UNIVERSITÉ PARIS II
PANTHÉON-ASSAS

BANQUE DES MEMOIRES

Master 2 droit comparé des affaires

Dirigé par Madame la Professeure Marie Goré

2020

Le droit à l'oubli, étude comparée entre la France et les Etats-Unis

Alexis Andréani

Monsieur le Professeur Pierre-Emmanuel Audit

Résumé

A une époque où, en quelques clics, il est possible de mettre en ligne une quantité d'informations énormes pour une audience quasi-illimitée, la protection des données est fondamentale pour la sauvegarde des droits fondamentaux des individus.

Le Règlement Général pour la Protection des Données, dernière grande législation européenne dans cette optique, institue un nouveau droit : le droit à l'oubli. Il permet à tout individu de demander l'effacement de ses données à une entité qui les a collectées.

Depuis la parution de la proposition de RGPD en 2012, les auteurs ne cessent de s'interroger : est-ce un nouveau droit à part entière ? Est-il un outil supplémentaire pour sauvegarder sa vie privée ? Qu'en est-il de des conflits qu'il pourrait engendrer avec la liberté d'expression et d'autres droits fondamentaux ?

Peu à peu, avec l'aide de la Cour de Justice de l'Union Européenne, les juridictions internes des Etats membres essayent de cerner le domaine et le régime de ce droit.

Aux Etats-Unis, ce droit n'existe pas, ou en tout cas sous une forme embryonnaire. Cette lacune pourrait se révéler problématique : si aujourd'hui la CJUE fait preuve d'une certaine précaution quant à la portée territoriale de ce droit, rien ne nous ne dit qu'elle ne changera pas de position. Les limites du RGPD pourraient ainsi s'étendre à des horizons plus éloignées que les simples limites de l'Union européenne.

L'objectif de cette étude est d'analyser quels sont les éléments empêchant la mise en place d'un droit à l'oubli aux Etats-Unis, en comparant la législation de ce pays sur la vie privée et sur la protection des données à celle de la France.

A travers cette comparaison, nous avons l'ambition de mieux comprendre le droit à l'oubli, d'en définir l'exercice et les limites. Si le droit à l'oubli a d'abord existé en Europe, rien n'interdit que le Vieux Continent ne s'inspire de la législation étasunienne en matière de protection des données.

Cette étude permet aussi de mesurer l'efficacité réelle de ce droit nouveau, qui commence tout juste à être appliqué par les tribunaux.

Sommaire

Remerciements

Je tiens tout d'abord à remercier mon directeur de mémoire, Monsieur le Professeur Pierre-Emmanuel Audit, qui a su me diriger vers un plan cohérent pour organiser cette étude comparée.

Un remerciement particulier au personnel de la bibliothèque du centre de droit comparé, qui m'a accompagné dans mes recherches tout au long de l'année.

Mes remerciements à mes parents, qui m'ont aidé à relire et peaufiner mon mémoire.

Enfin, des remerciements sont de rigueurs pour Aliénor, Myriam, Antoine, Victor et Samy, mes camarades proches du master, sans qui cette année aurait été bien moins amusante.

Je ne remercie pas le pangolin.

Table des abréviations

RGPD	Règlement Général pour la Protection des Données
CNIL	Commission National Informatique et Libertés
COPPA	Children's Online Privacy Protection Act
CCPA	California Consumer Protection Act
FTC	Federal Trade Comission
CEDH	Cour Européenne des Droits de l'Homme
CJUE	Cour de Justice de l'Union Européenne

INTRODUCTION

Dans son ouvrage *Surveiller et Punir*, le philosophe Michel Foucault théorise ce qu'il appelle la société de surveillance. Il se base pour cela sur le modèle de gestion de la quarantaine mise en place par l'autorité publique pour gérer les pestiférés à la fin du XVIIe siècle. La ville était organisée comme un « espace clos, découpé, surveillé en tous ses points, où les individus sont insérés en une place fixe, où les moindres mouvements sont contrôlés, où tous les événements sont enregistrés, où un travail ininterrompu d'écriture relie le centre et la périphérie, où le pouvoir s'exerce sans partage, selon une figure hiérarchique continue, où chaque individu est constamment repéré[1] ». Il fait un parallèle entre cette gestion de crise épidémique et la société de la toute fin du XIXe siècle. Dans les écoles, dans les prisons, dans les casernes, dans les hôpitaux, dans les asiles psychiatriques, il constate qu'une division binaire de l'individu était opérée : entre le bon élève et le mauvais élève, entre l'individu dangereux et l'inoffensif ou entre le « fou » et le saint d'esprit. Exactement comme les autorités divisaient les pestiférés et les non-infectés pendant les quarantaines, la société sépare le « normal » de « l'anormal » pour contrôler, corriger ou soigner ce dernier. La société de surveillance est basée sur une succession de lieux d'enfermement où chacun passe d'un milieu clos à un autre tout au long de sa vie.

Il oppose ce système de surveillance à celui du panoptisme, issu du modèle de prison appelé panoptique inventé par John Bentham[2], un philosophe anglais du XVIIIème siècle. Michel Foucault décrit le principe de ce système de prison comme il s'ensuit : « à la périphérie un bâtiment en anneau; au centre, une tour; celle-ci est percée de larges fenêtres qui ouvrent sur la face intérieure de l'anneau ; le bâtiment périphérique est divisé en cellules, dont chacune traverse toute l'épaisseur du bâtiment ; elles ont deux fenêtres, l'une vers l'intérieur, correspondant aux fenêtres de la tour; l'autre, donnant sur l'extérieur, permet à la lumière de traverser la cellule de part en part[3] ». Dans chaque cellule, un prisonnier, et, dans la tour, un gardien surveille chacune des cellules. Par l'effet de la lumière qui entre dans chaque cellule par l'extérieur, il peut saisir les ombres projetées par les silhouettes des prisonniers. A l'inverse, eux n'ont aucun aperçu de la personne qui les surveille. Le principe du panoptisme est l'invisibilisation du pouvoir. Le prisonnier sait qu'il peut être surveillé, mais il n'en a aucune certitude. Le prisonnier va donc s'autodiscipliner, car la seule possibilité de la surveillance suffit à le contrôler. Le panoptisme rend donc la surveillance « permanente dans ses effets, même si elle est discontinue dans son action [4]». Loin de limiter ce modèle à la prison, Michel Foucault l'extrapole à la société

[1] M. Foucault, *Surveiller et Punir,* Gallimard, Paris, 1975, p. 199
[2] J. Bentham, *Panopticon*, *Works*, éd. Browning, L IV, 1780 p. 60 - 64
[3] Foucault, *Surveiller,* op. cit., p. 201
[4] Foucault, *Surveiller*, op. cit., p. 202

entière : « c'est en fait une figure de technologie politique qu'on peut et qu'on doit détacher de tout usage spécifique[5] ».

Michel Foucault ne pense pas que la société contemporaine correspond à la société de surveillance qu'il décrit. Il ne l'apparente pas non plus au modèle basé sur le panoptique. Il constate que « la discipline, qui était si efficace pour maintenir le pouvoir, a perdu une partie de son efficacité. Dans les pays industrialisés, les disciplines entrent en crise »[6]. C'est de ce postulat que va partir Gilles Deleuze, philosophe français contemporain de Foucault, pour théoriser la société de contrôle, qui, pour lui, caractérise la société moderne vers laquelle a transitionné celle décrite par Foucault. En se basant sur le panoptisme, il va décrire notre société comme un modèle qui n'a pas besoin d'enfermement pour surveiller, où l'autorité est invisible et où le contrôle s'opère dans l'espace ouvert.

Si en 1990, Gilles Deleuze décrit déjà l'informatique comme outil principal du contrôle opéré sur la population[7], 30 ans plus tard, le constat est aggravé : la démocratisation d'internet et le progrès technique ont introduit le numérique dans tous les aspects de notre vie, en faisant un enjeu déterminant pour le respect de la vie privée. Quand auparavant, la discipline nécessitait l'immobilisation de l'individu, aujourd'hui c'est la liberté et la circulation qui sont nécessaires au fonctionnement du pouvoir : c'est à travers nos traces numériques que notre liberté et notre vie privée sont mises en cause. Ces traces supposent du mouvement, une action. Or la plupart de nos actions engendrent aujourd'hui une trace numérique : écrire un mail, se déplacer dans la rue avec un téléphone, retirer de l'argent à un distributeur automatique, etc.

La société de surveillance disciplinait en traitant l'élément « anormal », en le séparant du reste de la société. A l'inverse, dans la société de contrôle, « les mécanismes de maîtrise se font toujours plus « démocratiques », toujours plus immanents au champ social, diffusés dans le cerveau et le corps de citoyens »[8]. Les actions simples décrites ci-dessus font en effet partie de la vie quotidienne. Même si aujourd'hui la question de la protection de la vie privée face au numérique est centrale, implicitement ces actions vont être considérées comme anodines avant d'être vues comme dangereuses.

Le numérique a dépassé depuis longtemps le stade de l'utilitaire et est aujourd'hui tout autant, sinon plus, un outil de divertissement qu'un outil pratique. Il engendre un besoin d'exposition. Pour Bernard E. Harcourt, professeur de droit à l'université de Colombia, ce besoin et ce désir de s'exposer marquent l'étape suivante de la société de contrôle : il parle de société d'exposition[9]. A la différence des modèles

[5] Foucault, *Surveiller*, op. cit., p. 207
[6] M. Foucault, *Dits et Écrits*, t. 2, Paris, Gallimard, 2001 p. 532-534
[7] Gilles Deleuze, *Post-scriptum sur les sociétés de contrôle*, dans *Pourparlers 1972 - 1990*, Paris, Les éditions de Minuit, 1990
[8] M. Hard & A. Negri, *Empire*, Cambridge, Harvard University Press, 2000, p. 48
[9] B. E. Harcourt, *La société d'exposition*, Paris, Seuil, 2020

de Foucault et de Deleuze, qui agissaient contre la volonté de l'individu, ici le pouvoir fonctionne en exploitant notre désir : « on n'est pas mis dans une cellule panoptique, on n'est pas coincés, ce n'est pas de la coercition, ça marche au désir, ça marche à notre volonté »[10]. Il explique que le cliché de la comparaison avec le « Big Brother » de George Orwell est éculé : la situation est différente, sinon pire que la société décrite dans *1984*. Il n'existe pas d'œil omniscient qui collecte des données sur une société opprimée par la puissance publique. L'information est souvent donnée librement par les individus eux-mêmes du fait de leur dépendance à la technologie. Le contrôle va bien au-delà de l'action de l'Etat : l'enjeu de la protection des données est plus centré autour de l'action des entités privées que de celles des pouvoirs publics.

Enfin, contrairement à la société décrite dans *1984*, l'enregistrement de nos actions par la trace numérique a dépassé depuis longtemps le seul objectif de surveillance. Le principal intérêt de nos données est leur monétisation. Les données personnelles permettent de cibler la publicité et d'identifier le besoin du consommateur, leur valeur économique est donc immense. Or il n'a jamais été aussi facile de les collecter : la gratuité est de mise sur internet, toute personne munie d'un ordinateur peut y accéder, il suffit ensuite d'exploiter l'énorme masse de données que les usagers livrent à la Toile chaque jour.

Cette facilité d'exploitation est la raison pour laquelle il est nécessaire de reprendre le contrôle de nos données personnelles. Le Conseil d'Etat déclarait en 1998 que l'espace d'internet « n'était pas naturellement celui du droit »[11]. Internet est un espace de liberté anonymisé qui transcende les frontières, il est donc en effet difficile de le réglementer. Le Règlement Général sur la Protection des Données (RGDP), entré en vigueur en 2018, est le dernier effort de l'Union Européenne en faveur de la protection des données personnelles des individus. C'est le premier texte normatif européen à contenir une définition du droit à l'oubli.

Selon l'article 17 de ce règlement, c'est le droit de la personne concernée « d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant »[12]. L'article expose ensuite les conditions dans lesquelles l'oubli peut s'opérer, puis il en définit les exceptions.

« Oubli » doit donc être compris comme « effacement ». Il est intéressant de noter que le titre de l'article dans le projet de RGPD était « droit à l'oubli numérique et à l'effacement » et qu'il est maintenant titré « droit à l'effacement (« droit à l'oubli ») ». L'expression a été reléguée entre des guillemets et des parenthèses. Ce changement

[10] *B. Harcourt : "Cette société d'exposition, est une société de servitude volontaire par la séduction",* émission *La grande table à idées*, podcast France Culture, 09/01/2020, à 6 minutes 4 secondes

[11] Conseil d'Etat, *Internet et les réseaux numériques,* rapport de Jean-François et Isabelle Falque-Pierrotin, 1998, p.6

[12] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD), article 17, alinéa 1

de titre reflète tout à fait ce que ces termes représentent. L'oubli n'est pas un concept juridique, le décréter est impossible.

En 2014, dans l'arrêt *Costeja c/ Google Spain*, à la suite de la consécration par la Cour de Justice de l'Union Européenne (CJUE) des conditions du droit au déréférencement[13], de nombreux auteurs ont pris peur en songeant aux conséquences de ce qu'ils ont appelés eux-mêmes le droit à l'oubli, car le terme n'apparait nulle part dans l'arrêt. L'assimilation de « l'oubli » au « déréférencement » est compréhensible : dans le projet de RGPD paru en 2012, le terme est évoqué ; or c'est à la lumière de ce projet que la CJUE a interprété la directive de 1995[14] sur la protection des données pour consacrer le droit au déréférencement. Toutefois, l'oubli est un mécanisme très humain, le transposer au domaine du droit n'est pas si simple.

Le processus de l'oubli du cerveau humain fait toujours l'objet de débat au sein de la communauté scientifique. Une chose est cependant sûre : si, dans l'opinion commune, l'oubli est vu comme une chose négative, les scientifiques s'accordent pour dire que c'est un mécanisme essentiel de la mémoire humaine. Nous ne parlons pas ici de l'oubli pathologique lié à l'amnésie ou à une maladie comme Alzheimer, mais simplement du mécanisme de déclin naturel de nos souvenirs propre à toute personne. L'hypermnésie, ou la capacité à pouvoir se rappeler de façon très précise une immense majorité de ses souvenirs, est en effet vue comme une pathologie[15]. « Nul bonheur, nulle sérénité, nulle espérance, nulle fierté, nulle jouissance de l'instant présent ne pourrait exister sans faculté d'oubli »[16] disait Nietzsche. L'oubli est salvateur, il permet de faire face à l'écoulement du temps : il nous empêche de ressasser le passé pour mieux se concentrer sur le moment présent.

S'il est reconnu comme une fonction cognitive indispensable, dans le domaine du droit la notion d'oubli engendre la méfiance. Il est possible de supprimer une information, mais la décréter « oubliée » revient à ordonner aux personnes qui s'en souviennent de la retirer de leur mémoire. Non seulement cela est digne d'un des pires scénarios d'anticipation orwellien, mais cela engendre un conflit avec d'autres libertés fondamentales. Une personne se souvenant d'une information décrétée oubliée n'aurait plus le droit de l'exprimer, ce qui serait une entrave à la liberté d'expression. Et tout autre individu souhaitant retrouver l'information frappée d'oubli en serait incapable, mettant ainsi en péril la liberté d'information et la liberté de la presse.

---

[13] CJUE, *Google Spain SL, Google Inc. / Agencia Española de Protección de Datos, Mario Costeja González*, C-131/12, 13 mai 2014

[14] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

[15] La première personne atteinte d'hypermnésie, une étatsunienne du nom de Jill Price, décrit sa mémoire comme « un fardeau », car le fait de se rappeler de tout a pour conséquence de vivre tout le temps dans le passé. Voir E. Parker, L. Cahill, J. L. Mcgaugh, *A Case of Unusual Autobiographical Remembering,* Neurocase, Février 2007, Volume 12(1), p. 35-49

[16] F. Nietzsche, *Considérations intempestives*, II, 1, 1874 tr. fr. Bianquis G., éd. Aubier-Montaigne

Le droit à l'oubli est donc un concept flou et ambigu. Les rédacteurs du RGPD lui ont préféré le terme « droit à l'effacement », mais ont quand même choisi de le conserver dans le titre de l'article 17. Peut-être que cette expression, si elle n'est pas très pertinente juridiquement, possède une connotation morale que n'a pas le droit à l'effacement. Droit à l'oubli évoque un droit au pardon, à la rédemption, le droit de voir nos actes passés ne plus resurgir sur le devant de la scène. Il ne s'agit pas simplement de voir son passé effacé, mais plutôt de pouvoir profiter du présent sereinement.

