DONNÉES PERSONNELLES

Le California Consumer Privacy Act : beaucoup de bruit pour rien ?

En Californie, une loi sur la protection des données personnelles vient d'entrer en vigueur. Souvent comparée au RGPD, cette loi est en fait d'une portée bien plus limitée, aussi bien dans son champ d'application que dans les droits qu'elle confère aux consommateurs californiens et dans les obligations qu'elle impose aux entreprises dans cet État.

Les traditionnels vœux de nouvel an ont été accompagnés, cette année, dans de nombreuses boîtes e-mail, de notices d'information concernant le traitement de leurs données personnelles par des sociétés californiennes. En effet, le California Consumer Privacy Act ((« *CCPA* »), adopté le 28 juin 2018, est entré en vigueur le 1er janvier 2020. Cette loi est souvent présentée comme le pendant californien du RGPD, et ses dispositions concernant l'information et les droits de consommateurs s'en rapprochent effectivement. Cependant, elle est d'une portée extrêmement limitée et les obligations qu'elle impose aux entreprises californiennes semblent dérisoires comparées à l'approche globale adoptée par le RGPD et sa mesure emblématique, le privacy by design.

Une compétence matérielle et territoriale beaucoup plus restreinte que le RGPD

Comme son nom l'indique, le CCPA ne traite que des données personnelles des consommateurs résidant en Californie collectées par des entreprises dans le cadre de leurs activités professionnelles. Bien que la protection de la vie privée soit inscrite dans la constitution californienne, le CCPA n'est donc qu'une législation sectorielle et non un texte cherchant à mettre en œuvre de façon générale des principes fondamentaux du droit.
Son application est d'autant plus restreinte que le législateur californien a fait le choix d'en exempter les entreprises de petite et moyenne taille, et qu'il ne concerne donc que les entreprises ayant une activité commerciale en Californie et :

- ayant un chiffre d'affaires supérieur à vingt-cinq millions de dollars (25.000.000 US$) ;
- achetant, recevant à des fins commerciales, vendant ou partageant à des fins commerciales, seules ou avec des tiers, les informations personnelles de plus de 50.000 consommateurs ; ou
- générant plus de cinquante pour cent de ses revenus annuels de la vente de données personnelles des consommateurs[1].

Cette présence d'un seuil de chiffre d'affaires à partir duquel les obligations du CCPA sont applicables, associée à une exception pour les sociétés dont l'activité concerne spécifiquement la collecte et le traitement des données personnelles semble très pragmatique. Comme l'exprimait le Professeur Frisson-Roche récemment dans ces colonnes[2], on regrette que le RGPD, dont les coûts de mise en œuvre sont bien plus élevés, n'ait pas adopté une approche similaire et ne permette qu'une exemption très partielle pour les PME (absence d'obligation de tenir un registre pour les sociétés de moins de 250 employés), qui est de plus d'un intérêt assez limité.

La notion de résident californien est définie par référence à sa définition fiscale dans le California Code Of Regulation[3] comme toute personne présente dans l'État pour tout objet autre que temporaire ou transitoire et toute personne domiciliée dans l'État se trouvant hors de l'État pour une raison temporaire ou transitoire. Tous les résidents européens qui ont reçu une notice CCPA dans leurs boîtes mail ont donc été victimes des politiques d'envoi généralisé de ces notices alors qu'ils n'étaient pas concernés par l'application du CCPA (et donc d'un traitement de données dont la conformité au RGPD semble plus que douteuse...).

Ce choix des personnes concernées comme critère de l'application territoriale constitue une différence majeure avec le RGPD qui utilise à titre principal, pour établir sa compétence, l'existence d'un établissement du responsable de traitements ou du sous-traitant dans l'Union européenne puis, à titre subsidiaire, l'existence

de traitements par des responsables de traitement et sous-traitants établis hors de l'Union européenne mais qui sont dirigés vers des personnes concernées se trouvant sur le territoire de l'Union européenne. Le CCPA protège donc uniquement les résidents de l'État de Californie alors que l'approche européenne a tout d'abord été de chercher à policer les traitements de données effectués sur son territoire, pour n'acquérir qu'avec le RGPD un caractère extraterritorial en poliçant également les traitements effectués hors de l'Union européenne mais visant les ressortissants communautaires, ce dernier critère de rattachement étant d'ailleurs beaucoup moins clairement défini que dans le CCPA et devant faire l'objet d'une clarification jurisprudentielle.

