et peuvent faire l'objet d'un recours pour excès de pouvoir devant le juge administratif* » (CE, 17 juill. 2013, n° 359417, JCP G 2013, n° 891, p. 1527, note Erstein).

Le Conseil d'État a jugé que les dispositions de l'article 230-8 du code de procédure pénale ne prévoyant de règles particulières relatives au maintien ou à l'effacement des données du traitement des antécédents judiciaires qu'en cas de décisions de relaxe, d'acquittement, de non-lieu ou de classement sans suite, le législateur doit être regardé comme n'ayant entendu ouvrir la possibilité d'effacement que dans les cas où les poursuites pénales sont, pour quelque motif que ce soit, « *demeurées sans suite* ». Hors cette hypothèse, les données ne peuvent être effacées qu'à l'issue de la durée de conservation fixée par voie réglementaire et le procureur de la République ne peut alors que refuser une demande d'effacement avant ce terme (CE, avis, 30 mars 2016, n° 395119, Rec. CE, JCP 2016, J. 630, note Blay-Grabarczyk K.).

À propos du traitement des antécédents judiciaires - TAJ - le Conseil constitutionnel a estimé qu'en « *privant les personnes mises en cause dans une*

procédure pénale, autres que celles ayant fait l'objet d'une décision d'acquittement, de relaxe, de non-lieu ou de classement sans suite, de toute possibilité d'obtenir l'effacement de leurs données personnelles inscrites dans le fichier des antécédents judiciaires, les dispositions contestées portent une atteinte disproportionnée au droit au respect de la vie privée ». Il en a conclu que le premier alinéa de l'art. 230-8 C. proc. pén., dans sa rédaction résultant de la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, devait être déclaré contraire à la Constitution (Cons. const. décis. n° 2017-670 QPC du 27 oct. 2017, pt. 14 ; sur la compétence de la juridiction judiciaire pour connaître du recours en effacement du fichier TAJ, contre une décision du procureur de la République, en vertu de l'art. 230-8 C. proc. pén., Trib. confl. 8 oct. 2018, n° C4134).

Partie 2 Numérique et libertés - Division 3 Les droits de la personne concernée - Chapitre 4 Le droit à la maîtrise de ses données - Section 3 Le droit à l'effacement - § 2. La loi française

1018 - Le fichier national automatisé des empreintes génétiques - FNAEG -

L'article 706-54 du code de procédure pénale dispose que : « *Le fichier national automatisé des empreintes génétiques, placé sous le contrôle d'un magistrat, est destiné à centraliser les empreintes génétiques issues des traces biologiques ainsi que les empreintes génétiques des personnes déclarées coupables de l'une des infractions mentionnées à l'article 706-55 en vue de faciliter l'identification et la recherche des auteurs de ces infractions. Sont conservées dans les mêmes conditions les empreintes génétiques des personnes poursuivies pour l'une des infractions mentionnées à l'article 706-55 ayant fait l'objet d'une décision d'irresponsabilité pénale en application des articles 706-120, 706-125, 706-129, 706-133 ou 706-134* (...) ».

Voir, au visa de l'article 8 Conv. EDH, sur le fait que le régime actuel de conservation des profils ADN dans le FNAEG n'offre pas, en raison tant de sa durée que de l'absence de possibilité d'effacement, une protection suffisante à l'intéressé (pt. 45) et que la condamnation pénale du requérant pour avoir refusé de se soumettre au prélèvement destiné à l'enregistrement de son profil dans le FNAEG s'analyse en une atteinte disproportionnée à son droit au respect de sa vie privée et ne peut passer pour nécessaire dans une société démocratique (pt. 46), CEDH, 22 juin 2017, Aycaguer c. France, n° 8806/12, D. 2017. 1363

À cet égard, a été cassé un arrêt ayant relaxé un prévenu du chef de refus de se soumettre au prélèvement biologique destiné à l'identification de son empreinte génétique, au motif que la CEDH, dans l'affaire Aycaguer c. France, a estimé que le régime actuel de conservation des profils ADN dans le FNAEG, n'offrait pas, en raison tant de sa durée que de l'absence de possibilité d'effacement, une protection suffisante à l'intéressé. La cour d'appel avait ainsi jugé qu'au vu de cette décision mais aussi de la nature ainsi que du degré de gravité des faits principaux reprochés au prévenu, il convenait d'appliquer la jurisprudence de la CEDH et de constater que la condamnation pour l'infraction visée à l'article 706-56, II, du code de procédure pénale serait contraire à l'article 8 Conv. EDH. Pour la Cour de cassation, cette analyse n'était pas fondée dès lors que le refus de prélèvement a été opposé par une personne qui n'était pas condamnée mais à l'encontre de laquelle il existait des indices graves ou concordants rendant vraisemblable qu'elle ait commis l'une des infractions mentionnées à l'article 706-55, « *de sorte qu'elle avait alors la possibilité concrète, en cas d'enregistrement de son empreinte génétique au fichier, d'en demander l'effacement* » (Cass. crim., 15 janv. 2019, n° 17-87.185).