« C'est précisément pour éviter les conséquences néfastes ou douloureuses de ces rappels d'informations que le concept de droit à l'oubli a été imaginé »[17]. Apparu pour la première fois en 1966, sous la plume du professeur Gérard Lyon-Caen, celui-ci le définissait en effet comme « la prescription de faits qui ne sont plus d'actualité »[18]. Il commentait une décision du Tribunal de Grande Instance de Seine, qui statuait sur la demande d'une ancienne maîtresse du célèbre Landru de recevoir des dommages et intérêts pour le préjudice causé par la diffusion d'un film sur ce dernier[19]. Une dizaine d'années plus tard, lors de l'élaboration de la loi Informatique et Libertés[20], le sénateur Jacques Thyraud relève dans l'article 26 une consécration du droit à l'oubli. Il dit que « l'informatique a apporté essentiellement un changement de dimension : elle a introduit, en effet, une capacité de mémorisation considérable au point que certains peuvent craindre qu'elle ne porte atteinte à l'un des droits les plus fondamentaux de l'être humain : le droit à l'oubli » [21]. Son observation était visionnaire : le progrès technologique et l'émergence d'internet a donné une nouvelle vie à l'expression, qui était restée comme outil corolaire au droit à la prescription.

Au niveau européen, le Conseil de l'Europe consacre l'existence d'un droit à l'effacement dans la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel de 1981. Elle dispose que « Toute personne doit pouvoir obtenir, le cas échéant, la rectification de ces données ou leur effacement lorsqu'elles ont été traitées en violation des dispositions du droit interne donnant effet aux principes de base énoncés dans les articles 5 et 6 de la présente Convention »[22]. Cette convention a grandement inspiré la première initiative de l'Union Européenne visant à réguler les données personnelles : la directive 95/46/CE de 1997. C'est la CJUE qui a déduit de cette directive l'existence d'un droit au déréférencement en 2014 dans l'arrêt *Costeja c/ Google Spain*, déjà cité plus haut.

En Europe, le droit à l'oubli a donc une histoire et est ancré dans le champ du droit. L'article 17 du RGPD n'est pas si novateur. Il regroupe des principes déjà existants. Le droit à l'effacement, même s'il n'est pas précisément défini, figure après

[17] Boizard, Maryline*, Le temps, le droit à l'oubli et le droit à l'effacement*, *Les Cahiers de la Justice*, vol. 4, no. 4, 2016, pp. 619-628.
[18] C. Costaz, *Le droit à l'oubli,* Gaz. Pal 1995. 2 Doctr. 965
[19] TGI Seine, 4 oct. 1965, JCP 1966 II, 14482, obs. Lyon-Caen
[20] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
[21] J. Thyraud, Rapport n°72 relatif à la loi Informatique et libertés, 1977, p. 6
[22] Convention STCE 108 du 28 janvier 1981, article 8, c)

tout dans la convention de 1981 du Conseil de l'Europe imaginée 25 ans avant le RGPD. Soulignons tout de même qu'une des nouveautés apportée par le RGPD par rapport à la décision *Google Spain* est d'avoir élargi le déréférencement en instituant un droit à l'effacement. Le déréférencement n'est qu'une méthode parmi d'autres pour exercer ce droit.

Aux Etats-Unis, la situation n'est pas du tout la même. L'expression est plus ou moins inconnue avant le projet de RGPD de 2012, qui a fait réagir outre-Atlantique de par sa vocation à s'appliquer à toutes les entreprises qui offriraient des services à des européens, peu importe leur implantation territoriale[23]. Le droit à l'oubli a même été qualifié de « plus grande menace pour la liberté d'expression sur internet de la prochaine décennie »[24]. Même si la portée de l'article 17 est limitée, notamment au regard de la liberté d'information et de la liberté d'expression[25], la conception de la liberté d'expression aux Etats-Unis est totalement différente de celle des européens. Le sacro-saint 1er Amendement est à l'origine de nombreuses libertés, dont celle de commercer. En obligeant des entreprises comme Google ou Facebook à se conformer au RGPD, cette liberté pourrait être menacée, et les garanties fournies par l'article 17 pourraient ne pas suffire. Là réside l'intérêt de la comparaison : mettre en lumière ce que pourrait être le droit à l'oubli aux Etats-Unis face au sens qu'il revêt déjà en Europe.

Les tribunaux étatsuniens ont été confrontés à la même question de savoir si les individus avaient le droit de voir leur passé retiré des médias ou d'œuvres artistiques à leur demande. Dans une affaire *Melvin v/ Reid*[26], une ancienne prostituée découvrait en 1930 l'existence d'un film relatant les épisodes de sa vie passée qu'elle souhaitait voir oubliée. En utilisant « le droit au bonheur » de l'article 1er de la Constitution Californienne[27], les juges de la Cour d'appel donnent droit au demandeur à des dommages et intérêts contre le producteur du film. La comparaison avec l'affaire de la veuve Landru (précédemment citée) est intéressante : les faits sont très similaires, même si la solution est différente. Dans les deux arrêts, il y a l'idée du droit à la réinsertion, le droit d'avoir la maîtrise sur sa vie privée passée. Là où les juges californiens ont loué et protégé la réinsertion du demandeur, les juges français vont partiellement débouter la requérante en mentionnant l'objectivité du film de Claude Chabrol. On voit donc que, tout comme en France, c'est en tant que droit à la réhabilitation que sont apparus les premiers germes de ce que pourrait être le droit à l'oubli.

---

[23] Règlement n°2016/679, dit Règlement Général sur la Protection des Données, 2018, article 3, alinéa 2

[24] "*in fact it represents the biggest threat to free speech on the Internet in the coming decade*", J. Rosen, *The right to be Forgotten*, 64 Stanford Law Review online 88, p.1

[25] Règlement n°2016/679, dit Règlement Général sur la Protection des Données, 2018, article 17, alinéa 3, a)

[26] *Melvin v. Reid,* 112 Cal.App. 285, 297 P. 91, 1931

[27] *"pursuing and obtaining safety, happiness, and privacy",* Article 1er de la Constitution Californienne

Les juges californiens n'avaient pas d'autres choix que d'utiliser le concept vague de ce droit au bonheur. En tant que système de *common law*, l'Etat de Californie ne disposait pas de principe de responsabilité général de celui qui commet un dommage. Le droit de la responsabilité étatsunien utilise le modèle des *torts*, or le *tort* de *public disclosure of private facts* n'existait pas encore. Retenu en 1976 dans le *Restatement (Second) of Torts* et adopté par la plupart des Etats, ce tort est encore aujourd'hui l'outil principal pour réglementer l'atteinte à la vie privée des personnes dans les médias. Il dispose que constitue une ingérence « la révélation au public de faits qui relèvent manifestement de la vie privée d'autrui, à condition que ces faits soient de nature à choquer toute personne raisonnable et qu'ils ne présentent pas d'éléments de nature à éveiller un intérêt légitime dans le public »[28]. Nous verrons que ce *tort* n'est pas très efficace, essentiellement en raison de cette condition limitative d'intérêt légitime du public visant à protéger la liberté d'information et laissée à l'appréciation très large des tribunaux.

Comme dernière référence au droit à l'oubli, on peut citer une disposition des *Fair Informations Practices*, des recommandations adoptées par le *United States Department of Health* en 1973 pour protéger le traitement des données personnelles des individus. Cette disposition recommande qu'un « individu devrait avoir le droit de contester une donnée associée à sa personne, et si cette contestation aboutit, d'avoir la possibilité d'effacer, rectifier, compléter ou amender cette information »[29]. Ces recommandations vont inspirer une majeure partie des textes adoptés par le Congrès destinés à protéger la vie privée et les données numériques. Finalement, la disposition concernant le droit à l'oubli ne sera reprise que pour le *Children's Online Protection Act* de 1998[30]. Jusqu'à aujourd'hui, le droit à l'oubli aux Etats-Unis concerne donc uniquement les mineurs et n'est protégé formellement que par ce texte.

Enfin, il convient de préciser que la protection des données aux Etats-Unis a été élaborée sous la forme de textes législatifs très ciblés, portant sur la sécurité sociale[31], les communications électroniques[32] ou le droit des enfants, comme cité plus haut. Adoptés pour répondre à des problématiques différentes du droit à l'oubli, notamment des problèmes d'hacking ou de télémarketing, ils ne permettent pas vraiment l'effacement des données personnelles à la demande de l'utilisateur. Le

---

[28] "*One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that:*
(a) would be highly offensive to a reasonable person
(b) is not of legitimate concern to the public"
Restatement (Second) of Torts, § 652(D), 1977

[29] "*An individual should have the right to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended*" Code of fair information Practices, élaboré par le Unified States Department of Health, Education and Welfare, 1973

[30] "*The opportunity [of the parent] at any time to refuse to permit the operator's further use or future online collection of personal information from that child, and to direct the operator to delete the child's personal information",* Children's Online Privacy Protection Act of 1998, public law n°106-170, 15 U.S.C. 6501–6505, §312.6 (2)

[31] Health Insurance Portability Act of 1996, public law 104–191

[32] Cable Communications Policy Act of 1984, public law 98-549, U.S.C. §551

pragmatisme cher aux systèmes de *common law* est en cause : constatant les lacunes des tribunaux dans ce domaine, le Congrès a cherché avec chacun de ces textes à répondre à un problème spécifique. L'avantage est que ces textes sont efficaces dans leur finalité, mais ils peuvent difficilement être utilisés pour un problème corolaire mais différent de leur objectif premier. Les systèmes de *common law* étants réticents à l'élaboration de grands textes généraux, et les Etats-Unis ne faisant pas exception, ils ne possèdent pas de texte général, comme le RGPD, qui serait susceptible de mieux protéger les données personnelles des individus.

Le constat est donc clair : avec des textes efficaces, mais trop ciblés, et un droit à l'oubli qui est resté cantonné au domaine du respect du droit à la vie privée en tant que droit au pardon, le droit à l'effacement tel qu'entendu par l'article 17 du RGPD semble être très peu présent aux Etats-Unis.

Tout au long de cette étude comparative, nous proposons d'identifier et d'analyser les limitations empêchant la mise en place d'un véritable droit à l'oubli aux Etats-Unis, tel qu'il se dessine en France et en Europe.

Il est nécessaire de définir et explorer le fondement juridique du droit à l'oubli qu'est la vie privée dans chacun des systèmes (I). Il s'agira ensuite de comparer l'exercice de ce droit à l'oubli dans les deux ordres juridiques, à travers les conditions et les limitations qui lui sont opposées. (II).

TITRE 1 / La vie privée : fondement du droit à l'oubli

Les premières apparitions du droit à l'oubli découlent d'un souci de respect de la vie privée. Même si aujourd'hui, c'est dans une optique plus ciblée de protection des données qu'il est envisagé, son principal fondement reste le droit à la vie privée. Pour mieux comprendre l'écart de protection du droit à l'oubli entre le système français et le système étatsunien, il est donc nécessaire de comparer leur conception du droit à la vie privée et la façon dont il est sauvegardé. Il faut commencer par préciser que, aux Etats-Unis, c'est une notion englobant plusieurs droits très différents, alors qu'en France, le droit à la vie privée est un grand principe unifiant toutes les formes du respect de la vie privée (1). Après avoir établi cette distinction, il sera nécessaire de comparer l'étendue du droit à la protection des données dans les deux pays (2).

Chapitre 1 : un domaine de la vie privée différemment défini entre les deux pays

Aux Etats-Unis, il y a une distinction très nette entre droit à la vie privée au sens de droit à l'autonomie de la volonté et le droit à la protection des données personnelles (1). La situation en France est plus complexe, car les deux droits semblent être pour l'instant unifiés (2).

Section 1 : Aux Etats-Unis, une notion divisée

Aux Etats-Unis, le droit au respect de la vie privée est mentionné pour la première fois dans un célèbre article de 1890 intitulé « *the right to privacy* »[33]. Les deux avocats l'ayant écrit plaidaient pour la consécration d'un droit à être laissé tranquille, notamment par la presse à scandale. Ce droit devait se matérialiser par la création d'un nouveau délit dans le droit de la responsabilité de la *common law*. Le développement de la photographie et des nouvelles technologies menaçait en effet la vie privée des individus. Ce n'était pas un enjeu majeur avant la fin du XIXe siècle, raison pour laquelle ce droit ne figure ni dans la Déclaration des Droit de l'Homme de 1789 ni dans les amendements de la Constitution américaine. A la suite de cet article, les cours et les Etats américains vont reprendre à leur compte ce délit d'intrusion dans la vie privée dans le droit des *torts.* Dès le début du siècle, le droit à être laissé tranquille va donc recevoir une application horizontale, c'est-à-dire qu'il devra être respecté entre les personnes privées. L'application verticale de ce droit sera adoptée

[33] Samuel Warren, Louis Brandeis, *The right to privacy*, Harvard Law Review, vol. 4, 1890, pp. 193-220

plus tard dans le XXè siècle avec l'arrêt *Grisworld v. Connecticut*[34], qui consacrera constitutionnellement le droit à la vie privée en le dégageant des zones d'ombre de la Constitution.

Dans cet arrêt, il était question de l'intrusion des forces de police dans la vie conjugale pour empêcher la prise de contraceptifs. Il ne s'agissait donc pas tant de constitutionaliser la prise de contraceptifs que de protéger le secret de la vie privée face à l'intrusion étatique. Plus tard, dans l'arrêt *Roe v. Wade*[35], la Cour Suprême protège le droit à l'autonomie de la personne, le droit à pouvoir faire des choix, en l'occurrence celui d'avorter. On passe donc du droit à ne pas subir une intrusion à un droit général d'autonomie. Cette protection de l'autonomie du choix servira de fondement pour autoriser le mariage entre personnes de couleurs de peau différentes[36] et, plus récemment, au mariage entre personnes de même sexe[37].

Ce droit à l'autonomie de l'individu est donc protégé constitutionnellement et, même si sa consécration a soulevé de nombreuses critiques, son existence n'est plus remise en cause aujourd'hui. Ce droit rassemble le volet positif de la sauvegarde de la vie privée, dans le sens où il n'empêche pas mais au contraire il permet.

Le volet de la protection de la vie privée au sens strict, c'est-à-dire qui empêche l'intrusion, est complètement séparé de ce volet de l'autonomie de l'individu. Alors que cette dernière est fondée sur la *liberty* mentionnée dans le 14e amendement et est incorporée dans la clause de *due process*, la protection du secret de la vie privée est protégée par le 4e amendement, qui offre des garanties pénales contre les fouilles et les perquisitions intrusives de l'Etat. Il s'agit toujours de protection de la vie privée, mais dans un sens tout à fait différent de celui dégagé de la *liberty* du 14e amendement. A côté de ces garanties en matière de procédure pénale qui ont leur propre histoire jurisprudentielle (qui tend d'ailleurs à voir l'érosion de ces garanties), il existe aussi la jurisprudence liée à la protection des données, qui est la plus lacunaire au niveau constitutionnel. Nous verrons en effet que la Cour Suprême a refusé par deux fois de consacrer un droit à la protection des données. En dehors du volet constitutionnel, le *Privacy Act* de 1974 instaure un semblant de protection des données au niveau fédéral avec de nombreuses exceptions.

Dans son opinion de l'arrêt *Grisworld*, le juge Hugo Black écrivait que la vie privée est un concept « large, abstrait et ambigu »[38]. Le juge à l'initiative de la consécration constitutionnelle du droit à la vie privée avoue donc lui-même la complexité et la polysémie du terme. La vie privée comme nous l'entendons en France ne revêt pas moins de trois sens différents outre-Atlantique, chacun possédant sa propre construction jurisprudentielle et ses propres fondements. Il faut distinguer la *liberty*, de *l'informational privacy*, qui ne sont pas protégés du tout avec la même

[34] *Grisworld v. Connecticut*, 381 U.S. 479, 1965
[35] *Roe v/ Wade*, 410 U.S. 113, 1973
[36] *Loving v. Virginia*, 388 U.S. 1, 1967
[37] *Obergell v. Hodges*, 576 U.S. 644, 2015
[38] *Grisworld v. Connecticut*, 381 U.S. 479, 1965

intensité. Cela pose aussi la question de la portée réelle du droit au respect de la vie privée. Englobe-t-il aussi bien le droit à l'autonomie de la personne que le droit à la protection des données ? Ou bien le droit à la protection des données serait-il un droit à part, certes découlant du droit à la vie privée mais devant être consacré séparément de manière formelle ? Peut-être que le modèle étatsunien est plus pertinent que le modèle français sur ce point, car si la vie privée n'est pas protégée également sur tous ses versants, au moins est-elle segmentée en fonction de ce qu'elle protège, ce qui permet de préciser au mieux son régime dans chaque domaine. En France, la construction jurisprudentielle autour de l'article 9 du Code Civil amène à penser que la vie privée est un fourre-tout englobant aussi bien l'autonomie de l'individu que la protection d'autrui dans son espace vital ou que la protection des données.