Alors que le RGPD a pour vocation de couvrir tous les traitements de données effectués dans l'Union européenne ou ciblant des personnes concernées situées dans l'Union, le CCPA ne concerne que les traitements des informations personnelles des Californiens, où que soient situés le responsable de traitement ou le sous-traitant, ce qui lui donne paradoxalement une extra-territorialité au moins aussi importante que celle du RGPD.

Quelques notions de base similaires

Le CCPA définit tout d'abord les informations personnelles comme toute « *information qui directement ou indirectement, identifie, est liée à, décrit, peut être associée, ou pourrait raisonnablement être associée à un consommateur ou un foyer particulier.* »[4] Le CCPA énonce ensuite une très longue liste d'exemples, non limitatifs, d'informations personnelles qui incluent le nom, l'adresse, l'adresse IP, l'adresse e-mail, le numéro de sécurité sociale, de passeport, de permis de conduire, numéro de carte bancaire, informations biométriques, informations commerciales, historique de navigation sur Internet, données de géolocalisation…

Cette définition est très proche de celle du RGPD qui définit comme une donnée à caractère personnel « *toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»)* » ; et précise ensuite qu' « *est réputée être une 'personne physique identifiable' une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* ».

Il est intéressant de constater que la définition d'informations personnelles du CCPA est plus large que celle qui existait déjà dans le code civil californien et a été étendue par l'utilisation des termes « *directement ou indirectement* » pour qualifier la possibilité d'identifier une personne avec les informations considérées, qui semble un emprunt direct au droit européen. En effet, par cette notion, les autorités de protection des données et la Cour de justice de l'Union européenne ont procédé à une interprétation très extensive de la notion de données personnelles pour inclure par exemple l'adresse IP (qui est expressément couverte par le CCPA) ou comme l'a fait la Cnil, suivie par le Conseil d'État, dans le dossier JC Decaux, les adresses MAC de téléphones portables après qu'elles ont été très fortement pseudonymisées[5]. L'ajout du terme foyer (« *household* ») ne nous semble en revanche pas présenter un véritable intérêt, puisqu'un foyer étant par nature composé d'individus, les informations permettant, directement ou indirectement, l'identification d'un foyer permettent donc dans tous les cas l'identification d'individus.

L'exclusion par le CCPA des données publiquement disponibles, définies comme les données disponibles dans les registres gouvernementaux de la définition des informations personnelles ne constitue pas non plus une différence majeure par rapport au RGPD. Tout d'abord, le CCPA restreint la définition des données en excluant les données biométriques collectées par une entreprise (les données biométriques peuvent en effet par nature être considérées comme publiquement disponibles) mais aussi les données qui sont utilisées pour un objet qui n'est pas compatible avec l'objet pour lequel les données sont collectées et communiquées dans les registres gouvernementaux, ce qui constitue une réelle limite à la réutilisation de ces données. De plus, le RGPD prévoit également un traitement spécial pour les données personnelles présentes dans les registres publics, puisqu'il prévoit, dans son article 86, que les données à caractère personnel figurant dans les documents officiels détenus par une autorité publique pour l'exécution d'une mission de service public peuvent être communiquées conformément au droit applicable de l'État membre afin de concilier le droit d'accès du public aux documents officiels et le droit à la protection de données personnelles. La loi Informatique et libertés[6] prévoit, elle, dans son article 7 que « *ses dispositions ne font pas obstacle à l'application, au bénéfice de tiers, des dispositions relatives à l'accès aux documents administratifs et archives publiques.* » Les deux législations permettent donc le traitement des données personnelles présentes dans les registres publics mais encadrent ces traitements, en les limitant pour le CCPA aux traitements compatibles avec l'objet pour lequel le registre public est maintenu et en instaurant une obligation d'information préalable des personnes concernées pour le RGPD, sauf lorsque cette information se révèle manifestement impossible ou exigerait des efforts disproportionnés.