Partie 2 Numérique et libertés - Division 3 Les droits de la personne concernée - Chapitre 4 Le droit à la maîtrise de ses données - Section 3 Le droit à l'effacement - § 2. La loi française

1019 - Condamnation à l'effacement de données et code pénal : peine complémentaire d'effacement

L'article 226-23 du code pénal dispose que :

« *Dans les cas prévus aux articles 226-16 à 226-22-2, l'effacement de tout ou partie des données à caractère personnel faisant l'objet du traitement ayant donné lieu à l'infraction peut être ordonné. Les membres et les agents de la Commission nationale de l'informatique et des libertés sont habilités à constater l'effacement de ces données* ».

Partie 2 Numérique et libertés - Division 3 Les droits de la personne concernée - Chapitre 4 Le droit à la maîtrise de ses données - Section 3 Le droit à l'effacement - § 3. L'opposition, le droit à l'oubli numérique et le déréférencement

1020 - Oubli numérique et procédé de désindexation

Une autre forme d'oubli numérique peut s'opérer au moyen du procédé de désindexation. Là encore, les demandes de déréférencement formulées par les requérants ont connu des fortunes diverses, que ce soit devant la CJUE ou devant les juridictions françaises.

Partie 2 Numérique et libertés - Division 3 Les droits de la personne concernée - Chapitre 4 Le droit à la maîtrise de ses données - Section 3 Le droit à l'effacement - § 3. L'opposition, le droit à l'oubli numérique et le déréférencement - A. Jurisprudence de la CJUE

1021 - Affaire Google Spain c. Costeja

L'arbitrage entre la protection des individus et la liberté d'expression a été au coeur de l'arrêt « *Google Spain c. Costeja* » de la CJUE, à propos du référencement des personnes physiques par les moteurs de recherche. La Cour reconnaît, au visa des articles 12, sous b), et 14, alinéa 1er, sous a), de la directive 95/46 relative à la protection des données à caractère personnel, le droit au déréférencement, consistant à « *supprimer de la liste de résultats, affichée à la suite d'une recherche effectuée à partir du nom d'une personne, des liens vers des pages web, publiées par des tiers* » (pt. 82). La personne concernée peut ainsi – eu égard à ses droits fondamentaux au titre des articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne – demander que l'information ne soit plus mise à la disposition du grand public du fait de son inclusion dans une telle liste de résultats. Ces droits « *prévalent, en principe, non seulement sur l'intérêt économique de l'exploitant du moteur de recherche, mais également sur l'intérêt de ce public à accéder à ladite information lors d'une recherche portant sur le nom de cette personne* ». Il en serait autrement « *s'il apparaissait, pour des raisons particulières, telles que le rôle joué par ladite personne dans la vie publique, que l'ingérence dans ses droits fondamentaux est justifiée par l'intérêt prépondérant dudit public à avoir, du fait de cette inclusion, accès à l'information en question* » (CJUE, 13 mai 2014, Google Spain aff. C-131/12, Comm. com. élec. 2014, Etudes 13, Debet A, D. 2014. J. 1476, note V.-L. Benabou et J. Rochfeld et 1481, note N. Martial-Braz et J. Rochfeld, JCP 2014, n° 768, note L. Marino, Légipresse, 2014, n° 317, p. 323, Tribune E. Drouard et Légipresse 2014, n° 319, p. 467, note N. Mallet-Poujol, RLDI 2014/106, n° 3535, comm. C. Castets-Renard, n° 3536, comm. D. Forest, n° 3537, comm. A. Casanova ; RLDI, 2014/107, n° 3550, comm. O. Pignatari et n° 3569, note J. Le Clainche, RLDI 2014/109, n° 3609, comm. R. Perray et P. Salen).

Sur les questions préjudicielles sur la portée de l'arrêt « *Google Spain c. Costeja* » et l'application du droit au déréférencement à des données sensibles, voir CE, Ass. 24 févr. 2017, n° 391000 : Rec. CE.

Sur les questions préjudicielles sur la portée de ce déréférencement à l'échelle de l'ensemble des noms de domaine du moteur de recherche, voir CE, 19 juill. 2017, n° 399922, Rec. CE tables ; Com. com. électr. 2017, n° 9, com. 85, note Debet A.