Section 2 : En France, une notion unifiée

Alors que l'article fondateur du droit au respect de la vie privée aux Etats-Unis est paru en 1890, ce n'est que beaucoup plus tard que la notion sera intégrée dans le spectre juridique français. Absente de la Constitution de la IVème comme de la Vème République, elle ne fera son apparition qu'en 1970, dans la lettre de l'article 9 du Code Civil. En 1974, lors de la ratification de la Convention Européenne de Sauvegarde des Droits de l'Homme et des Libertés Fondamentales, la France accepte se plier à l'article 8 de la Convention, qui impose lui aussi le respect de la vie privée d'autrui. Par la suite, la jurisprudence de la CEDH sur la vie privée aura une grande influence sur la construction de ce droit en France.

L'article 9 du Code Civil dispose simplement que « chacun a droit au respect de sa vie privée », suivie dans le second alinéa de mentions concernant le pouvoir conféré au juge de prendre des dispositions pour faire cesser une atteinte à la vie privée. A noter que, aux Etats-Unis, il n'existe pas de texte général sur la vie privée. Il y a le droit des *torts*, propre à chaque Etat mais globalement unifié en ce qui concerne la vie privée, il existe la jurisprudence étatique qui précise le régime de ces *torts* et il y a les décisions de la Cour Suprême qui ont dégagé la notion de vie privée des amendements à la Constitution. On retrouve ici les caractéristiques d'un système de *common law*, réticent aux principes généraux et utilisant la législation pour des faits très précis, d'où le droit des torts, qui consiste en une longue liste de cas où la responsabilité d'une personne peut être engagée.

En France, la protection de la vie privée dans le volet civil consiste donc seulement en un principe général très lapidaire. C'est seulement à travers la jurisprudence que l'on peut délimiter le domaine et le régime de la vie privée, car le texte ne contient aucune précision sur l'application du respect de ce droit.

Comme aux Etats-Unis, on retrouve en France le sens de la liberté négative, c'est-à-dire la protection de l'intimité des personnes contre les intrusions[39]. Il faut préciser que le droit à l'image, qui découle de cette sauvegarde de l'intimité, est considéré comme un droit distinct de la vie privée depuis 2005[40]. Est présente également l'affirmation positive de la liberté via la jurisprudence de la Cour Européenne des Droits de l'Homme, dont les magistrats ont décidé que le choix d'avoir des enfants[41] ou celui de faire une interruption volontaire de grossesse[42] fait partie de la vie privée de l'individu. L'autonomie de la volonté de l'individu, pierre angulaire de la jurisprudence constitutionnelle américaine sur la vie privée, se retrouve donc aussi en France.

Il existe une mention de l'atteinte au droit au respect de la vie privée dans le Code Pénal aux articles 226-1 et suivant. La constitution de l'atteinte est ici bien plus précise, puisqu'elle est caractérisée « en captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privée ou confidentiel ». L'atteinte est valable aussi pour la captation d'images. A la différence des Etats-Unis, où le volet pénal du respect de la vie privée concerne l'intégrité du domicile et de la personne, là il concerne uniquement la captation d'image ou de paroles ainsi que leur détention. Même si cette disposition figure dans le code pénal, son fondement n'en reste pas moins le principe général du droit au respect à la vie privée. La preuve est que cet article a été rédigé en même temps que l'article 9 du Code Civil, en 1970. Le législateur a simplement voulu ériger une partie spécifique du non-respect de la vie privée au rang d'infraction.

La protection des données personnelles est, elle aussi, unifiée sous la bannière de l'article 9 du Code Civil. Aux Etats-Unis, ce qu'ils appellent *informational privacy* est strictement séparé de la *liberty* protégée par le 14ème amendement. L'équivalent le plus proche de cette « vie privée informationnelle » que la France possède est la protection des données et celle-ci n'est pas séparée de la vie privée.

La CEDH a en effet basé plusieurs de ses décisions concernant la protection des données sur l'article 8 de la Convention. Elle a par exemple statué que certaines informations publiques recueillies par les autorités publiques peuvent relever de la vie privée[43]. Dans une autre décision, elle a même fondé une obligation positive de protection des données sur l'article 8 de la Convention. Depuis, les Etats ont l'obligation de permettre aux intéressés de pouvoir accéder de façon effective à toutes leurs informations[44]. On note ici que le RGPD a grandement été influencé par le Conseil de l'Europe, puisqu'on retrouve les dispositions de ces arrêts dans son

[39] « est illicite toute immixtion arbitraire dans la vie d'autrui » Civ. 1ère , 6 mars 1996, n° 94-11273
[40] Civ. 1ère, 10 mai 2005, n°02-14.730
[41] CEDH, sect. III, 2 octobre 2012, Knecht c/ Roumanie, n° 10048/10
[42] CEDH, sect. IV, 20 mars 2007, Tysiac c/ Pologne, n°5410/03
[43] CEDH sect. II, 18 novembre 2008, C. c/ Turquie, n°22427/04
[44] CEDH sect. III, 27 octobre 2009, H c/ Roumanie, n°21737/03

contenu[45]. Le Conseil Constitutionnel a mis sa pierre à l'édifice en prescrivant que la collecte, l'enregistrement ou la conservation de données personnelles doivent être justifiées par un motif d'intérêt général imposé par le droit au respect de la vie privée.

Relevons également que la Charte des Droits Fondamentaux, dans son caractère résolument moderne, distingue un droit à la protection des données différent du droit à la vie privée[46]. Il y a donc un décalage entre la perception française de la vie privée et celle de l'Union européenne, alors que le Conseil de l'Europe semble pencher lui aussi du côté de l'unité de la vie privée.

L'intérêt de savoir si la distinction entre données personnelles et vie privée n'a pas seulement un intérêt de classification, elle permettrait effectivement de clarifier mieux le régime des deux notions. Par exemple, dans la loi informatique et libertés, désormais obsolète, l'article 5 dispose que :

« Sont soumis à la présente loi les traitements de données à caractère personnel :

1° Dont le responsable est établi sur le territoire français. Le responsable d'un traitement qui exerce une activité sur le territoire français dans le cadre d'une installation, quelle que soit sa forme juridique, y est considéré comme établi ;

2° Dont le responsable, sans être établi sur le territoire français ou sur celui d'un autre Etat membre de la Communauté européenne, recourt à des moyens de traitement situés sur le territoire français, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur ce territoire ou sur celui d'un autre Etat membre de la Communauté européenne. »

Si le point 2 laisse penser qu'un utilisateur en dehors de l'Union pourrait voir la loi s'appliquer à lui, le juge français a pour l'instant refusé d'appliquer cette loi aux responsables de traitements situés en dehors de son territoire[47]. Dans les faits, il existe donc une limitation géographique inhérente aux données personnelles. Cependant, il n'existe pas de limitation géographique pour la protection de la vie privée. L'article 113-2 du Code Pénal dispose que « La loi pénale française est applicable aux infractions commises sur le territoire de la République. L'infraction est réputée commise sur le territoire de la République dès lors qu'un de ses faits constitutifs a eu lieu sur ce territoire. » La chambre criminelle a considéré par ailleurs que, pour les infractions commises sur internet, la loi française devrait s'appliquer[48]. « Par analogie, il est alors

[45] « La personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données à caractère personnel » RGPD, article 15

[46] « toute personne a droit à la protection des données à caractère personnel la concernant » article 8.1, Charte des Droits Fondamentaux

[47] TGI Paris, 14 avril 2008. En l'espèce, une personne souhaitait voir certaines informations inscrites sur google supprimées en se fondant sur la loi informatique et libertés. Le tribunal a refusé l'application de la loi française. Elle a considéré que google.fr n'était pas le responsable du traitement, et que les moyens de traitements utilisés étaient implantés en Californie chez Google.Inc. C'est donc la loi californienne qui s'appliquait.

[48] Cass. Crim, 14 décembre 2010, n°10-80.088

aisé de considérer que la loi pénale française serait applicable à un responsable de traitement établi hors de l'Union européenne, pourvu que l'atteinte portée aux données à caractère personnel soit constitutive d'une infraction pénale »[49].

Selon cette analyse, il existe tout de même une certaine étanchéité entre la notion de donnée personnelle et celle de vie privée. En surface, la première impression est que la notion de vie privée regroupe aussi bien la liberté individuelle que les données personnelles, mais la différence de régime décrite plus haut prouve le contraire. Cette différence ne semble pas être voulue, elle semble seulement liée à une mauvaise définition des deux termes et de leur domaine.

Il est donc primordial de bien définir ce qu'est la vie privée et ce que sont les données personnelles. En France, la limite est encore floue, alors qu'aux Etats-Unis, la séparation est très nette et n'est pas sujette à débat. Le droit aux données personnelles existe, la loi Informatique et Libertés ainsi que la jurisprudence de l'article 9 du Code Civil le démontre bien, pourtant en droit interne il lui manque une présence plus affirmée, qui lui conférerait la codification ou la constitutionnalisation.

Il est compliqué de situer le droit à l'oubli dans cet environnement juridique. Quand les frontières des données personnelles et de la vie privée sont aussi vagues, où situer ce droit nouveau enfanté par ces deux notions ? Il est né pour protéger la vie privée, il est maintenant utilisé pour la protection des données. Préciser le domaine de ces droits aidera à circonscrire un droit à l'oubli dont on a pour l'instant du mal à discerner le contour.

[49] L. Chelby, « Droit à l'oubli numérique la loi informatique et libertés, et le projet de règlement européen », dans *Le droit à l'oubli numérique – données numériques, approche comparée*, 1ère ed., édition Larcier, Bruxelles, 2015, p. 105

Chapitre 2 / Les données personnelles : un droit protégé inégalement

Après avoir défini le domaine de la protection des données dans les deux pays, il est maintenant nécessaire d'étudier l'étendue de cette protection. Cela servira à mieux cerner la possibilité du droit à l'oubli. Sur le plan constitutionnel, c'est l'intensité de la protection qui est inégale, puisqu'en France le droit est consacré sous la forme de la vie privée alors qu'il ne l'est pas aux Etats-Unis (1). Sur le plan législatif, c'est sur la forme que les deux systèmes diffèrent, puisque outre-Atlantique c'est la protection sectorielle qui est privilégiée, alors que l'Hexagone a préféré une suite de lois plus générales (2).

Section 1 / La protection constitutionnelle des données personnelles

L'étude du spectre constitutionnel en protection des données sera faite d'abord par celui des Etats-Unis (A) et ensuite celui de la France (B).

A) Le cadre constitutionnel des Etats-Unis

Précédemment, il a été dit que le volet autonomie de la vie privée avait été consacré aux Etats-Unis dans l'arrêt *Grisworld v. Connecticut* puis que son régime avait été précisé dans la célèbre affaire *Roe v. Wade*. Qu'en est-il des données personnelles ? Par trois fois, la constitutionnalisation de ce que les Etats-Unis appellent *informational privacy* a été débattue et par trois fois elle a été rejetée. En France, si le droit n'existe pas en tant que tel, il a été reconnu sous l'égide de la vie privée.

Nous avons vu que la vie privée au sens de la protection contre les intrusions est discernable dans le 4ème amendement qui règlemente les perquisitions et les saisies de l'Etat sur la propriété des personnes. Ce volet de la vie privée dispose de sa propre jurisprudence se rapportant uniquement à la procédure pénale. Pour les arrêts sur la protection des données, c'est successivement cet amendement et le 14ème relatif à la « liberty » visée dans l'arrêt *Roe v/ Wade* qui vont être utilisés pour rejeter le pourvoi.

Dans l'arrêt *Whalen v/ Roe*[50], il s'agissait de contester la constitutionalité d'une loi New-Yorkaise qui établissait une liste de médicaments potentiellement dangereux. Les personnes achetant ces médicaments en pharmacie avaient l'obligation d'indiquer sur un formulaire certaines informations personnelles comme leur âge, leur nom et leur

[50] *Whalen v. Roe*, 429 U.S. 589, 1977

adresse. Ces documents étaient ensuite compilés numériquement. Les demandeurs avançaient que cette mesure n'était pas justifiée et attentait à leur vie privée sur plusieurs plans. Elle limite tout d'abord leur autonomie à faire des choix, dans le sens où la rétention d'information peut les dissuader d'acheter les médicaments. Par ailleurs, ils soutiennent que la collecte d'informations est une intrusion non-nécessaire dans leur vie privée. La vie privée du 4ème amendement et celle du 14ème sont donc en jeu ici, et la Cour Suprême en fait bien la distinction[51]. La décision, même si elle est unanime, ne rejette pas en bloc les prétentions des parties. La Cour reconnait que la concentration de grandes quantités de données est une menace pour la vie privée. Elle énonce même que, sous certaines circonstances, le droit à avoir ses données protégées pourrait avoir une assise constitutionnelle[52]. Cependant, elle argumente que, dans le cas de l'espèce, la collecte d'information n'est pas une atteinte sérieuse et est proportionnée. D'une part, elle déclare qu'il n'y a aucune preuve que la collecte d'information fasse l'objet d'un traitement autre que la finalité initiale. Les informations sont sécurisées. D'autre part, la compilation d'informations médicales est nécessaire et faite par des « pratiques de la médecine moderne »[53].

La Cour Suprême opère donc un simple contrôle de proportionnalité mais ne conteste pas l'existence d'un droit aux données personnelles. Il n'en reste pas moins que le contrôle opéré est assez léger. La cour de district avait relevé dans l'échelon précédent que l'Etat de New York n'avait pas pu justifier la nécessité de la collecte. La Cour Suprême énonce toutefois que ce n'est pas une raison pour rendre la loi inconstitutionnelle, et que l'Etat de New York a simplement fait usage de son pouvoir souverain de police. Aucun critère ni faisceau d'indice n'a été donc identifié, on voit donc mal comment une loi pourrait être jugée inconstitutionnelle après un tel contrôle de proportionnalité. La Cour Suprême pourrait énoncer à chaque affaire que l'Etat était dans le bon droit d'utiliser son pouvoir législatif comme il le voulait.

Le fait de dire qu'il n'existe aucune preuve que les informations ne seront pas traitées autrement que pour leur première finalité suffit donc à valider le traitement litigieux. A contrario, la reconnaissance d'un droit à la protection des données exigerait la preuve d'une mauvaise utilisation des données. Or ce n'est pas seulement le traitement illicite des données qui devrait être prohibé, mais aussi sa simple collecte lorsqu'elle concerne des informations trop sensibles. Apporter ce type de preuve est

---

[51] « *The cases sometimes characterized as protecting "privacy" have in fact involved at least two different kinds of interests. One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions. Appellees argue that both of these interests are impaired by this statute » Whalen v. Roe*, 429 U.S. 598, 599, 600

52 « Recognizing that, in some circumstances, that duty arguably has its roots in the Constitution » Whalen v. Roe, 429 U.S. 605

53 « disclosures of private medical information to doctors, to hospital personnel, to insurance companies, and to public health agencies are often an essential part of modern medical practice » Whalen v. Roe, 429 U.S. 602

en plus très compliqué. La reconnaissance constitutionnelle de la protection des données semble donc compromise.

La même année, la Cour Suprême va avoir l'occasion de préciser sa jurisprudence avec l'arrêt *Nixon v/ Administration of General Services*[54]. L'arrêt oppose l'ex-président Nixon et l'administration américaine. Celle-ci avait émis un règlement permettant la saisie de tous les « documents présidentiels » que Nixon possédait pour les archiver. Il était convenu de retourner à Nixon les documents de nature privée qui auraient pu se trouver dans les documents traités.

Nixon reproche donc à ce règlement d'ingérer dans sa vie privée. La Cour Suprême va rejeter sa demande. Comme dans *Whalen*, elle va considérer qu'il existe une espérance légitime de vie privée pour les communications personnelles du demandeur. La Cour va toutefois changer son raisonnement. Au lieu d'effectuer un contrôle de proportionnalité de l'acte, elle va mettre en balance les intérêts du public et de l'archivage avec la préservation de la vie privée du Président. Cette mise en balance des intérêts et cette notion d'espérance légitime sont propres à la jurisprudence du 4ème amendement sur l'intrusion de l'Etat dans le domicile de la personne[55]. Alors que l'arrêt *Whalen* se rapprochait plutôt de la jurisprudence du 14ème amendement, celui-ci raisonne sur la base du 4ème. Cela montre bien que la protection des données est un droit nouveau et complexe, et que la Cour Suprême hésite encore sur le fondement qu'elle doit lui conférer.