Finalement, le traitement des informations personnelles est défini comme « *toute opération ou ensemble d'opérations qui est effectuée sur des données*

personnelles ou un ensemble de données personnelles, que ce soit ou non par des moyens automatisés[7] ». Cette définition, beaucoup moins bavarde que celle du RGPD, remplit le même objet puisqu'elle couvre toute manipulation des données personnelles.

Des droits pour les consommateurs beaucoup plus restreints que selon le RGPD

Le CCPA accorde aux consommateurs californiens un droit d'information et un droit d'accès, qui sont beaucoup plus restreints que le RGPD. Étonnamment, d'un point de vue logique, les droits des consommateurs concernant leurs informations personnelles sont énoncés dans le CCPA avant les obligations d'informations des consommateurs, qui sont également très peu étendues au vu de ce qui est prévu par le RGPD.

Les informations mises à disposition du consommateur californien

Toute entreprise soumise au CCPA doit tout d'abord informer le consommateur, au plus tard au moment de la collecte de ses informations des catégories d'informations personnelles le concernant qui sont collectées ainsi que de la finalité du ou des traitements de ces informations. Comme dans le cadre du RGPD, tout traitement ultérieur requiert une nouvelle information. Comparée à la très longue liste d'informations obligatoires de l'article 13 du RGPD, cette mention peut sembler d'un intérêt très limité. Cependant, il est loin d'être certain que la longueur et le caractère indigeste des mentions obligatoires de l'article 13 du RGPD constituent réellement un progrès dans la protection des libertés individuelles, et l'approche américaine, signalant simplement l'existence d'un traitement de données nous semble, sur ce point, plus pragmatique et au moins aussi efficace. En effet, la notice Informatique & libertés soumise aux personnes concernées européennes est probablement encore moins lue que les conditions générales de vente lors de la conclusion de contrats d'adhésion et a donc une utilité pratique quasi nulle.

Le CCPA[8] impose aux entreprises de mentionner dans leurs Privacy Policies ou, en leur absence, sur leur site Internet, les informations suivantes, qui doivent être actualisées au minimum tous les ans : une liste des catégories d'informations personnelles collectées par l'entreprise dans les 12 mois précédents, une liste des catégories d'informations personnelles qu'elle a communiquées à des tiers à des fins commerciales, une description des droit d'accès des consommateurs et de leur droit à ne pas être discriminé sur la base de leur refus de communiquer des informations personnelles. Cette démarche semble plus utile que l'information préalable du RGPD, qui fournit aux personnes concernées des informations au moment où elles ne sont pas intéressées par ces informations, mais n'impose en revanche pas (sauf si le traitement est fondé sur le consentement, ce qui est rarement le cas pour les traitements de données de consommateurs) d'obligation de tenir ces informations à leur disposition quand elles pourraient en avoir besoin.

Le consommateur américain est donc uniquement informé de l'existence d'un traitement de ses données personnelles lors de leur collecte et peut accéder en ligne au type d'information qui est collecté par chaque société et être informé uniquement de son droit d'accès et de son droit de ne pas être discriminé sur la base de son refus de communication. Si l'on peut contester la longueur excessive des mentions du RGPD, il faut convenir que le bilan est ici particulièrement mince. Le responsable de traitement californien ne semble même pas avoir l'obligation d'informer le consommateur californien de la totalité de ses droits en application du CCPA, puisque le droit à l'effacement n'est pas mentionné.

Le droit d'accès

Selon le CCPA, le consommateur californien peut demander à ce que toute entreprise qui collecte ses informations personnelles lui communique les catégories d'informations personnelles le concernant ainsi que les informations spécifiques le concernant qu'elle a collectées, les catégories de sources auprès desquelles ces informations ont été collectées, la finalité commerciale de la collecte ou de la vente de ces informations et les catégories de tiers avec lesquels l'entreprise partage les informations. Le consommateur californien peut également s'adresser aux entreprises qui vendent ses données personnelles ou les communiquent pour des besoins commerciaux pour être informé des catégories d'informations que l'entreprise a collectées à son sujet, des catégories d'informations que l'entreprise a vendues et des catégories de tiers auxquels l'entreprise a vendu ou communiqué ses données.