Sur la limitation, à l'expiration d'un délai suffisamment long après la dissolution de la société concernée, de l'accès aux données personnelles concernant certaines personnes, aux tiers justifiant d'un intérêt spécifique à la consultation des données figurant dans le registre des sociétés, voir CJUE, 9 mars 2017, aff. C-398/15, Comm. com électr, 2017 n° 7, comm. 66, note Metallinos N.; Légipresse 2017, n° 353, p. 494, note Pautrot B.).

1022 - Illustrations

Une demande de désindexation avait, par exemple, échoué dans une affaire où les requérants déploraient « *l'utilisation de leur patronyme comme mot clé sur les moteurs de recherche* ». Leur nom donnait, en effet, accès au titre d'un article archivé sur le site « lesechos.fr » faisant état d'un arrêt du Conseil d'État les concernant dans une affaire disciplinaire qui remontait à 2006. Il s'agissait certes d'un site de presse électronique, pour lequel étaient applicables les dispositions spécifiques de l'ancien article 67 de la loi de 1978, relatif aux traitements de journalisme. Mais ce refus demeure quelque peu sévère, dans la mesure où l'appréciation des motifs légitimes de désindexation pouvait être plus clémente que pour une demande de suppression, car ne portant pas atteinte à la liberté d'expression (TGI Paris 9 mai 2012, Légipresse 2012, n° 297, p. 504, note Mallet-Poujol N. ; confirmé par CA Paris 26 févr. 2014, inédit).

Toutefois, la position des juges du fond a été confirmée par la Cour de cassation , approuvant le raisonnement selon lequel le fait d'imposer à un organe de presse, soit de supprimer du site internet dédié à l'archivage de ses articles, qui ne peut être assimilé à l'édition d'une base de données de décisions de justice, l'information elle-même contenue dans l'un de ces articles, le retrait des nom et prénom des personnes visées par la décision privant celui-ci de tout intérêt, soit d'en restreindre l'accès en modifiant le référencement habituel, excède les restrictions qui peuvent être apportées à la liberté de la presse (Cass. 1re civ., 12 mai 2016, n° 15-17.729 ; sur le fait que « *le choix du nom d'une personne physique comme mot-clé destiné à faciliter le référencement par les moteurs de recherche sur internet des pages qui le supportent n'est pas fautif lorsqu'il n'est associé à aucune autre donnée personnelle, et ne le devient, le cas échéant, que lorsqu'est répréhensible le contenu de la page à laquelle ce mot-clé est associé* », voir Cass. 1re civ., 10 sept. 2014, n° 13-12464).

À la lumière de l'arrêt « *Google Spain c. Costeja* », la Cour de cassation a énoncé que « *la juridiction saisie d'une demande de déréférencement est tenue de porter une appréciation sur son bien-fondé et de procéder, de façon concrète, à la mise en balance des intérêts en présence, de sorte qu'elle ne peut ordonner une mesure d'injonction d'ordre général conférant un caractère automatique à la suppression de la liste de résultats, affichée à la suite d'une recherche effectuée à partir du nom d'une personne, des liens vers des pages internet contenant des informations relatives à cette personne* ». Dans cette affaire, reprochant à la société Google Inc. d'exploiter, sans son consentement, des données à caractère personnel le concernant, par le biais du moteur de recherche Google.fr, un individu a saisi le juge des référés, sur le fondement de l'art. 809 du code de procédure civile, pour obtenir la cessation de ces agissements, constitutifs, selon lui, d'un trouble manifestement illicite. Après avoir ordonné à la société Google Inc. de supprimer les liens qui conduisent, lors de recherches opérées sur le moteur Google.fr incluant les nom et prénom du requérant, aux deux adresses URL précisées en son dispositif, l'arrêt enjoint à cette société de supprimer les liens qui conduisent, lors de recherches opérées dans les mêmes conditions, à toute adresse URL identifiée et signalée par le requérant comme portant atteinte à sa vie privée, dans un délai de sept jours à compter de la réception de ce signalement. Cette seconde injonction est annulée par la Cour de cassation, au motif qu'en « *prononçant ainsi une injonction d'ordre général et sans procéder, comme il le lui incombait, à la mise en balance des intérêts en présence* », la cour d'appel a violé les articles 38 et 40 de la loi de 1978 (Cass. 1re civ., 14 févr. 2018, n° 17-10.499, RLDI 2018/146, n° 5187, obs. Costes L.). Il est constant que le droit au déréférencement ne s'apprécie pas dans l'absolu, au regard de la nature des données personnelles diffusées, mais qu'il dépend du contexte de leur diffusion, contexte de nature à déterminer s'il existe un intérêt prépondérant du public à y avoir accès.