La solution est ici plus argumentée que dans *Whalen*. La saisie concernait 42 millions de pages et 880 enregistrements, et seule une infime partie concernait la vie privée du Président, le reste rapportant ses actes pendant l'exercice de sa fonction. Il était de plus convenu que la partie non-officielle des documents allait être rendue à Nixon à la fin du traitement. Le fait qu'un très faible pourcentage de la saisie relève de la vie privée du demandeur n'écarte pas tout droit à la vie privée, disent les juges, mais dans le cadre d'un *balancing test*, cela suffit à écarter l'intrusion à la vie privée pour préserver l'intérêt d'archiver. Notons que cette décision n'était pas unanime, deux juges ont émis une opinion dissidente, trouvant la mesure trop intrusive.

Pour la seconde fois, les prémices d'un droit à *l'informational privacy* son esquissés mais cette fois aussi la finalité de l'intrusion l'emporte. Dans *Whalen*, c'est le pouvoir de police de l'Etat de New York qui était invoqué, ici ce sont l'intérêt du public à savoir et l'archivage. Le droit est reconnu mais pas consacré, ce qui va être dénoncé par le juge Scalia dans le dernier arrêt en date sur le sujet.

En l'espèce, des employés d'une société affiliée à la NASA se sont plaints d'une enquête sur leur passé effectuée avant leur recrutement[56]. Cette enquête se déroulait en deux temps. La personne devait d'abord remplir un formulaire en mentionnant des informations tel que le nom, l'adresse, les expériences professionnelles passées ou la

[54] *Nixon v/ Administration of General Services*, 433 U.S. 425, 1977
[55] *Katz v/ United States*, 389 U.S. 387, 1967
[56] *Nasa v. Nelson*, 562 U.S. 134, 2011

prise de substance illicite. La personne autorise ensuite la NASA à envoyer des demandes d'information complémentaires aux anciens employeurs, aux écoles et tout autre organisme susceptible de donner plus d'informations sur le candidat. Ces compléments d'information comportent notamment des demandes de renseignement sur l'intégrité financière, l'abus d'alcool et de drogues ou la stabilité émotionnelle et mentale. Les demandeurs dénoncent donc l'intrusion de ces enquêtes dans leur vie privée informationnelle.

34 ans après l'arrêt *Whalen*, la Cour Suprême va réaffirmer que *l'informational privacy* pourrait exister. Toutefois, comme pour les autres arrêts, la violation de ce droit hypothétique est justifiée. La Cour utilise la formulation suivante qui est très parlante :

"Assuming, without deciding, that the Government's challenged inquiries implicate a privacy interest of constitutional significance, that interest, whatever its scope, does not prevent the Government from asking reasonable questions of the sort included on SF–85 and Form 42 in an employment background investigation that is subject to the Privacy Act's safeguards against public disclosure"[57]

Le fait de dire « assuming, without deciding » veut bien dire que ce droit est toujours hypothétique, et que l'affaire est décidée sur sa base alors qu'il n'est pas consacré. Il est écrit textuellement que même si ce droit existait, il n'y aurait pas d'atteinte à la vie privée. Le problème va donc bien au-delà de l'existence de la vie privée informationnelle dans l'ordre constitutionnel. Même dans le cas où elle existerait, elle serait inefficace, la Cour l'a montré à trois reprises dans chaque décision. Pendant 34 ans, les juges ont fait miroiter la possibilité d'un droit qui de toute façon n'aurait aucune utilité.

Malgré son profond accord avec la décision, le juge Scalia va souligner dans sa *concurring opinion* l'hypocrisie de la Cour quant au perpétuel miroitement de ce droit. Il critique la tiédeur de la Cour Suprême, en ce qu'elle identifie toujours ce droit à la vie privée informationnelle dans la périphérie de la Constitution sans jamais l'intégrer. Il vaudrait mieux déclarer que le droit n'existe tout simplement pas, et c'est d'ailleurs le cas selon lui[58]. Il dit littéralement que le raisonnement de la cour n'a pas de sens, que fonder une décision sur un fondement inexistant heurte l'image et l'intelligence de la Cour[59].

La reconnaissance de la protection des données semble donc impossible, malgré ce que soutient l'opinion majoritaire de la Cour. Le fait le plus parlant est l'absence totale d'une seule citation de la Constitution dans les prétentions des parties. Ils soutiennent simplement que le gouvernement fédéral viole la Constitution avec cette enquête, sans pouvoir viser un amendement précis. Ni les juges, ni les parties

[57] *Nasa v. Nelson*, Syllabus, 2
[58] "At this point the reader may be wondering: "What, after all, is the harm in being 'minimalist' and simply refusing to say that violation of a constitutional right of informational privacy can never exist?"
[59] "It harms our image, if not our self-respect, because it makes no sense. The Court decides that the Government did not violate the right to informational privacy without deciding whether there is a right to informational privacy"

ne sont capables d'identifier clairement l'existence de la vie privée informationnelle, c'est donc qu'elle n'a peut-être pas lieu d'être constitutionnellement et simplement dire ce droit possible n'y changera rien.

Même en dehors de ce problème de fondement, l'argumentation de la Cour rend l'exercice de ce droit encore plus compliqué à envisager. Elle déclare que les questions posées sont raisonnables et non-intrusives. Comme dans *Whalen*, les juges énoncent qu'il n'existe pas d'obligation constitutionnelle de prouver la nécessité de cette enquête, éludant donc l'incapacité à justifier la finalité de cette opération. Son deuxième argument est que le *Privacy Act* de 1974 protège les informations contre toute divulgation injustifiée.

Prenons l'exemple de la Cour, et étudions son raisonnement en faisant comme si la vie privée informationnelle existait vraiment dans l'ordre constitutionnel. Cela va permettre de relever les différences que ce droit aurait avec le droit de l'Union européenne. Les juges disent que la nécessité de la collecte n'est pas à prouver. Voilà une grande différence avec le RGPD, qui met la finalité au centre de tout. Le traitement n'est licite que s'il est effectué dans une certaine finalité pour laquelle la personne voyant ses données traitées a consenti[60]. La finalité ici n'est jamais exposée, il s'agit juste de se renseigner sur la personne recrutée. Dans l'Union européenne, « avant de mettre en œuvre un traitement mais également tout au long de sa durée de vie, il faut systématiquement se poser les questions relatives à la légalité, la finalité, la légitimité et la proportionnalité de tout acte lié au traitement en respectant un esprit de minimisation en termes de périmètre et de durée »[61]. Aux Etats-Unis, il suffit que les données soient sécurisées et soient protégées contre la divulgation injustifiée, mais le responsable du traitement n'a aucune responsabilité générale qui pèse sur sa tête.

La Cour Suprême avance aussi le critère de la nature des informations collectées, mais ce critère est difficilement sujet à commentaire car il s'agit de l'appréciation souveraine des juges de ce qui entre ou n'entre pas dans la vie privée. Notons tout de même que ce critère paraît d'appréciation très stricte. Par trois fois, les informations traitées sont considérées comme raisonnables, si bien que l'on se demande dans quels cas elles auraient été jugées irraisonnables étant donnée la nature des faits de l'espèce. Si le fait de subordonner le recrutement d'une personne à ses antécédents psychiatriques et sa prise de drogues illégales n'est pas considéré comme une intrusion dans la vie privée, qu'est-ce qu'il l'est vraiment ?

Dans ces conditions, l'émergence d'un droit à l'oubli est difficilement imaginable. L'objet du droit à l'oubli est de permettre à une personne de reprendre le contrôle de ses données, que ce soit en les effaçant ou en les décontextualisant. Dans ces trois arrêts, la justification principale de la légitimité de la collecte est la sécurité des données une fois qu'elles sont rassemblées par l'autorité publique. C'est seulement ce que les juges appellent *unwarranted disclosure*, c'est-à-dire la

[60] RGPD, article 5, alinéa 2

[61] BENSSOUSAN A., *Règlement européen, sur la protection des données, textes, commentaires et orientations pratiques*, 2e édition, Bruxelles, 2017, page 238

divulgation injustifiée, qui est un risque pour la vie privée. Or le droit à l'oubli va bien plus loin que ça : le seul retrait du consentement de la personne concernée peut permettre l'effacement des données. Le droit à l'oubli part de la personne, ce ne peut être la seule conséquence d'une faute du responsable du traitement. L'illicéité du traitement n'est qu'une des raisons que la personne concernée peut invoquer pour faire valoir son droit à l'oubli. Ici, par trois fois, il n'a pas été prouvé que les données pouvaient faire l'objet d'une fuite ou être utilisées illégalement. Le droit constitutionnel américain ne semble donc pas prêt à utiliser le droit à l'oubli car il cherche la faute du responsable du traitement alors que ce droit est une possibilité qui est accordée à la personne concernée.

La protection des données au niveau constitutionnel aux Etats-Unis a donc suivi le cheminement inverse du modèle français. Alors qu'en 1977, la Cour Suprême identifiait une possibilité de droit à la vie privée informationnelle qui laissait penser une consécration dans une décision prochaine, aujourd'hui ce droit semble plus loin que jamais de faire son entrée dans le spectre constitutionnel. Il peut être dommage de voir un manque de progression dans un intervalle de presque 40 ans. Alors que dans les années 70, l'informatique n'en était qu'à ses débuts, aujourd'hui elle est primordiale dans chaque aspect de notre vie. La logique voudrait que l'accroissement de la protection des données aille de pair avec le progrès technologique. Or il n'en est rien, puisqu'au mieux la position de la Cour Suprême a stagné, au pire elle a régressé.

Il ne faut cependant pas oublier que les Etats-Unis post-11 septembre n'ont rien à voir avec ce qu'était le pays 30 ans auparavant. Le traumatisme infligé a eu pour conséquence de voir la sécurité de la nation érigée au-dessus des droits de la population dans une majorité des cas de figure. Dans un tel contexte, la constitutionnalisation d'un droit à la protection des données semble improbable…

En France, depuis l'institution de l'article 9 du Code Civil, la protection de la vie privée n'a fait que prendre de l'importance. Depuis 1995, la vie privée est rattachée au bloc de constitutionalité et, dans les années 2000, le Conseil Constitutionnel n'a eu de cesse d'encadrer la protection des données.

B) Le cadre constitutionnel français

Rappelons que, tout comme aux Etats-Unis, la vie privée ne figure nulle part dans le bloc de constitutionalité. Absente de la Constitution de 1958 comme de celle de 1946, le Conseil constitutionnel va d'abord la fonder en 1995 sur la liberté individuelle de l'article 66 de la Constitution. Il jugera que « la méconnaissance du droit au respect de la vie privée peut être de nature à porter atteinte à la liberté individuelle »[62]. Probablement insatisfait de ce fondement, qui rattachait implicitement le respect de la vie privée au seul ordre judiciaire, le Conseil constitutionnel va rattacher la vie

[62] Conseil constitutionnel, 18 janvier 1995, n° 94-352 DC

privée en 1999 à l'article 2 de la Déclaration de la Déclaration des Droits de l'Homme et du Citoyen[63]. Il dispose que « la liberté » est « un droit imprescriptible de l'Homme ». On peut constater deux avantages à ce changement de fondement. Il constitue déjà un argument d'autorité, la déclaration des droits de l'homme ayant une signification morale plus importante que la Constitution de 1958. En outre, le fait de rattacher la vie privée à l'article 66 implique que c'est seulement la privation de liberté que l'ordre judiciaire protège qui est sauvegardée. Fonder la vie privée sur la liberté de la DDHC permet d'en intégrer tous les aspects dans le bloc de constitutionnalité, dont le volet concernant l'autonomie de l'individu à faire des choix.

Ce fondement rappelle beaucoup celui que les Etats-Unis ont utilisé pour constitutionaliser ce seul volet de la vie privée. Dans l'arrêt *Roe v/ Wade*, c'est la liberté du 14ème amendement qui est visée. Celui dispose que « aucun Etat […] ne privera une personne de sa vie, de sa liberté ». La Cour Suprême et le Conseil constitutionnel ont eu exactement le même raisonnement : fonder le concept moderne de vie privée sur un texte ancien qui promeut la liberté comme droit imprescriptible. Il est étonnant de voir certaines similitudes dans l'évolution constitutionnelle de systèmes complètement différents.

A partir de cette entrée de la vie privée dans le bloc constitutionnel, la protection des données va faire l'objet d'un encadrement de plus en plus poussé par le Conseil constitutionnel. En particulier, une décision de 2014 qu'il convient de comparer aux décisions de la Cour Suprême précédemment étudiées.

Des députés et des sénateurs ont saisi le Conseil constitutionnel pour contester une loi qui établissait un registre national recensant les personnes physiques auxquelles les établissements de crédits ont accordé des prêts à la consommation. Ce registre « a pour finalité de prévenir les situations de surendettement des personnes physiques n'agissant pas pour des besoins professionnels »[64]. Il conserve des informations sensibles telles que les incidents de paiement, la situation de surendettement ou les procédures de liquidation judiciaire prononcées. Tous les organismes financiers ont l'obligation de le consulter avant d'accorder un prêt à une personne.

Les requérants soutiennent donc « que la création d'un registre national des crédits aux particuliers porte, en raison de l'ampleur du registre, du caractère sensible des informations qu'il contient et de ses modalités de consultation, une atteinte disproportionnée au droit au respect de la vie privée »[65].

Le Conseil constitutionnel va d'abord statuer que « la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière

[63] Conseil constitutionnel, 23 juillet 1999, n° 99-416 DC
[64] Article L. 333-7 de la loi relative à la consommation
[65] Conseil Constitutionnel, 13 mars 2014, n°2014-690, considérant 41

adéquate et proportionnée à cet objectif »[66]. Il prend comme visa la vie privée protégée par l'article 2 de la Déclaration des Droits de l'Homme et du Citoyen.

Il va ensuite accueillir favorablement la demande des requérants, en décidant « qu'eu égard à la nature des données enregistrées, à l'ampleur du traitement, à la fréquence de son utilisation, au grand nombre de personnes susceptibles d'y avoir accès et à l'insuffisance des garanties relatives à l'accès au registre, les dispositions contestées portent au droit au respect de la vie privée une atteinte qui ne peut être regardée comme proportionnée au but poursuivi »[67].

Sans pour autant insérer le droit à la protection des données dans le bloc de constitutionalité, cet arrêt l'encadre et l'intègre dans la protection de la vie privée, ce qui est un pas que la Cour Suprême n'a pas encore franchi. Les faits sont assez similaires avec le dernier arrêt en date de la Cour Suprême : dans la décision Nelson, il s'agissait de collecter des données sensibles sur des usagers et de décider de leur recrutement en fonction de ces données.

La décision du Conseil constitutionnel est totalement inverse à la position de la Cour Suprême. Déjà, le Conseil Constitutionnel ne s'est pas posé la question de savoir si les données personnelles sont protégées par le droit au respect de la vie privée. Il a directement visé l'article 2 de la DDHC, ce qui rappelle que la protection de la vie privée en France est un concept élastique protégeant tout ce que les cours estiment légitime d'y appartenir. Alors que la Cour Suprême a considéré la loi comme constitutionnelle sur la base d'un droit qui pourrait exister, le Conseil Constitutionnel a décidé que la loi était contraire à la Constitution en visant un droit à la vie privée faisant explicitement parti du bloc de constitutionalité. Sur le terrain du fondement, le raisonnement français semble donc plus solide que l'étatsunien.

Dans la justification de l'inconstitutionnalité, il existe de nombreuses différences entre les deux arrêts. Nous l'avons dit que les critères utilisés par la Cour Suprême sont la raisonnabilité des informations collectées au regard du motif et leur sécurité lorsqu'elles sont traitées. Sur ce premier critère de proportionnalité, le Conseil Constitutionnel semble plus strict sur son appréciation. Dans les deux espèces, il est question de la situation financière de l'individu, et dans la décision étatsunienne on y ajoute d'autres informations telles que son intégrité psychologique. Les faits sont donc de la même teneur, pourtant la solution est différente. La Conseil constitutionnel considère que la nature des informations traitées est une intrusion à la vie privée, il est donc probable qu'avec les faits de la décision *Nelson,* la solution du Conseil Constitutionnel aurait été la même, puisque ces faits étaient objectivement encore plus intrusifs.

Les deux cours procèdent à un contrôle de proportionnalité, seulement la Cour Suprême va faire primer l'intérêt de l'Etat sur la nature des informations collectées. Là où le Conseil parle d'intérêt général, la Cour Suprême parle de « the Government

[66] Conseil Constitutionnel, 13 mars 2014, n°2014-690, considérant 51
[67] Conseil Constitutionnel, 13 mars 2014, n°2014-690, considérant 57

interests »[68]. Les intérêts en balance ne sont donc pas les mêmes : l'intérêt général est l'intérêt de tous et est censé bénéficier à tous, l'intérêt d'Etat est seulement celui de l'Etat.