La notion de finalité semble se rapprocher de celle du RGPD. Cependant, sa définition montre bien l'aspect très sectoriel du CCPA, puisqu'il ne prévoit que 7 finalités possibles pour le traitement des données des consommateurs :

- l'audit lié à une interaction en cours avec les consommateurs et les transactions en cours, y compris le comptage des publicités envers chaque visiteur unique, vérifier le positionnement et la qualité des publicités ;
- la détection des incidents de sécurité, la protection contre des activités frauduleuses et la poursuite de telles activités ;
- le débuggage pour identifier et réparer des erreurs qui gênent une fonctionnalité existante ;
- une utilisation éphémère, sous réserve que les informations personnelles ne soient pas communiquées à un tiers ni utilisées pour construire un profil du consommateur ou altérer son expérience

individuelle en dehors de l'interaction en cours, y compris sans s'y limiter dans le cadre d'individualisation contextuelle de publicités montrées dans le cadre de cette interaction ;
- la fourniture de services au nom de l'entreprise, y compris la maintenance ou la gestion des comptes, la fourniture de services clients, l'exécution des commandes, la fourniture de financement, la fourniture de services de publicité ou de marketing ou d'analyse ou d'autres services similaires ;
- la recherche interne pour le développement technologique ;
- les activités de vérification ou de maintenance de la qualité ou de la sécurité d'un service ou d'un objet possédé, fabriqué par ou pour ou contrôlé par l'entreprise.

Ce droit d'accès est donc extrêmement limité puisque le consommateur américain, contrairement à la personne concernée européenne n'a pas le droit de savoir qui sont les destinataires de ses données ou la durée de leur conservation mais surtout il est d'une faible utilité puisqu'il ne s'accompagne d'aucun droit de rectification et d'un droit d'effacement réduit à la portion congrue.

Le droit à l'effacement

Dans sa rédaction telle qu'elle ressort du CCPA[9], le droit à l'effacement californien peut sembler a priori plus étendu que le droit à l'oubli prévu par l'article 17 du RGPD. En effet, le RGPD prévoit que le droit à l'oubli ne s'exerce que dans 6 cas précisément déterminés et sur ces 6 cas, cinq concernent en fait des cas où la base juridique du traitement a disparu. Le seul cas où le droit à l'effacement peut s'exercer réellement en droit communautaire alors que la base juridique du traitement existe encore est donc le cas où les données ont été collectées sur Internet et, même dans ce cas (ou dans l'un des autres cas) le RGPD prévoit 5 exceptions générales (exercice de la liberté d'expression ; respect d'une obligation légale ; motifs d'intérêt public, archives et recherches scientifiques ; nécessité pour assurer la constatation, l'exercice ou la défense de droits en justice).

Le CCPA adopte une approche différente en posant le droit à l'effacement en principe général, puis en listant 9 exceptions. Sur ces neuf exceptions, il est intéressant de constater que quatre sont communes avec celles prévues au RGPD : exercice de la liberté d'expression ; respect des obligations de l'entreprise en application du code pénal californien ; recherche scientifique ; respect d'une obligation légale. L'exception prévue par le RGPD fondée sur les motifs d'intérêts publics n'a logiquement pas à s'appliquer, puisque le CCPA concerne uniquement les entreprises dans le cadre de leurs relations avec les consommateurs et l'exception concernant la nécessité du traitement de données pour assurer la constatation, l'exercice ou la défense de droits en justice est en fait fournie par une exemption générale des dispositions du CCPA pour ce type de données.

