Le California Consumer Privacy Act (CCPA), à cheval entre deux cultures

S’inspirant de son cousin et homologue européen, le RGPD, le CCPA dénote toutefois sur certaines caractéristiques qui lui sont propres. Petit précis à l'usage des entreprises françaises implantées en Californie.

Temps de lecture : minute

20 décembre 2019

Approuvé en juin 2018 et effectif dès le 1er janvier 2020, le California Consumer Privacy Act va marquer de son empreinte les prochains mouvements réglementaires qui auront lieu aux Etats-Unis. Même si 11 États ont d’ores et déjà adopté des lois pour la protection des données, le CCPA marque d’une pierre blanche un momentum américain de grande envergure. Ce dernier va effectivement régir la protection des données des consommateurs californiens mais va notamment permettre la régulation des acteurs tech de la Silicon Valley.

Le CCPA, une loi emblématique qui cache la multitude

Cette réglementation s’inscrit dans la tendance générale à une plus grande responsabilité des entreprises vis-à-vis de la protection des données des consommateurs. Elle a pour but de permettre aux résidents californiens de disposer d’un meilleur contrôle de leurs données personnelles. Ainsi, l’Etat de Californie souhaite protéger au mieux les droits des consommateurs tout en accordant un meilleur respect de la vie

privée et en améliorant la transparence de l'utilisation des données personnelles.

Ce texte est également le fer de lance d'une vague législative qui englobe de nombreux états américains. En effet, depuis 2018, un certain nombre d'entre eux ont déjà adopté des textes relatifs à la protection des données.

Le dernier en date a pris effet le 1er octobre dans l'État du Nevada en votant la loi Senat Bill 220 (SB 220) début 2019. Il vient compléter une loi existante en apportant un volet concernant la protection des données personnelles des clients de sites services en ligne. Un premier pas important puisque inexistant jusqu'alors. Cependant, bien que dans la même veine que le CCPA, ce texte n'en a pas la même portée puisqu'il ne concerne que les données personnelles récupérées en ligne.

Ce fourmillement de textes de loi autour des mêmes problématiques de "privacy" présentent tous des spécificités qui leurs sont propres et rendent les choses parfois compliquées au niveau légal. De fait, une loi fédérale est désormais évoquée avec insistance. Cela offrirait aux acteurs du digital de disposer d'un environnement stable et légal permettant de créer des produits/solutions où acteurs économiques et utilisateurs pourront trouver un consensus quant à l'utilisation des données personnelles.

Le CCPA, " cousin " américain du RGPD ?

A ce jour, on ne compte plus les articles se demandant ce qui distingue le CCPA du RGPD et qualifiant même le CCPA de " version américaine du RGPD " ou encore de " RGPD light ".

Or si le CCPA est indéniablement inspiré par le RGPD, et accorde aux consommateurs certains droits sur la façon dont leurs informations

personnelles sont collectées et utilisées, les deux réglementations présentent des différences très claires tant au niveau de la nature des droits d’accès des données utilisateurs que de la mise en œuvre de ces derniers.