Sur le critère de la sécurité, il suffit qu'aux Etats-Unis que les données soient protégées contre la divulgation injustifiée. Le Conseil constitutionnel est bien plus strict. Il énonce « que l'article L. 333-20 subordonne à une autorisation individuelle et une habilitation, selon des procédures spécifiques internes aux établissements et organismes financiers, la consultation du registre par les personnels des établissements et organismes financiers ; qu'en renvoyant à un décret en Conseil d'État les modalités d'application de cette autorisation, le législateur n'a pas limité le nombre de personnes employées par ces établissements et organismes susceptibles d'être autorisées à consulter le registre »[69]. Cela a pour conséquence qu'il y a « une insuffisance des garanties relatives à l'accès au registre ». La simple délégation de la modalité de l'accès au registre a suffi à rendre le traitement sécurisé, là ou aux Etats-Unis la seule mention du Privacy Act de 1974 a suffi à justifier la sécurité du traitement. La sécurité du traitement est donc évaluée bien plus strictement, il ne suffit pas qu'une loi la protège.

Sur les deux critères évalués par la Cour Suprême, le conseil constitutionnel est donc bien plus vigilant dans son contrôle de proportionnalité. Les différences ne s'arrêtent cependant pas là : les conditions de forme du traitement sont également une raison pour le rendre inconstitutionnel dans la décision française. Est évoqué son ampleur, sa fréquence ou encore le nombre de personnes y ayant accès. Ce sont des critères qui ne sont pas du tout pris en compte par la Cour Suprême. Ces critères rappellent le RGPD, qui attache une certaine importance à la durée du traitement par exemple, qui ne doit pas excéder la finalité pour laquelle l'information a été collectée. Ce n'est pas parce qu'un traitement à un instant T est licite qu'il le sera plusieurs années plus tard. Cette inspiration n'est probablement pas un hasard, le projet de RGPD étant paru en 2012, soit deux ans avant la décision.

Le conseil constitutionnel a donc bien plus encadré la protection des données que ne l'a fait la Cour Suprême. Ses critères sont plus exigeants et plus nombreux. Le droit à l'oubli a donc plus sa place dans le système juridique français. Une importance bien plus grande est accordée à la personne : l'appréciation stricte de la nature de l'information traitée et la mention de l'intérêt général en sont la preuve. Aux Etats-Unis, il semble que l'intérêt de l'Etat pèse plus lourd que celui du citoyen en matière de données personnelles.

Il faut cependant garder en tête une distinction primordiale : tandis que la Constitution française survole l'intégralité de la pyramide des normes et s'applique aussi bien horizontalement que verticalement, la Constitution américaine est d'application seulement verticale, elle ne s'applique donc qu'entre l'Etat et le

[68] *Nasa v. Nelson*, Syllabus, 2, a)
[69] Conseil Constitutionnel, 13 mars 2014, n°2014-690, considérant 56

particulier. Il est donc des domaines qui ne sont pas ceux de la Constitution. Pour avoir un véritable aperçu de la protection des données étatsunienne et de la possibilité d'un droit à l'oubli, il faut donc examiner la législation fédérale. Après tout, comme le dit le juge Scalia, il appartient peut-être aux citoyens et non à la Constitution de forger ce droit…[70]

Section 2 / La protection des données au niveau fédéral et étatique comparée à la législation européenne

La législation étatsunienne sur la protection des données n'a rien à voir avec celle de l'Europe. Selon P.M Schwartz et K-N Peifer, dans l'Union européenne la vie privée est un droit essentiel à l'existence même du citoyen, en dehors de tout contexte. C'est un droit que chaque résident détient dans chaque aspect de sa vie. Aux Etats-Unis, la vie privée suit la logique du marché. La vie privée du consommateur est protégée plus que la vie privée en général. La logique de la protection des données est donc très mercantile[71]. Les textes les plus importants sur la protection des données que sont le *Privacy Act* de 1974 et *l'Electric Communications Act* de 1986 se révèlent aujourd'hui inadaptés à l'ère d'internet en étant incapables de protéger les individus dans chaque aspect de leur vie numérique. L'arrêt *Nasa v. Nelson* analysé ci-dessus avait d'ailleurs pour enjeu la constitutionnalité du *Privacy Act*, qui a été validée par la Cour Suprême. Actuellement, c'est la *Federal Trade Comisson*, instance protectrice des droits des consommateurs, qui est la cour garante de la protection des données aux Etats-Unis. Elle surveille les pratiques de confidentialité des entreprises et sanctionne quand elle constate une tromperie dans la politique de confidentialité de l'entreprise. Là encore, la protection des données concerne seulement le volet commercial.

Comme la vie privée n'est pas un droit subjectif comme elle peut l'être en France, l'individu ne peut s'en prévaloir dans chaque aspect de sa vie. Dans un tel contexte, un droit à l'oubli est difficilement envisageable. La FTC connait certes d'un certain nombre d'affaires où elle constate des traitements illicites de la part d'entreprises, mais elle est étrangère au concept de retrait de consentement ou de changement de finalité. Quel est le préjudice que subit l'individu en tant que

[70] "Like many other desirable things not included in the Constitution, "informational privacy" seems like a good idea—wherefore the People have enacted laws at the federal level and in the states restricting the government's collection and use of information. But it is up to the People to enact those laws, to shape them, and, when they think it appropriate, to repeal them. A federal constitutional right to "informational privacy" does not exist » Nasa v. Nelson, 562 U.S.134, opinion du juge Scalia, p. 1

[71] « In the EU, rights talk forms a critical part of the postwar European project of creating the identity of a European citizen. As Jiirgen Habermas argues, this task is a constitutional one that is central to the EU's survival. In the United States, by contrast, data privacy law is based on the idea of consumers whose interests merit governmental protection in a marketplace marked by deception and unfairness. In the United States, the focus is on "marketplace discourse" about personal information and the safeguarding of "privacy consumers » P. M. Schwartz et K.-N. Peifer, *Transatlantic Data Privacy*, Georgetown Law Journal, 2017, n° 106, p. 115

consommateur quand il veut retirer son consentement ? Ce n'est pas évident à discerner.

Influencés par le RGPD, certains Etats commencent à adapter leur droit pour améliorer la protection des données des individus. Nous étudierons le texte adopté par la Californie en janvier 2020 sur la protection des données : le *California Consumer Privacy Act* (CCPA). Cet acte va donner toute une série de nouveaux droits aux individus qu'ils pourront opposer aux entreprises. Comme le RGPD, ce texte a moins pour but la sécurisation des données que de conférer aux individus un contrôle plus important sur celles-ci.

Malheureusement, le domaine de cette loi est encore trop réduit. Créée spécialement pour contrer les géants d'Internet que sont Facebook ou Google, ce texte concerne seulement les entreprises ayant plus de 25 millions de dollars de chiffre d'affaire seulement si elles collectent les données de 50 000 consommateurs[72]. Cela réduit drastiquement le nombre d'entreprises contraintes par le texte, surtout par rapport au RGPD qui s'applique à tout organisme qui traite des données. La prise de conscience liée au RGPD est cependant toute récente, et il est normal que l'Etat commence par s'atteler aux organismes les plus dangereux en termes de protection des données avant de s'occuper des plus petits.

Un point qui mérite une critique plus sévère à la légèreté des sanctions. Une violation est passible d'une amende de 2500$ qui peut être majorée jusqu'à 7500$ en cas de violation intentionnelle[73]. Pour un texte qui est censé viser les plus grosses compagnies de l'Etat, la sanction n'est pas du tout rédhibitoire. Il s'agit d'une bouchée de pain pour toutes ces compagnies de la Silicon Valley engrangeant des milliards de dollars de chiffre d'affaire par an. Si ce texte constitue un premier pas certain dans la direction d'une plus grande protection des données, il est probable que son effectivité ne sera pas très grande si les sanctions restent en l'état. Pour rappel, l'article 83 du RGPD dispose que le non-respect d'une injonction de l'autorité publique peut aller jusqu'à 20 millions d'amende ou 4% du chiffre d'affaire annuel, selon le montant le plus élevé. Il y a donc un écart gigantesque entre les deux législations, qui n'ont pas du tout le même pouvoir de dissuasion.

L'objet du CCPA est de conférer toute une série de droits aux individus tel le droit d'opposition, le droit d'accès ou encore le droit à l'information, qui oblige le responsable du traitement à transmettre à l'individu la finalité du traitement. Toutes

[72] "has annual gross revenues in excess of twenty-five million dollars" et "Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices" CCPA, Section 1798.140 c)

[73] "Any business, service provider, or other person that violates this title shall be subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars ($2,500) for each violation or seven thousand five hundred dollars ($7,500) for each intentional violation" CCPA, Section 1798.155

ces dispositions sont fortement inspirées du RGPD. Nous ne les étudierons pas en détail pour se concentrer sur le droit à l'effacement.

Ce droit est une avancée remarquable. C'est la première fois qu'une forme de droit à l'oubli pour les adultes est mise en avant dans un texte normatif aux Etats-Unis. Il a pour différence avec le RGPD qu'il n'expose pas les motifs pour les lesquels le droit à l'oubli peut être demandé. Il est disposé que le consommateur a un droit à l'effacement de toutes les données traitées par la compagnie[74]. On retrouve cette idée que c'est le consommateur qui est avant tout protégé et non l'individu. Ce texte, même s'il constitue un progrès remarquable, reste donc ancré dans une conception très étatsunienne de la vie privée. L'absence de motifs n'est pas très réjouissante. Simplement dire que tout consommateur a le droit à voir ses données effacées ne suffit pas. Mettre les raisons justifiant une requête d'effacement de données aurait facilité les futures demandes, car tout consommateur ne peut pas exiger l'effacement de ses données à tout moment sans se justifier. On peut donc se poser des questions sur l'efficacité pratique de cette disposition.

Cette interrogation est encore plus légitime quand on voit la série d'exception qui est posée au principe. La première semble être la plus limitative. Elle dispose que la compagnie ne sera pas obligée de recourir à l'effacement si les données litigieuses sont nécessaires pour procurer un bien ou un service demandé par le consommateur, ou que la compagnie pouvait raisonnablement anticiper au vu des relations commerciales entre les deux parties. Dans le même paragraphe, il y aussi une exception pour l'accomplissement du contrat signé entre le consommateur et la compagnie[75].

Il existe neuf séries d'exceptions pouvant empêcher l'effacement des données, mais il semble que celle-ci suffise à débouter la plupart des demandes. Il est difficile de discerner quel cas n'entre pas dans cette catégorie. Il suffit que la compagnie puisse invoquer un futur service ou produit que le consommateur aurait pu demander pour refuser l'effacement. Cette exception va donc contre la volonté du consommateur, puisqu'il est possible de refuser l'effacement sur la base d'un besoin qu'il n'a pas encore exprimé. Il semble qu'il soit très facile d'inventer un besoin sur la base de la relation actuelle entre le consommateur et la compagnie. Evidemment, il faudra voir la sévérité dont feront preuve les tribunaux à propos de cette exception, mais elle n'est certainement pas une bonne nouvelle pour l'effectivité du droit à l'effacement.

Le problème est que cette exception élude le motif primaire du droit à l'oubli : le retrait du consentement. Si toute relation contractuelle actuelle ou future entre les

[74] "A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer." CCPA, 1798.105 a)

[75] " A business or a service provider shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or service provider to maintain the consumer's personal information in order to […] provide a good or service requested by the consumer, or reasonably anticipated within the context of a business' ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer" CCPA, 1798.105 d) 1)

parties est susceptible de rejeter une demande de déréférencement, alors cela veut dire que le consentement du consommateur au début du contrat sonne la fin de cette potentielle demande avant même qu'elle puisse exister. Or c'est précisément l'inverse de ce que le droit à l'oubli est censé proposer : un droit au pardon, la possibilité de racheter une erreur que l'on a commise. En l'état actuel du texte, cette exception cantonne la possibilité de déréférencement à une situation de traitement illicite, quand le traitement est proprement injustifiable.

Les limitations suivantes sont semblables à celle du RGPD, avec l'exception d'obligation légale, celle de la transparence ou celle de la liberté d'expression. Nous touchons là aux motifs et aux limitations du droit à l'oubli, qu'il faudra expliciter dans un second titre.

TITRE II / L'exercice du droit à l'oubli

Après avoir exploré les fondements du droit à l'oubli, il est nécessaire d'en étudier l'exercice. L'étude de la portée géographique du droit à l'oubli ne sera pas faite. Cette question est fondamentale et a connu des développements récents[76], toutefois il s'agit d'une problématique purement européenne, dans le sens où un tel débat n'existe pas aux Etats-Unis. L'étude comparative est donc impossible.

Le droit à l'oubli s'appuie en partie sur la notion de consentement. C'est un des fondements sur lequel un responsable de traitement peut s'appuyer pour collecter les données d'un individu. Nous verrons que la portée du consentement n'est pas du tout la même en France et aux Etats-Unis, ce qui rend inégale l'exercice du droit à l'oubli (1). Il faudra ensuite s'intéresser à la liberté d'expression, première limite au droit à l'oubli posée par le RGPD. Nous l'étudierons sous l'angle de l'intérêt légitime du public à s'informer (2). Nous ferons enfin un point sur le droit à l'oubli pour les mineurs, car c'est la seule catégorie de personnes ayant une possibilité de droit à l'oubli aux Etats-Unis, et qu'elle bénéficie d'une protection particulière en Europe (3).

Chapitre 1 : La portée du consentement

Il est aujourd'hui possible de poster en quelques clics une énorme quantité de médias sur les réseaux sociaux, où ils pourront être vus par une infinité de personnes. Dans un tel contexte, il est nécessaire d'avoir un droit au repentir. La possibilité de retirer le consentement sur une donnée permet de corriger une erreur que l'on a faite sur un coup de tête, sans y avoir sérieusement songé. Même si ce retrait est une possibilité légale en Europe, sa mise en effet reste complexe : on sait maintenant qu'une information effacée sur Facebook ne l'est pas réellement et est conservée dans la base de données même si elle n'est plus visible. Il est par ailleurs impossible de supprimer son compte Facebook, on ne peut que le désactiver. A ce problème-là s'ajoute une limitation de la portée du consentement aux Etats-Unis, où il est difficile de récupérer une information qui s'est échappée dans la vie publique (1). En Europe, le retrait du consentement est une possibilité accordée par le RGPD (2).

Section 1 / Aux Etats-Unis, des données cédées et difficilement récupérables

L'outil principal utilisé aux Etats-Unis pour faire respecter le droit à la vie privée trouve son origine dans le droit des *torts*. Pour rappel, le §652 du *Restatement of torts* dispose que la responsabilité est encourue pour « la révélation au public de faits qui relèvent manifestement de la vie privée d'autrui, à condition que ces faits soient de

[76] Voir Conseil d'Etat, 10e et 9e chambres réunies, N° 399922, 27 mars 2020

nature à choquer toute personne raisonnable et qu'ils ne présentent pas d'éléments de nature à éveiller un intérêt légitime dans le public ». Ce texte n'est pas fédéral, mais la plupart des Etats l'ont adopté et il constitue aujourd'hui le standard en matière de protection de la vie privée. Analyser ce texte sous le regard du droit à l'oubli fait apparaître deux difficultés. La seconde est le problème de l'intérêt légitime du public, qui est lié à la liberté d'information et donc à la liberté d'expression, que nous étudierons plus tard. Celle qui nous intéresse à présent est la nécessité que les faits ressortent manifestement de la sphère privée.

Aux Etats-Unis, dès lors qu'une donnée ou un fait sort de la vie privée, la personne n'a plus de moyens de faire jouer la responsabilité du diffuseur sur la base du droit des torts. Au regard du droit à l'oubli, cela pose un problème. Pour récupérer une information, encore faut-il l'avoir laissée filtrée à l'origine. Le principe même du droit à l'oubli est que toute personne a un droit persistant sur ses données, même lorsqu'elle les a cédées à autrui. La vision de la vie privée proposée par les Etats-Unis constitue donc forcément une barrière à sa mise en place.

La jurisprudence étatsunienne a une vision de la vie privée très restrictive. Les tribunaux considèrent que, selon le lieu où le fait litigieux est survenu, la personne consent d'office à ne pas faire jouer son droit à la vie privée. Dans un arrêt *Gill v/ Heart Publishing Co*[77], la Cour Suprême californienne a jugé une affaire où un jeune couple a été pris en photo dans une posture romantique sans leur consentement. Ils étaient à leur lieu de travail, qui était un commerce de confection de glace dans un marché ouvert. La Cour considère que ces faits ne relèvent pas de la vie privée, car les demandeurs ont volontairement assumé cette pose romantique dans un lieu public[78]. Citant Warren et Brandeis, elle dit qu'il faut protéger la *privacy of private* life (malheureusement intraduisible), et que si par un fait quelconque les faits cessent d'être privés, il faut retirer la protection[79]. Cela veut bien dire que si les faits sortent de la vie privée, la personne consent d'office à ce qu'ils ne soient plus protégés.