Le CCPA prévoit également 4 exceptions originales à cette obligation d'effacement. La première prévoit le droit pour l'entreprise de continuer à traiter les données si ce traitement est nécessaire « *pour finaliser la transaction pour laquelle les informations personnelles ont été collectées, fournir un bien ou service demandé par le consommateur ou raisonnablement anticipé dans le contexte de la relation d'affaires avec le consommateur ou d'une autre manière pour exécuter un contrat entre l'entreprise et le consommateur* ». Cette exception n'a pas lieu d'exister en droit européen puisque le droit à l'effacement n'y existe pas si le traitement de données est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures pré-contractuelles prises à la demande de celle-ci, sauf si les données ont été collectées sur Internet. Le CCPA prévoit deux autres exceptions qui reflètent la sensibilité californienne aux nécessités de la société de l'information (et le poids du lobbying des sociétés informatiques et de e-commerce) : les données nécessaires pour la détection d'incidents de sécurité et la prévention de la lutte contre la fraude et les données nécessaires pour procéder à des opérations de débuggage pour identifier et réparer des erreurs qui endommagent des fonctionnalités existantes. Concernant ces deux types de traitements de données, ils peuvent généralement être effectués par les entreprise européennes sur la base juridique de l'intérêt légitime (puisque ce traitement ne porte pas a priori atteinte aux libertés et droits fondamentaux des personnes concernées). Cependant, il semble peu probable qu'une autorité européenne trouve que cet intérêt légitime d'une entreprise constituerait un motif impérieux prévalant sur les droits et libertés de la personne concernée lorsque cette dernière formule une demande d'effacement.

La dernière exception propre au CCPA constitue une divergence majeure. En effet, le CCPA prévoit que l'entreprise peut refuser la demande d'effacement du consommateur lorsqu'elle souhaite effectuer toute autre utilisation interne des informations personnelles du consommateur d'une manière légale qui est compatible avec le contexte dans lequel le consommateur a fourni l'information. Alors que le droit européen prévoit expressément un droit de retirer son consentement (quand ce dernier est la base juridique) ou de s'opposer à un traitement fondé sur des motifs légitimes, le droit américain refuse au consommateur tout droit à l'effacement d'un traitement qui était raisonnablement prévisible. On touche là à une différence fondamentale du CCPA par rapport au RGPD. Alors que le RGPD prévoit explicitement que les données ne peuvent être conservées que pendant une durée n'excédant

pas celle nécessaire au regard des finalités du traitement (qui doit être indiquée à la personne concernée), le CCPA lui permet de traiter les données aussi longtemps que le responsable de traitement l'estime nécessaire, le consommateur qui a communiqué une fois les données ne pouvant pas demander l'arrêt du traitement de données tant que ce traitement était prévisible lors de la collecte de données.

Le droit d'interdire la vente de ses informations personnelles

Le CCPA prévoit que le consommateur peut à tout moment interdire à une entreprise de procéder à la vente de ses informations personnelles et oblige les entreprises traitant les informations des consommateurs californiens à installer sur leur site internet un bouton « *Ne vendez pas mes informations personnelles* » permettant au consommateur d'exercer ce droit. Ceci veut dire qu'en l'absence d'interdiction du consommateur, la vente de ses données est autorisée, sous réserve néanmoins qu'il en ait été préalablement informé. Cette interdiction doit de plus être renouvelée tous les 12 mois par le consommateur.

En droit communautaire, de manière générale, la seule base juridique permettant la vente de données personnelles semble être le consentement (sauf si la personne concernée a elle-même vendu ses données pour leur revente, auquel cas le contrat pourrait être considéré comme fondé sur le contrat conclu avec la personne concernée). Le CCPA adopte une approche plus protectrice pour les données des mineurs de moins de 16 ans, pour lesquels le principe est une interdiction qui ne peut être levée que par une autorisation du mineur s'il est entre 13 et 16 ans ou de ses parents.