La qualification du lieu comme appartenant à la sphère publique paraît de plus assez sévère. Le lieu est un marché public, mais ils sont sur leur lieu de travail, sur lequel ils ne sont que deux. Ils n'étaient pas là en tant que promeneurs ou touristes, ils travaillaient. La décision revient à dire que toute action effectuée sur leur lieu de travail ne relève pas de leur vie privée. En France, la protection de la vie privée s'étend au lieu de travail, parfois de manière très extensive. Par ailleurs le droit à l'image protège même ceux qui sont dans un lieu public, à partir du moment où le cliché est diffusé, que les personnes sont reconnaissables et qu'elles n'ont pas consenti à la diffusion. Le problème dans cet arrêt est que le consentement est accordé implicitement. La seule chose qui aurait pu permettre la mise en jeu de la

[77] *Gill v/ Heart Publishing Co*, 40 Cal.2d 224, 1953

[78] "In considering the nature of the picture in question, it is significant that it was not surreptitiously snapped on private grounds, but rather was taken of plaintiffs in a pose voluntarily assumed in a public market place."

[79] "and to whatever degree and in whatever connection a man's life has ceased to be private, […] to that extent the protection is to be withdrawn"

responsabilité des diffuseurs dans cette affaire est le fait que le cliché soit embarrassant pour les demandeurs. Le couple étant simplement l'un dans les bras de l'autre, la Cour n'a considéré le cliché comme étant un préjudice.

Dans une affaire autrement plus grave[80], le champ de la vie privée a été encore plus réduit. En l'espèce, une magistrate colombienne a reçu des menaces de mort car elle avait poursuivi un baron de la drogue en justice pour meurtre. Elle a été dans l'obligation de changer de pays et de s'installer aux Etats-Unis. Elle a été nommée en tant que consul, et seuls les autres consuls ainsi que quelques voisins étaient au courant de son passé. Un journal local a révélé dans un article la véritable identité de l'ancienne magistrate, tout en précisant son adresse exacte. Elle agit donc en responsabilité, notamment pour non-respect de la vie privée. Les juges vont considérer que l'identité de la personne était accessible au public, elle ne pouvait donc plus être protégée par le *Restatement of torts*.

Les juges vont ici bien plus loin que dans l'arrêt précédent. Si l'on peut comprendre qu'une photo non-embarrassante prise dans un lieu public (fut-il aussi un lieu de travail) ne soit pas protégée, quoi de plus privé qu'un fait passé pouvant mettre la vie d'une personne en danger ? La Cour fait preuve ici d'un raisonnement très froid, elle constate seulement que l'information est passée dans la sphère publique, pas sa nature. Sa justification est que la demandeuse révélait couramment son identité, notamment en donnant sa carte professionnelle ou en signant le bail de sa maison sous son nom.

Plusieurs objections peuvent être soulevées quant à cette décision. Les risques encourus par la révélation des faits auraient pu être plus pris en considération par les juges, qui n'en ont pas fait grand cas. Ces faits relevaient de la sphère privée de façon tout à fait incontestable. Sur la simple base de l'usage de son ancien nom, les juges semblent considérer que la demandeuse a abandonné toute volonté de protéger son passé, qui est forcément à la portée de tous. Or ce n'est pas parce qu'elle utilise son nom qu'elle accepte que son passé ne soit révélé. Le raccourci semble un peu rapide. Son nom est certes corrélé à ce qui lui est arrivé mais pas plus qu'il n'est lié à sa vie privée en général. En suivant ce raisonnement, on peut considérer que l'utilisation d'un nom a pour conséquence l'abandon total de vie privée. La Cour basait son raisonnement sur un article paru en Colombie qui révélait la situation de l'ancienne magistrate en mentionnant son nom. Toutefois l'article ne dévoilait pas son nouveau lieu d'habitation ni son adresse. Or ici elle a été révélée par la presse étatsunienne, ce qui constitue la plus grande intrusion dans la vie privée étant donné les conséquences qu'aurait pu avoir cette information sur la vie de la demandeuse.

Cette affaire montre à quel point il est facile pour une information de sortir du domaine privé et de ne plus être protégée. Pourtant, pour que la protection soit efficace, il faut nécessairement un juste milieu. Le *tort* de *disclosure of private facts* cité plus haut a pour objet d'engager la responsabilité d'une personne qui a révélé une

[80] *Duran v/ Detroit News*, 504 N.W.2d 715, Mich. Ct. App, 1993

information qui appartient à la vie privée. La protection permise par cette disposition nécessite que l'information soit révélée, sinon la protection n'a pas lieu d'être. Les deux dernières jurisprudences donnent l'impression que dès diffusion de l'information, la protection disparaît, ce qui rend le *tort* inefficace.

Il existe des affaires où les juges ont accueilli favorablement l'action en responsabilité sur la base de ce *tort*. On peut citer la décision *Multimédia WMAZ, Inc v/ Kubach*[81], où une émission sur le SIDA censée flouter le visage des personnes interviewées a malencontreusement révélé le visage d'un des intervenants pendant quelques secondes. Celui-ci a donc agit en responsabilité pour *disclosure of private facts.* Son état de santé était connu de plusieurs dizaines de personnes, dont ses collègues, ses amis, sa famille et son groupe de soutien lié à sa maladie. La Cour a jugé que ces circonstances ne suffisaient pas à effacer le caractère privé de l'information.

Le tort trouve donc bien une utilité. La jurisprudence est cependant très versatile. Quelle est la différence entre, dans cette dernière affaire, la révélation de l'état de santé à un certain nombre de personnes et, dans la seconde, l'utilisation courante d'un nom ? Les critères ne sont pas évidents à dégager, et la jurisprudence manque d'une ligne directrice. L'appréciation semble très casuistique. Il ne faut toutefois pas oublier que, même si ce tort est appliqué dans presque tous les Etats, il n'en est pas pour autant un texte fédéral. Chaque Etat en fait donc sa propre interprétation, ce qui n'aide certainement pas à donner à dresser une idée générale de son efficacité.

Il n'en reste pas moins que, au regard du droit à l'oubli, le tort de *disclosure of private facts* ne parait pas aller dans la bonne direction. Aussitôt divulguée, l'information semble échapper à son détenteur, qui accepte par défaut qu'elle ne soit plus protégée. L'information peut être de nature privée, sa nature ne change pas, mais elle ne peut plus être protégée. C'est toute la différence avec l'article 17 du RGPD, qui permet qu'une personne puisse retirer le consentement sur une donnée qu'elle a consenti à transmettre.

Section 2 / En Europe, la possibilité de retirer son consentement

L'arrêt *Google Spain* est connu comme l'arrêt fondateur en matière de droit à l'oubli en Europe. Il interprète la directive 95/46/CE pour en dégager un droit au déréférencement. Si les prémices de ce droit existaient dans la loi informatique et libertés de 1978 ou la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel de 1981, c'est véritablement dans cet arrêt que ce droit est devenu effectif.

[81] *Multimédia WMAZ, Inc v/ Kubach* 443 S.E.2d 491, Georgia Ct. App, 1994

Pour rappel, les faits concernaient un ressortissant espagnol, qui a découvert qu'en tapant son nom sur Google, le moteur de recherche le renvoyait vers un article de presse sur une vente aux enchères relatives à une saisie pratiquée en recouvrement de dettes. Il a donc demandé à Google que ces liens soient effacés. Devant l'absence de réponses, il va s'adresser à l'agence de protection de données espagnoles, qui va à son tour poser une série de questions préjudicielles à la CJUE.

Les juges ont décidé que la détention de données licites peut devenir « avec le temps incompatible avec la directive lorsque ces données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées. Tel est notamment le cas lorsqu'elles apparaissent inadéquates, qu'elles ne sont pas ou plus pertinentes ou sont excessives au regard de ces finalités et du temps qui s'est écoulé. »[82] Trois conditions non-cumulables sont donc nécessaires pour mettre en jeu le droit à l'oubli : l'inadéquation, donc l'illicéité de l'information. Cela est plein de bon sens, une fausse information de continuer à être traitée. Ensuite vient la question de la finalité. Une information a été collectée dans un certain but, quand ce but a été atteint ou qu'il n'a plus lieu d'être, l'information peut être déréférencée. Une troisième condition qui est liée à celle de la finalité est celle du passage du temps, qui rend l'information obsolète et inutile.

Le RGPD va reprendre l'apport de l'arrêt en y ajoutant des précisions. La personne concernée va pouvoir retirer son consentement. Cette question est très liée à celle de la finalité, l'article 6 et l'article 9 du RGPD y font référence. Il n'existe pas de consentement général à voir ses données traitées, le traitement ne peut être fait que si la personne concernée a spécifiquement consenti à une ou plusieurs finalités. On peut d'ailleurs imaginer que si une personne veut retirer son consentement, ce sera parce que la finalité du traitement s'est éteinte. Le législateur européen a voulu cependant laisser une liberté supplémentaire à l'individu, en lui permettant simplement de retirer son consentement, en dehors de tout problème de finalité. Va être ajouté également un droit d'opposition général dans l'article 21 du RGPD, qui permet à une personne d'effacer ses données pour des raisons tenant à sa situation particulière.

Il existe donc un considérable écart entre la législation européenne et celle des Etats-Unis. Dans l'Union européenne, les individus gardent un droit d'effacement de leurs données même lorsque le traitement a été explicitement consenti. L'information accessible publiquement peut toujours être protégée. Même sans la législation sur le droit à l'oubli, les dispositions du droit français sur le droit à l'image ou sur la vie privée auraient sans doute suffi à rendre les arrêts précités plus favorables au demandeur.

Si la lettre du RGPD permet donc le retrait du consentement qui entrainerait l'effacement de données, encore faut-il qu'en pratique une telle action soit réalisable en pratique. En décembre dernier, le Conseil d'Etat a connu d'une dizaine d'affaires traitant du droit à l'oubli qu'il convient d'étudier en partie.

[82] CJUE, *Costeja c/ Google Spain*, C-131/12, 13 mai 2014

Dans ces arrêts, le Conseil d'Etat statue sur des décisions de la CNIL concernant le droit au déréférencement. Rappelons que l'article 17 du RGPD permet d'effacer une donnée, déréférencer n'est qu'une manière d'exercer ce droit. Il s'agit à chaque fois d'un recours pour excès de pouvoir contre la décision initiale. Dans tous ces arrêts, la CNIL a donc débouté (au moins en partie) la demande de déréférencement. Nous en étudierons un seul sous l'angle du retrait du consentement. Notons que dans ces arrêts, le motif du déréférencement est soit la fin de la finalité pour laquelle les données sont collectées, soit le retrait pour raisons particulières de l'article 21. Le retrait du consentement à une information est rarement utilisé, même si on peut l'apparenter à celui de la finalité. Il est tout de même pertinent de l'analyser car il est la forme la plus poussée de droit à l'oubli. Autoriser le déréférencement quand un traitement est illicite ou quand la finalité a disparu parait évident lorsque l'on veut mettre en place un droit à l'oubli. Permettre de retirer une information que l'on a nous-même donnée est moins évident, et cette possibilité revient à pousser le droit à l'oubli à sa limite. Il convient donc de voir comment, en pratique, ce motif de déréférencement est jugé par les cours.

En l'espèce[83], une requérante demande le déréférencement de liens faisant état de sa condamnation en 2018 pour violences conjugales. Ces liens mènent vers une interview qu'elle avait faite de son plein gré pour un magazine. Google ayant refusé le déréférencement, la requérante a fait appel à la CNIL pour mettre en demeure le moteur de recherche. Se voyant opposée un refus, elle fait un recours pour excès de pouvoir auprès du Conseil d'Etat pour annuler la décision. Le Conseil d'Etat a débouté la demande.

Il faut d'abord rappeler le cadre juridique du litige. Il s'agit de l'article 17 du RGPD portant sur le droit à l'oubli, mais également sur l'article 10, qui porte spécifiquement sur le traitement des données faisant état de procédure pénales. Pour le traitement de ce type de donnée, la CJUE a rendu un arrêt le 24 septembre 2019[84] pour aiguiller les juridictions. Elle explique que les juridictions sont tenues d'ordonner le déréférencement seulement si les données se rapportent à une étape antérieure de la procédure en cause, et que les motifs d'intérêt public pouvant potentiellement maintenir les liens litigieux ne sont pas supérieurs à l'atteinte aux droits fondamentaux de la personne concernée. A noter qu'elle fonde sa décision sur la directive 95/46/CE et pas sur le RGPD, qui remplace pourtant celle-ci.

Le Conseil d'Etat dit par ailleurs qu'il incombe à la CNIL de scruter un faisceau d'indices composé de « la nature des données en cause, de leur contenu, de leur caractère plus ou moins objectif, de leur exactitude, de leur source, des conditions et de la date de leur mise en ligne et des répercussions que leur référencement est susceptible d'avoir pour la personne concernée et, d'autre part, de la notoriété de cette personne, de son rôle dans la vie publique et de sa fonction dans la société. »

[83] Conseil d'Etat, 10e et 9e chambre réunies, n° 429154, 6 décembre 2019
[84] CJUE, C-136/17, 24 septembre 2019

On peut dès lors constater qu'obtenir un déréférencement n'est pas une mince affaire. Retirer son consentement ne suffit pas, les juridictions vont examiner si le déréférencement est pertinent. L'article 10 du RGPD alourdit encore plus les conditions en disposant que « le traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes fondé sur l'article 6, paragraphe 1, ne peut être effectué que sous le contrôle de l'autorité publique ». Ce type de données étant sensibles, le RGPD rappelle que l'administration aura le dernier mot quant à toute forme de traitement, dont la suppression ou le déréférencement fait partie. Cela semble constituer une barrière supplémentaire pour le droit à l'oubli, d'autant plus que la demande de déréférencement de données liées aux condamnations pénales devrait être conséquente.

Le Conseil d'Etat dit que la CNIL « a pu légalement estimer » que le référencement était nécessaire à l'information du public. Cette formulation valide la décision de première instance sans y ajouter, même si le Conseil d'Etat souligne que la décision se fait « en dépit des répercussions qu'est susceptible d'avoir pour l'intéressée le maintien des liens ». La CNIL a donc considéré que l'atteinte au droit au respect de la vie privée n'était pas suffisamment importante pour déréférencer le lien. Son premier argument est que les données avaient été données par la personne elle-même en interview. Elle dit que les liens « se bornent, pour l'essentiel, à reprendre les propos que la requérante a elle-même choisi de tenir au sujet de sa condamnation dans une interview accordée à un magazine à grand tirage ».

L'intérêt de retirer son consentement est d'avoir le droit de se repentir pour des actions passées. L'argument selon lequel c'est la requérante qui est l'origine de ces liens peut, à première vue, paraître absurde, puisqu'il est la source de la possibilité de retirer son consentement. Elle a librement communiqué des données et souhaite à présent les retirer. Cette situation est prévue par le RGPD et ne peut être utilisé comme argument montrant l'inconséquence de la demandeuse qui aurait elle-même fourni les renseignements qu'elle souhaite effacer.

Cette critique doit être cependant tempérée. Il y a en effet une différence entre consentir à un traitement et donner une interview pour un grand magazine dont on sait pertinemment qu'il sera accessible à des milliers d'individus. Se plaindre de l'atteinte à la vie privée dans ce cas peut, à juste titre, être considéré comme de la mauvaise foi. Les listes de critères établis par le Conseil d'Etat et la CJUE et compilées par la CNIL disposent en effet que « le fait que la diffusion d'une information s'effectue par un organe de presse est à prendre en considération et peut peser dans l'appréciation qui sera faite d'une demande de déréférencement »[85]. Ce critère est compréhensible, la grande portée offerte au consentement par l'article 17 du RGPD ne peut être absolue, il faut savoir la limiter. Sur cet arrêt, on peut toutefois reprocher à la CNIL de ne pas avoir suffisamment approfondi son argumentaire. Elle semble en effet se

[85] « DROIT AU DEREFERENCEMENT : Les critères communs utilisés pour l'examen des plaintes », https://www.cnil.fr/sites/default/files/typo/document/Droit_au_dereferencement-criteres.pdf

cantonner à reprocher à la requérante d'avoir donné une interview, sans expliciter en quoi c'est un problème.

L'arrêt ne se prononce pas sur l'état de la procédure, cette condition ne peut donc pas être commentée, on supposera simplement que la procédure n'en est pas au même point que lors de l'interview puisque cela est passé sous silence. Le second argument est le caractère récent de l'interview et le dernier est que la requérante a une certaine notoriété liée à sa participation dans une série, ce qui serait un argument pour l'intérêt légitime du public à voir ces liens maintenus.