Le droit de ne pas être discriminé

Le CCPA énonce clairement une interdiction de refuser des biens ou des services, appliquer des prix différents, fournir des biens ou des services de qualité différents ou suggérer que le consommateur recevra des biens ou des services différents suite à l'exercice par le consommateur des droits qui lui sont conférés par le CCPA. Cependant, dans le paragraphe suivant, le CCPA autorise clairement à fournir des compensations financières (y compris sous la forme de différence de prix ou de qualité de produits) pour la vente par le consommateur de ses informations personnelles, sous réserve que la différence soit directement liée à la valeur fournie par les données du consommateur. Cette exception limite fortement cette interdiction de discriminer sur la base de l'acceptation ou non du traitement de ses propres informations personnelles. Cette disposition a cependant le mérite de poser une question que le droit européen a du mal à traiter et qui est celle de la rémunération (au sens large) de la personne concernée pour ses données personnelles. En effet, le droit communautaire ayant une approche de la protection des données personnelles sous l'angle de la défense des libertés publiques, il a tendance à privilégier la défense des droits fondamentaux abstraits des consommateurs sans se préoccuper de leurs intérêts économiques, et en leur ôtant la possibilité de faire un choix reflétant réellement leurs propres priorités.

Des modalités de mise en œuvre clairement définies

Le CCPA est très clair sur les modalités d'exercice de leurs droits par les consommateurs. Toute entreprise doit tout d'abord mettre à la disposition des consommateurs au moins deux méthodes pour exercer leur droit d'information, y compris un numéro de téléphone gratuit et si l'entreprise dispose d'un site internet, une page internet. Toute entreprise saisie par un consommateur d'une demande d'exercice de ses droits doit y répondre gratuitement dans les 45 jours par courrier postal ou électronique mais peut appliquer, après information préalable du consommateur, une période additionnelle de 45 jours. L'entreprise a le droit de vérifier l'identité du consommateur et il ne peut lui être demandé de communiquer à un consommateur ses informations personnelles plus de deux fois au cours d'une même période de douze mois.

Des sanctions dissuasives

Le CCPA prévoit que le consommateur dont les données personnelles font l'objet d'une violation (c'est-à-dire d'un accès non autorisé, vol, ou communication résultant d'un manquement de l'entreprise à son obligation de sécurité) peut obtenir des dommages et intérêts forfaitaires entre 100 et 750 US$ par incident ou le montant des dommages réellement encourus[10], qui doivent être calculés par les tribunaux en prenant en compte la nature et le sérieux de la violation, le nombre de manquements, la récidive, la durée du manquement, le caractère intentionnel de la violation ainsi que les actifs de l'entreprise. On mesure ici la différence avec le droit français, où seuls les dommages réellement subis et prouvés peuvent être indemnisés ce qui, pour un concept aussi abstrait que la violation du droit au respect des données personnelles, aboutit en pratique à une impossibilité d'indemnisation des personnes victimes de violations de leurs droits. Le montant des dommages forfaitaires, s'il semble limité, est en réalité fortement dissuasif si l'on se rappelle que l'Amérique est le pays des class actions. Une violation du CCPA qui toucherait un million de consommateurs californiens (sur quarante millions de californiens) peut ainsi résulter en des demandes de dommages et intérêts forfaitaires entre cent et sept cent cinquante millions de dollars américains, bien au-delà des vingt millions d'euros du RGPD. Les entreprises peuvent cependant échapper aux dommages forfaitaires si elles remédient à la violation dans un délai de 30 jours à compter de sa notification, auquel cas elles ne risqueront plus que d'être condamnées

pour les dommages réellement subis par les consommateurs (dans leur acceptation extensive en droit américain). On constate que seule est sanctionnée civilement la violation de la sécurité des données des consommateurs, mais non la violation de leurs droits d'information, d'accès ou d'effacement.

Le Procureur Général de l'État de Californie peut lui imposer des amendes civiles pour tout manquement au CCPA, si une entreprise ne remédie pas à un tel manquement dans un délai de trente (30) jours[11].Le montant maximal de ces amendes est de deux mille cinq cents dollars américains pour toute violation non intentionnelle et sept mille cinq cents dollars américains pour toute violation intentionnelle. Il convient de rappeler que ces montants s'entendent par violation, et donc que selon le nombre de consommateurs impliqués, ils peuvent rapidement devenir très importants. Le produit de ces amendes est destiné à alimenter un « *Customer Privacy Fund* » dédié à compenser tous coûts encourus pour les tribunaux et le Procureur Général de Californie dans la mise en œuvre du CCPA.