L'argument du temps écoulé est tout à fait pertinent, elle a consenti à donner ses informations il n'y a pas si longtemps, cela permet d'éviter l'abus de demande de droits à l'oubli dès qu'une bévue a été faite. Cela veut également peut-être dire que les faits litigieux sont peut-être encore d'actualité. L'argument de la personnalité publique est difficile à commenter, il s'agit de l'appréciation des faits d'espèces. On voit tout de même mal qu'il en aille de l'intérêt public que la population sache qu'une actrice de série a été condamnée pour violences conjugales.

Le retrait du consentement se heurte donc à un certain nombre d'obstacles en pratique. En plus de l'examen de l'opportunité du déréférencement par l'intermédiaire d'un faisceau d'indices, il est nécessaire de respecter les conditions limitatives posées par l'article 17§3 du RGPD.

Chapitre 2 / Le droit à l'oubli face à la liberté d'information

La première limitation posée par le RGPD dans l'article 17§3 est celle de la liberté d'expression et de la liberté d'information. Nous comparerons les législations des deux systèmes sous l'angle de l'intérêt légitime du public à s'informer, qui est souvent soulevé lors des débats sur le droit à l'oubli. La France et les Etats-Unis ont une conception de la liberté d'expression complètement différente. Les Pères fondateurs ont choisi de la placer au premier rang des amendements à la Constitution, et ses limites vont bien plus loin que celle de l'Hexagone. Cet éloge du libre discours va souvent mettre à l'écart la vie privée, ce qui ne facilite pas la mise en place d'un droit à l'oubli (1). En France, nous verrons que la liberté d'information constitue également une forte limite au droit à l'oubli (2).

Section 1 / Aux Etats-Unis, l'intérêt légitime contre le droit au respect de la vie privée

L'intérêt du public est ce qui est pour le mieux pour le bien de tous. Dans le cadre du droit à l'oubli, l'apport de la donnée litigieuse au public doit être supérieure à

l'intrusion dans la vie privée effectuée. Aux Etats-Unis, il va s'opposer au droit au respect de la vie privée, le droit à l'effacement n'existant pas vraiment.

La liberté d'expression est un droit d'une importance fondamentale aux Etats-Unis. Dans l'opinion dissidente de l'affaire *Abrams v. United States*[86], où il était question de la liberté d'expression de personnes étant contre l'intervention étatsunienne lors de la première guerre mondiale, le juge Holmes dit que « l'ultime bien commun ne peut être atteint que par la libre circulation des idées ». Lors de l'apparition du projet de RGPD en 2012, il y a eu une certaine réticence à cette idée de droit à l'oubli outre-Atlantique, où de nombreux médias se sont inquiétés sur les conséquences que pourrait avoir ce droit sur la liberté d'expression[87].

Très souvent, l'intérêt légitime du public à s'informer sera jugé supérieur lorsqu'il est en conflit avec le droit au respect de la vie privée. L'affaire *Haynes v. Alfred A. Knop, Inc.*[88] nous montre un aperçu de ce conflit de droits. En l'espèce, il était question de la publication d'un livre traitant de la migration des populations rurales étatsuniennes vers les zones urbaines du nord entre les années 1940 et 1970. Un personnage existant réellement était décrit dans le livre. L'homme était décrit comme ayant eu un mariage chaotique, où son alcoolisme l'avait rendu parfois violent envers son épouse. Plusieurs dizaines d'années plus tard, il est devenu diacre d'une Eglise et s'est remarié. Aucune personne de la communauté n'était au courant de son passé. Il assigne donc l'auteur du livre en responsabilité, sur la base du tort de *public disclosure of private facts.*

Sa demande a été rejetée non-pas en raison de l'intérêt légitime qu'aurait pu avoir la communauté envers le passé de leur diacre actuel, mais en raison de l'intérêt historique de l'œuvre. Le juge considère que tous les détails révélés au sujet de la vie du demandeur sont nécessaires au propos du livre, dès lors le public a un intérêt légitime à les voir, parce que sans eux le livre perd de sa substance. C'est un exemple de la personne individuelle sacrifiée pour l'intérêt collectif : nul doute que le demandeur a dû voir sa vie bouleversée, d'autant plus qu'il était devenu un notable de la communauté et avait trouvé la rédemption.

On peut reprocher au juge la rigidité de son raisonnement. La vie privée du demandeur et les faits racontés dans le livre ne sont pas incompatibles, il n'était pas du tout nécessaire de choisir entre l'un ou l'autre. Il aurait suffi d'employer un nom fictif, ou même ne pas employer de nom du tout. Ainsi, la vie privée du demandeur aurait été préservée tout autant que les propos du livre. Mais le juge rejette cet argument et va jusqu'à dire que le changement du nom aurait changé lui aussi le propos du livre, qui aurait eu moins de crédibilité. Notons qu'ici, l'intérêt légitime repose à la frontière de la liberté d'information et du droit à l'histoire, ou même de la transparence à fin

[86] *Abrams v. United States*, 250 U.S. 616, 1919
[87] Voir par exemple Adam Thierer*, Europe's 'Right to Be Forgotten': Privacy as Internet Censorship*, The Technology Liberation Front, 23 janvier 2012 ; ou encore Jerry Brito, *Your Right to Be Forgotten and My Right to Speak*, blog post, June 7, 2012
[88] *Haynes v. Alfred A. Knopf, Inc*., 8 F.3d 1222, 7th Cir, 1993

d'archives. C'est un concept qui ne se rattache donc pas seulement à la liberté d'expression, il est utilisé à chaque fois que l'intérêt commun est en jeu.

L'intérêt de cette affaire est qu'elle met en scène la forme primaire du droit à l'oubli. Il s'agit simplement d'un homme qui a changé et qui souhaite effacer son passé, ou en tout cas que ce dernier ne puisse pas ressurgir à tous moments pour ruiner sa vie actuelle. Il s'agit de droit au repentir. Le droit à l'oubli existe exactement pour ce genre de cas. On voit bien la limite qu'a le droit au respect de la vie privée aux Etats-Unis, balayé par les vents de la liberté d'information sans même un reproche pour l'auteur du livre qui a conservé le nom réel du demandeur. On peut y voir un raisonnement très typique de la *common law*. Son pragmatisme fait souvent primer le cas général sur le cas particulier, aussi dramatique soit-il. Le juge exprime en effet sa compassion pour le demandeur et sa compagne, il n'est pas insensible à leur situation. En France, même si l'intérêt historique des faits racontés avait été soulevé, il est probable que l'absence d'anonymisation aurait été reprochée à l'auteur.

Section 2 / En France, un intérêt légitime du public contre le droit à l'oubli

L'intérêt du public est discernable par trois fois dans l'article 17 du RGPD. Dans la première exception posée par le paragraphe 3, il est un corolaire de la liberté d'information. Il est également cité pour l'exception de transparence ou de droit à l'histoire. Enfin, il est cité pour l'exception de santé publique. Il semble donc qu'il soit la principale raison de la limitation du droit à l'oubli, les autres conditions limitatives étant plus rares. Sur tous les arrêts publiés par la Conseil d'Etat, à chaque fois il est cité au moins en partie pour justifier du refus de la demande en annulation. Il est donc pertinent d'étudier ces arrêts.

Notons que les articles et décisions visées sont à chaque fois les mêmes que dans l'arrêt précité, au mot près, seule la décision finale diffère. Le Conseil d'Etat cite l'article 17, parfois l'article 9 quand il s'agit d'informations sensibles et cite l'arrêt de la CJUE du 24 septembre 2019 sur les conditions d'application du droit à l'oubli. Ensuite, dans le dispositif, le Conseil d'Etat explique en quelques lignes pourquoi la CNIL a pu ou n'a pas pu légalement estimer que le déréférencement était opportun. L'intégralité du raisonnement ne sera pas réexpliquée, nous reprendrons simplement la décision finale.

Dans un premier cas[89], il s'agit de l'intérêt du public lié à la liberté d'information. En l'espèce, il s'agissait d'un maire d'une ville de taille moyenne qui a eu, en 2013, des propos très violents sur les gens du voyage. Les propos ont été tenus dans le cadre de sa vie privée, le demandeur affirmant qu'il ignorait être enregistré. Il a été condamné un an plus tard pour apologie de crimes contre l'humanité. Il souhaite le

[89] Conseil d'Etat, 10e et 9e chambres réunies, n°405464, 6 décembre 2019

déréférencement de liens faisant état de sa condamnation et de ses propos. La CNIL va rejeter sa demande, et le Conseil d'Etat va confirmer sa décision.

Comme dans le précédent arrêt, la CNIL a scruté un faisceau d'indices, composé du contenu des propos, du contexte, de leur source et de la place qu'a la personne qui les a tenues dans la vie publique. Sans surprise, le Conseil d'Etat et la CNIL vont tomber d'accord. La gravité des propos[90] et sa qualité de maire et de député depuis plusieurs années justifient le maintien des liens litigieux. Il en va naturellement de l'intérêt public que les habitants d'une ville sachent que leur maire tienne de tels propos. Cette affaire est un cas typique de personnalité dont la vie privée est mise en balance avec la liberté d'information du public. La solution paraît assez évidente, et il n'y pas lieu de la commenter plus avant. Nous soulèverons simplement que ce type de litiges était déjà très courant quand le droit à l'oubli n'existait pas.

Dans une seconde affaire[91], il s'agissait d'un médecin généraliste souhaitant le déréférencement de deux liens divulguant les coordonnées postales et téléphoniques de son cabinet et laissant la possibilité de rédiger des appréciations. La CNIL va également débouter la requérante, toujours pour une question d'intérêt prépondérant du public. Le Conseil d'Etat va rejeter son recours pour excès de pouvoir. Il est assez difficile de savoir quel est le motif du déréférencement. Il ressort de l'arrêt que la requérante semble avoir simplement tapé son nom sur un moteur de recherche et soit tombée sur ces sites référençant son travail de généraliste sans qu'elle ait donné son accord. Ce serait alors un cas de traitement illicite. Il est toutefois possible que l'on soit dans le cadre d'un retrait du consentement, ou même d'une absence de finalité. Il est dommage de ne pas en savoir plus sur le motif, car cela joue sur la décision. Un traitement illicite parait être une demande plus sérieuse qu'un retrait de consentement, par exemple.

Encore une fois, l'intérêt légitime va l'emporter ici. Cet intérêt est dans le cadre de la santé publique. Supposons que la demande ait été faite sur la base d'un traitement illicite, avec donc une absence de consentement. Cela veut dire que la santé publique est un intérêt supérieur à celui du respect du consentement du demandeur. Cette décision est justifiée, le but d'un médecin généraliste est de venir en aide aux personnes malades qui en ont besoin, et pour cela elles ont besoin de l'adresse du cabinet. L'atteinte à la vie privée n'est donc pas très importante, car cette atteinte fait partie de la vocation professionnelle de la demandeuse.

Dans la dernière affaire[92], il s'agit d'une personne demandant le retrait de deux liens menant vers un brevet qu'il avait elle-même déposé en 2006 auprès de l'Organisation Mondiale de la Propriété Intellectuelle. Ces liens faisaient également mention de son adresse. La CNIL va débouter sa demande, au motif que le code de la propriété intellectuelle dispose que les coordonnées des personnes déposant un brevet font l'objet d'une publicité en raison de l'intérêt scientifique qu'elles contiennent

[90] « Comme quoi, Hitler n'en a peut-être pas tué assez, hein »
[91] Conseil d'Etat, 9e et 10e chambres réunies, n°405910, 6 décembre 2019
[92] Conseil d'Etat, 9e et 10e chambres réunies, n°405910, 6 décembre 2019

pour les autres chercheurs qui veulent établir un contact. Le Conseil d'Etat a annulé la décision.

Il s'agit ici d'un cas de retrait du consentement, puisque le demandeur a lui-même déposé son brevet en 2006 et a donc agrée à partager les données litigieuses. Le Conseil d'Etat a encore une fois scruté le faisceau d'indices pour peser deux intérêts l'un contre l'autre, ici l'intérêt de la recherche scientifique contre le droit au respect de la vie privée. L'intérêt scientifique ne survit pas à cette pesée des droits, notamment en raison de l'ancienneté du brevet, le fait que le demandeur n'a plus de droits dessus depuis 2010, et qu'il n'a pas fait d'autres contributions à la communauté scientifique. L'intérêt pour la recherche est donc très limité et ne justifie pas la publicité de son adresse.

Plusieurs remarques peuvent être faites sur ces trois arrêts. L'intérêt légitime du public a été cité par trois fois, pour trois nécessités différentes : la recherche scientifique, la liberté d'information et la santé publique. Il apparaît donc qu'il sera la principale opposition que les demandeurs rencontreront pour toute demande de référencement. Or c'est le cas aussi aux Etats-Unis pour tout recours concernant la divulgation de faits privés. Les juges outre-Atlantique mesurent quelle est la plus grosse atteinte entre celle faite à la vie privée et celle faite à l'intérêt du public à s'informer. On a donc un même raisonnement pour deux droits différents. Cela conforte la théorie selon laquelle le droit à l'oubli n'est pas vraiment un droit à part entière. Il est un prolongement plus poussé du droit au respect de la vie privée, en ce qu'il permet de récupérer une information déjà donnée, alors que le droit à la vie privée protège une information qui n'aurait pas dû sortir dans l'espace public.

Le terme oubli a fait couler beaucoup d'encre depuis la proposition de RGPD de 2012, car dans l'imaginaire il évoque l'effacement de toute information, pas seulement sur internet mais aussi dans la mémoire humaine. Lorsque l'on regarde la réalité des faits, le droit à l'oubli n'est qu'un outil supplémentaire pour faire respecter le droit à la protection des données, et il consiste à déréférencer, pas à effacer et encore moins à oublier. Notons que la CNIL fait preuve d'une précaution particulière pour juger des demandes de déréférencement. De 2014 à 2016, 700 plaintes ont été enregistrées par la CNIL sur le sujet, dont 30% ont été accueillies favorablement[93]. Le droit à l'oubli n'est pas vraiment un manque en tant que tel aux Etats-Unis, son absence est simplement la conséquence d'une moins grande protection de la vie privée au profit d'autres droits. Le pays possède tout de même un texte fédéral sur le droit à l'oubli des mineurs, qu'il convient de comparer à la réglementation française et européenne sur le sujet.

[93] « Bilan 2015, un nombre record de plaintes », 8 avril 2016, https://www.cnil.fr/fr/bilan-2015-un-nombre-record-de-plaintes

Chapitre 3 / L'exercice du droit à l'oubli pour les mineurs

A une époque où les mineurs sont munis d'un portable et d'un accès internet de plus en plus tôt, il est nécessaire de les protéger de façon plus poussée contre les dangers du numérique. Aux Etats-Unis, ils sont protégés par le *Children's Online Privacy Protection Act* (COPPA) de 1998 (1) tandis qu'en France le RGPD leur octroient des garanties renforcées (2).

Section 1 / Le COPPA, seule texte instituant un droit à l'oubli aux Etats-Unis

Ce texte s'applique pour tous les mineurs ayant moins de 13 ans[94]. Il est possible de voir cela comme une première limite, 13 ans étant un âge relativement jeune. Un adolescent de 14 ou 15 ans n'est souvent pas familier des risques et des conséquences que son consentement peut avoir sur internet. Il aurait peut-être été judicieux de protéger les mineurs jusqu'à un âge plus avancé.

Le texte s'adresse à tous les sites web s'adressant aux enfants ou ayant conscience qu'ils collectent des données auprès d'eux[95]. Le texte exige que le consentement des parents au traitement des données doit être impérativement collecté de manière vérifiable pour tout mineur de moins de 13 ans[96]. L'opérateur doit également notifier les parents de l'utilisation des données collectées[97]. La protection est donc plutôt solide. Le consentement des parents n'est pas seulement demandé, il doit être vérifiable, ce qui empêche tout consentement accidentel du mineur. Le problème est que vérifier que le consentement a bien été accordé par un parent et non par le mineur est très dur à mettre en place sur internet. La notification de l'utilisation du traitement s'apparente à l'obligation de donner son consentement pour une finalité précise qu'impose le RGPD[98]. Le texte commande également que les données doivent être traitées seulement pour accomplir la finalité exprimée, ce qui est aussi une mesure du RGPD, qui accepte le changement de finalité seulement sous certaines conditions[99]. Ces similitudes montrent l'importance de cette notion de finalité : elle permet de protéger l'information contre des utilisations qui n'ont pas été consenties.

---

[94] "Child means an individual under the age of 13" COPPA, §312.2

[95] "Web site or online service directed to children means a commercial Web site or online service, or portion thereof, that is targeted to children" COPPA, §312.2

[96] "An operator is required to obtain verifiable parental consent before any collection, use, or disclosure of personal information from children" COPPA, §312.5

[97] "An operator must make reasonable efforts, taking into account available technology, to ensure that a parent of a child receives direct notice of the operator's practices with regard to the collection, use, or disclosure of personal information from children" COPPA, 312.4

[98] RGPD, article 6, 1) a)

[99] RGPD, article 6, 4)

En ce qui concerne le droit à l'oubli, le texte dispose que tout parent doit avoir la possibilité à tout moment de refuser le traitement actuel ou futur par l'opérateur[100]. La possibilité d'effacer existe bel et bien, le parent dispose d'un droit d'opposition que les sites doivent pouvoir lui fournir. Le problème réside dans l'application effective de ce droit d'opposition. C'est la *Federal Trade Comission* (FTC) qui s'occupe de sanctionner le non-respect du COPPA. Ce texte n'ouvre aucun recours individuel, c'est le procureur général de l'Etat où est commise la violation qui saisit la FTC pour obtenir l'effacement des données.

L'absence du recours individuel est un problème, il serait beaucoup plus simple d'ouvrir des possibilités de poursuite pour tout parent constatant un traitement illicite ou voulant effacer des données. Le passage par l'administration étatique ralentit forcément le processus. Si la forme de l'action n'est pas optimale, les résultats peuvent être tout à fait satisfaisants, la FTC ayant le pouvoir de sanctionner lourdement un site ne respectant pas le COPPA.

Dans l'affaire *United States v/ W3 Innovations*[101], LLC, une compagnie développant des applications pour enfants collectait toutes leurs adresses mails et donnait la possibilité de publier des informations personnelles en ligne, sur ce qui s'apparentait à un réseau social pour enfants. La compagnie n'a pas pu prouver qu'elle notifiait les parents des usagers de la finalité des informations collectées et que c'était bien les parents qui consentaient au traitement des données. En conséquence, l'affaire s'est terminée par une transaction entre la FTC et la compagnie, qui s'engageait à payer 50 000 dollars d'amende pour violation du COPPA et d'effacer toutes les données litigieuses.

Il a été dit plus haut que le droit à l'oubli doit se comprendre dans le sens d'un déréférencement ou d'une décontextualisation, pas d'un réel effacement. En l'espèce, c'est pourtant la suppression totale qui a été ordonnée, la forme la plus complète de droit à l'oubli. Il est très rare qu'une telle injonction soit prise, et sa radicalité mérite d'être nelevée. La FTC fait preuve d'une redoutable efficacité en la matière, elle n'hésite pas à ordonner des mesures drastiques. Cela constitue bien la preuve que les Etats-Unis connaissent tout à fait du droit à l'oubli, c'est simplement qu'il n'est disponible que pour les mineurs, qui bénéficient d'une plus grande protection des données. En Europe, le RGPD dispose aussi d'une protection augmentée pour les mineurs, même si cette protection n'est pas aussi forte que dans le projet de RGPD de 2012.

[100] "The opportunity at any time to refuse to permit the operator's further use or future online collection of personal information from that child, and to direct the operator to delete the child's personal information" COPPA, §312.6

[101] *United States v. W3 Innovations*, LLC, No. CV-11-03958, FTC File No. 102 3251 (N.D. Cal. Sept. 8, 2011)

Section 2 / Le RGPD, un recul de la protection des mineurs par rapport au texte initial

Le RGPD consacre son article 8 à la protection des mineurs, dont le consentement bénéficie d'une protection augmentée. La protection est destinée aux mineurs de moins de 16 ans, sachant que les Etats membres ont la possibilité de moduler cette limite d'âge jusqu'à un minimum de 13 ans. La législation est donc un peu plus protective que le COPPA, car la limite de protection peut aller jusqu'à 16 ans, en fonction de la volonté des Etats membres. Dans l'article 4 du projet de RGPD, qui contient toutes les définitions des termes utilisés dans le règlement, il était prévu de définir un enfant comme toute personne âgée de moins de 18 ans, reprenant ainsi la définition retenue par la Convention des Nations Unies concernant les droits de l'enfant. Cette définition n'a pas été retenue, et le terme « enfant » n'est donc tout simplement pas défini dans le RGPD.

Cet abandon de la définition est contestable. Les mineurs méritent d'être protégés plus amplement que les majeurs, et cette protection passe par poser clairement la distinction entre les deux statuts. Il aurait peut-être été plus judicieux de conserver une définition de l'enfant dans l'article 4, même si cela impliquait de ne pas conserver la définition des Nations Unies.

Les rédacteurs ont donc laissé le choix aux Etats Membres de choisir un âge entre 13 et 16 ans. Cela a l'avantage de la flexibilité, en fonction de chaque culture des Etats membres, qui pourront probablement conserver leur législation sur le sujet. Imposer à tous un âge un peu plus élevé aurait toutefois étoffé la protection. Les 18 ans posés par les Nations Unies sont peut-être un peu trop protecteurs, mais maintenir l'âge à 16 ans aurait été idéal.

La protection augmentée est très comparable à celle des Etats-Unis, car le traitement concernant des mineurs de moins de 13 ou 16 ans est licite seulement si c'est un parent qui a donné le consentement. Cela concerne seulement les offres directes de la société de l'information aux enfants.

L'article ajoute par ailleurs dans son paragraphe 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 ». La formule est au mot près similaire à ce que le COPPA dispose : « An operator must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology ». La reprise mot pour mot n'est certainement pas un hasard, et nul doute que le RGPD l'a repris du COPPA. Il est étonnant de voir cette similitude entre les deux pays en ce qui concerne la protection des mineurs, alors qu'il a été vu plus haut que les législations sur la protection des données et sur la vie privée sont radicalement opposées. On peut en conclure que peu importe les différences de point de vue, la protection des mineurs reste une priorité quel que soit le système de droit.

En ce qui concerne le droit à l'oubli, l'article 17 contient une disposition précise concernant les mineurs. Le paragraphe 1 f) de cet article dispose que l'effacement est possible lorsque « 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 ». Tout traitement des données concernant les mineurs de 13 ou 16 ans est donc susceptible d'une demande d'effacement, nonobstant toute considération de finalité, de consentement ou d'illicéité. Le déréférencement est possible par le statut même de la personne ayant consenti au traitement. L'article 17 offre ici une procédure accélérée pour le droit à l'oubli des mineurs, qui sont susceptibles de demander un déréférencement sans condition aucune, ce qui offre un filet de sécurité supplémentaire en plus de l'article 8. Cette initiative est louable, elle montre que les rédacteurs ont conscience de la dangerosité d'internet pour les enfants.

Cette disposition n'était pas dans le projet de RGPD, où il était simplement mentionné que l'effacement était possible « en particulier en ce qui concerne des données à caractère personnel que la personne concernée avait rendues disponibles lorsqu'elle était enfant »[102]. Il est de bon ton que la disposition sur l'article 8 ait été ajoutée, car cette phrase générale n'a pas vraiment portée juridique précise et n'aurait pas suffi à mieux protéger les mineurs. Il est toutefois dommage qu'elle ait été enlevée, une emphase sur la protection des enfants étant toujours un plus. La disposition du §1 f) ne mentionne que l'article 8 et pas le mot enfant, ce qui empêche de comprendre au premier regard qu'il s'agit d'une sécurité réservée aux mineurs. La phrase a été reléguée au considérant 65 du RGPD, dont la juridicité n'est pas avérée. Il est vrai qu'une disposition générale comme celle-là a peut-être plus sa place dans les considérants que dans la lettre du texte.

[102] Projet de RGPD, COM/2012/011 final, article 17 §1

Conclusion

Le but de cette étude était de dresser un portrait général du droit à l'oubli en France et aux Etats-Unis, en essayant de comprendre pourquoi le terme a germé dans l'Hexagone et pas outre-Atlantique. Le premier élément de réponse est la conception de la vie privée étatsunienne, qui est morcelée et dont tous les domaines ne sont pas protégés avec la même intensité. Si le volet de l'autonomie de la volonté est très bien protégé constitutionnellement, le volet de la protection des données n'a pas encore été consacré par la Cour Suprême. Au niveau fédéral, le choix de la protection sectorielle est trop centré sur la protection des consommateurs vis-à-vis du marché, et pas assez sur l'individu. Ceci est dû à l'absence de droits de la personnalité dans la culture de la *common law*, qui de par son caractère pragmatique légifère sur des problèmes ciblés et ne connait pas vraiment de principes généraux.

Dans les caractères du droit à l'oubli, la principale barrière aux Etats-Unis est leur conception du consentement, qui est lié au mur existant entre vie privée et vie publique. Quand une information sort de la vie privée, il est très difficile de la récupérer aux Etats-Unis, là où le RGPD a prévu une possibilité de retirer son consentement pour exercer le droit à l'oubli.

Malgré toutes ces différences, il s'avère que la principale limite dans les deux pays pour limiter le droit au respect de la vie privée aux Etats-Unis et le droit à l'oubli en France est l'intérêt légitime du public, concept malléable pouvant servir la liberté d'information tout comme le droit à la santé ou la recherche scientifique. Les arrêts étudiés nous ont permis de comprendre que le droit à l'oubli n'est pas un droit nouveau. Il est un embranchement du droit au respect de la vie privée, il n'est qu'un outil à son service. Les auteurs croyant y voir une nouvelle forme de despotisme pouvant ordonner l'oubli au mépris de tous les droits fondamentaux se sont donc fourvoyés.

Le droit à l'oubli n'est d'ailleurs pas totalement absent de la législation étatsunienne : il existe et est effectif pour les mineurs et commence à voir le jour dans les législations étatiques pour tous les individus. Il est temps pour les Etats-Unis de s'inspirer de l'Union européenne sur le sujet, car le rayonnement du RGPD finira peut-être par les atteindre qu'ils le veuillent ou non. Le 27 mars dernier, le Conseil d'Etat a en effet rendu un arrêt limitant la portée territoriale du droit au déréférencement. Son raisonnement est que si le RGPD n'interdit pas que le déréférencement porte sur l'intégralité des versions d'un moteur de recherche, il ne l'autorise pas non plus. Il déclare qu'il faut suffisamment mettre en balance les droits de la personne concernée et le droit à la liberté d'information pour pouvoir décider d'étendre une injonction à toutes les versions d'un moteur de recherche. Le Conseil d'Etat fait pour l'instant preuve de précaution car le droit à l'effacement n'est institué que depuis deux ans, et sa portée reste insuffisamment définie. Toutefois, comme la protection des données semble aller de plus en plus loin, rien ne nous dit qu'il ne durcira pas sa position un jour prochain…

Bibliographie

Bibliographie française et européenne

Ouvrages généraux

- BENSOUSSAN Alain, *Règlement européen sur la protection des données, textes, commentaires et orientations pratiques*, Bruylant, 2018

- BENTHAM John, Panopticon, Works, Browning, 1780

- DECHENAUD David, Le droit à l'oubli numérique, données nominatives, approche comparée, Larcier, 2015
-
- DELEUZE Gilles, *Pourparlers 1972 - 1990*, Les éditions de Minuit, 1990

- FOUCAULT Michel, *Dits et Écrits*, t. 2, Gallimard, 2001

- FOUCAULT Michel, *Surveiller et Punir,* Gallimard, 1975

- GROSJEAN Alain, Enjeux européens et mondiaux de la protection des données, Larcier, 2015

- HARCOURT Bernard, La société d'exposition, Seuil, 2020

- NIETZSCHE Friedrich, *Considérations intempestives*, Aubier-Montaigne, 1874

Articles

- BOIZARD Maryline*, Le temps, le droit à l'oubli et le droit à l'effacement*, *Les Cahiers de la Justice*, vol. 4, no. 4, 2016

- COSTAZ Catherine, *Le droit à l'oubli,* Gaz. Pal 1995. p. 961

- FALQUE-PIERROTIN Isabelle, *Internet et les réseaux numériques*, rapport du Conseil d'Etat, 1998

- LE STRUGEON Stéphanie, *Le California Consumer Privacy Act : premier pas vers un RGPD américain,* Revue de l'Union européenne 2020 p.41

- SIREDEY-GARNIER Fabienne. *Le droit à l'oubli et la loi du 29 juillet 1881*, *LEGICOM*, vol. 57, no. 2, 2016

- THYRAUD Jacques, *Rapport n°72 relatif à la loi Informatique et libertés*, 1977

Commentaires de jurisprudence

- TGI Seine, 4 oct. 1965, JCP 1966 II, 14482, obs. Lyon Caen

Décisions de jurisprudence

- TGI Seine, 4 oct. 1965
- TGI Paris, 14 avril 2008
- Cass. Civ. 1ère, 6 mars 1996, n° 94-11273
- Cass. Civ. 1ère, 10 mai 2005, n°02-14.730
- Cass. Crim, 14 décembre 2010, n°10-80.088
- Conseil d'Etat, 10e et 9e chambre réunies, n° 429154, 6 décembre 2019
- Conseil d'Etat, 9e et 10e chambres réunies, n°405910, 6 décembre 2019
- Conseil d'Etat, 10e et 9e chambres réunies, n°405464, 6 décembre 2019
- Conseil d'Etat, 10e et 9e chambres réunies, N° 399922, 27 mars 2020
- Conseil constitutionnel, 18 janvier 1995, n° 94-352 DC
- Conseil constitutionnel, 23 juillet 1999, n° 99-416 DC
- Conseil Constitutionnel, 13 mars 2014, n°2014-690
- CEDH, sect. IV, 20 mars 2007, Tysiac c/ Pologne, n°5410/03
- CEDH sect. II, 18 novembre 2008, C. c/ Turquie, n°22427/04
- CEDH sect. III, 27 octobre 2009, H c/ Roumanie, n°21737/03
- CEDH, sect. III, 2 octobre 2012, Knecht c/ Roumanie, n° 10048/10
- CJUE, Google Spain SL, Google Inc. / Agencia Española de Protección de Datos, Mario Costeja González, C-131/12, 13 mai 2014
- CJUE, C-136/17, 24 septembre 2019

Textes normatifs

- Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

- Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STCE), Conseil de l'Europe, 28 janvier 1981

- Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

- Charte des Droits Fondamentaux de l'Union Européenne du 7 décembre 2000

- Règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD)

Bibliographie étrangère

Ouvrages généraux

- HARD Michael & NEGRI Antonio, *Empire*, Harvard University Press, 2000

- MAYER-SCHÖNBERGER Victor, *Delete, the virtue of forgetting in the digital age,* Princeton University Press, 2009

Articles

- BRITO Jerry, *Your Right to Be Forgotten and My Right to Speak*, blog post, June 7, 2012

- PARKER E., CAHILL L., McGAUGH J. L., *A Case of Unusual Autobiographical Remembering,* Neurocase, Février 2007

- ROSEN J., *The right to be Forgotten*, 64 Stanford Law Review online 88

- SCHWARTZ P.M. et PEIFER K-N, *Transatlantic Data Privacy*, Georgetown Law Journal, 2017, n° 106, p. 115

- THIERER Adam*, Europe's 'Right to Be Forgotten': Privacy as Internet Censorship*, The Technology Liberation Front, 23 janvier 2012

- WARREN Samuel, BRANDEIS Louis, *The right to privacy*, Harvard Law Review, vol. 4, 1890, pp. 193-220

Décisions de jurisprudence

Arrêts de la Cour Suprême des Etats-Unis

- *Abrams v. United States, 250 U.S. 616, 1919*
- *Grisworld v. Connecticut, 381 U.S. 479, 1965*
- *Katz v/ United States, 389 U.S. 387, 1967*
- *Loving v. Virginia, 388 U.S. 1, 1967*
- *Roe v/ Wade*, 410 U.S. 113, 1973
- *Whalen v. Roe*, 429 U.S. 589, 1977
- *Nixon v/ Administration of General Services*, 433 U.S. 425, 1977
- *Nasa v. Nelson*, 562 U.S. 134, 2011
- *Obergell v. Hodges*, 576 U.S. 644, 2015

Arrêts d'autre cours étatsuniennes

- *Melvin v. Reid, 112 Cal.App. 285, 297 P. 91, 1931*
- *Gill v/ Heart Publishing Co, 40 Cal.2d 224, 1953*
- *Duran v/ Detroit News*, 504 N.W.2d 715, Mich. Ct. App, 1993
- *Multimédia WMAZ, Inc v/ Kubach 443 S.E.2d 491, Georgia Ct. App, 1994*
- *Haynes v. Alfred A. Knopf, Inc., 8 F.3d 1222, 7th Cir, 1993*
- *United States v. W3 Innovations*, LLC, No. CV-11-03958, FTC File No. 102 3251 (N.D. Cal. Sept. 8, 2011)

Textes normatifs

- Code of fair information Practices, 1973
- Restatement (Second) of Torts, 1977
- Cable Communications Policy Act, 1984
- Health Insurance Portability Act, 1996
- Children's Online Privacy Protection Act, 1998
- California Consumer Privacy Act, 2020

Table des matières

Annexes

Article 17
EU RGPD
"Droit à l'effacement («droit à l'oubli»)"

1. 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.

2. 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.

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.