En conclusion, on ne peut que constater le caractère extrêmement limité du CCPA aussi bien dans son champ d'application que dans les droits qu'il confère aux consommateurs californiens et les obligations qu'il impose aux entreprises de cet État, par rapport au RGPD. Ce texte ne contient aucune obligation générale pour les responsables de traitement, ne connaît pas le concept de données sensibles (désormais catégories particulières de données), ne met en place aucun mécanisme de gouvernance (délégué à la protection des données, registre de traitement, études d'impact, privacy by design...) au sein des entreprises californiennes pour imposer le respect de la protection des données et n'institue aucune autorité indépendante spécialisée en charge d'assurer son respect. Une décision d'adéquation de la Commission européenne au bénéfice du seul État de Californie sur la base de ce texte, comme il en a été discuté récemment au sein de la commission Justice et Affaires intérieures du Parlement européen[12], semble donc exclue. Le droit américain de la protection des données personnelles n'est cependant pas uniquement constitué du CCPA. Il repose tout d'abord sur le concept de privacy, qui est une doctrine et un tort qui a été développé à partir de la fin du XIXème siècle comme un droit d'être laissé en paix (« *right to be left alone* »).

Ce concept de privacy est bien plus étendu que le droit à la protection des données personnelles, puisqu'il englobe également le droit à la protection de la vie privée, la diffamation, la procédure pénale concernant les fouilles de domiciles et même le droit à la contraception et à l'avortement mais également beaucoup plus difficile à saisir. Il se retrouve dans la jurisprudence des différentes juridictions et dans les nombreuses lois passées, aussi bien au niveau fédéral qu'à celui des États pour assurer la protection des droits des individus, soit dans certains secteurs tels que par exemple les assurances ou la santé, soit au vu de la situation particulièrement fragile de certains types d'individus, tels que les enfants. Il en résulte un véritable patchwork de lois sur ce sujet et des frais de compliance particulièrement élevés, même comparés à ceux générés par la mise en œuvre du RGPD. Ceci explique peut être le récent enthousiasme des entreprises américaines pour l'adoption d'une législation fédérale de la protection des données.

Marc LEMPÉRIÈRE
Avocat associé
ALMAIN

Notes

(1) California Civil Code, Section 1798.140(c)(1)

(2) Expertise décembre 2020, Interview « Le droit de la compliance pour réguler Internet ? »

(3) California Code of Regulations, Titre 18, Section 17014

(4) California Civil Code, Section 1798.140(o)

(5) CE, 10èm et 9ème ch réunies, 8 février 2017, n°393714

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

(7) California Civil Code, Section 1798.140(q)

(8) California Civil Code, Section 1798.130(5)

(9) California Civil Code, Section 1798.105(a)

(10) California Civil Code, Section 1798.150

(11) California Civil Code, Section 155

(12) Jennifer Barker, "EU Parliament debates : Could California be considered adequate on its own?", 9 jan 2020, https://iapp.org/news/a/eu-parliament-debates-could-california-be-considered-adequate-on-its-own/?mkt_tok=eyJpIjoiTnpFNU1qTm1aREEyWVRZMiIsInQiOiJFY3I2eEpiaElBbnpCM25ieW0yT09UblZFSkNpelJKYVFSQTJzdGc3NGVOdXBcL25EUngxa0F6NXJqNEpsdTJoR2s4Y3M3eFJ5Q1NIcnVSRzdmN213ZW42Tkc3bjhNd2FGTlZhZm9QRHExR1RjZHZ5NG5tTUpVTEN3R3JpT29wSjgifQ%3D%3D

(13) Samuel Lauren et Louis Brandeis, *"The right to privacy"*, 4 Harvard L.R. 193 (Dec. 15, 1890)

Vous avez envie de vous exprimer sur un sujet qui vous tient à cœur, de partager votre analyse avec la communauté des lecteurs d'Expertises, d'exposer un point de vue différent sur un article déjà publié, de lancer un débat sur un thème émergent, ou simplement de commenter l'actualité du droit du numérique ?

Contactez la rédactrice en chef d'Expertises Sylvie Rozenfeld sr@expertises.info