RGPD	CCPA
	
Protège le **citoyen** européen.	Protège le **consommateur** californien.
Protège les données permettant d'**identifier** directement ou indirectement **une personne physique.**	Les données personnelles permettent d'**identifier** directement ou indirectement **une personne physique ET / OU un ménage.**
Concerne **toutes les organisations** : entreprises privées, institutions publiques, associations à but non lucratif.	Ne s'applique qu'à des **entreprises privées** (« businesses ») atteignant une certaine taille ou un certain volume de données générées.
Il est interdit de rémunérer l'utilisateur contre la mise à disposition de ses données personnelles car les données personnelles ne sont pas une propriété mais un droit.	Rémunération possible des utilisateurs contre l'octroi de leurs données personnelles.
TRANSPARENCE Les utilisateurs doivent recevoir une information claire et complète sur leurs droits ainsi que sur les traitements appliqués à leurs données personnelles. Cette information doit porter sur 1/le type d'informations collectées, 2/la raison pour laquelle celles-ci sont collectées et 3/le type de traitements par lesquels ces informations passent.	
Mention obligatoire de la base légale applicable au traitement des données.	Une simple information sur le traitement des données.
Devoir d'informer les utilisateurs quant au transfert international de leurs données.	Rien n'est prévu sur cet aspect.
Concept de Délégué à la Protection des Données qui doit être nommé dans les entreprises.	Concept inexistant.
Aucune notion de durée mais devoir d'information. L'information doit être à jour au fur et à mesure.	Les entreprises doivent dévoiler l'ensemble des tiers à qui sont mis à disposition les données et les types de traitements effectués sur les 12 mois précédents.
CONSENTEMENT	
Aucune information personnelle ne peut être collectée tant que l'utilisateur n'a pas donné son accord de manière explicite : notion d'opt-in.	N'exige pas un consentement actif de l'utilisateur. Il est possible de collecter des données à partir du moment où un service / une application est utilisée.
L'opt-in englobe l'ensemble des problématiques liées aux données personnelles : collecte, traitement et partage.	Droit pour les utilisateurs de demander de faire cesser la vente ou la mise à disposition de leurs informations personnelles à des tiers.
	Mise à disposition obligatoire d'un mécanisme accessible et par conséquent visible par tous permettant aux consommateurs d'exercer leur droit d'opposition à la vente de leurs données.
	Tout tiers recevant des informations personnelles à travers leur vente ne peut revendre ces informations personnelles que si les consommateurs ont fourni un avis explicite et ont eu la possibilité de s'opposer à cette revente.
	Les utilisateurs ne peuvent / doivent pas subir de discrimination en cas d'exercice de leurs droits.
PRISE EN COMPTE DES MINEURS Les responsables légaux doivent donner leur consentement actif	
Consentement pour les enfants de moins de 16 ans (possibilité de descendre à 13 ans).	Consentement pour les enfants de moins de 13 ans.
	Pour les enfants de 13 à 15 ans, le CCPA demande à l'enfant un consentement actif (« opt-in ») au partage de ses données.
DROIT D'ACCÈS ET DROIT D'EFFACEMENT Disposer d'un contrôle complet sur les données personnelles détenues par un acteur	
Sans limite dans le temps.	Droit d'accès applicable aux informations personnelles recueillies dans les 12 mois précédant la demande.
Possibilité de refuser de donner suite à une demande d'accès si celle-ci est infondée, excessive ou trop répétitive.	Aucune obligation de donner l'accès aux informations personnelles d'un utilisateur plus de deux fois en 12 mois.
Répondre aux demandes d'accès (ou d'effacement) sous un mois à partir de la réception de la demande.	Répondre aux demandes d'accès (ou d'effacement) sous 45 jours à partir de la réception de la demande.
Délai pouvant être étendu à deux mois supplémentaires.	Délai pouvant être prolongé de 45 jours supplémentaires lorsque cela est nécessaire.
Notification au demandeur sous un mois à compter de la réception de sa demande.	Le consommateur doit en être informé dans les 45 premiers jours.
Demande soumise par voie écrite, orale ou encore numérique.	Obligation de mettre à disposition un minimum de deux méthodes permettant de formuler une demande. Un numéro de téléphone est obligatoire.
L'effacement concerne l'ensemble des données associées à un utilisateur et ce quel que soit leur provenance.	L'effacement implique la suppression de toutes les données collectées directement depuis l'utilisateur. Implicitement cela signifie que les données récupérées via un tiers ne sont pas concernées.
PORTABILITE	
Les personnes concernées ont le droit de demander à recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement	La fourniture des informations à l'utilisateur se fait par voie électronique.
Cette transmission doit être faite dans un format structuré, couramment utilisé et lisible par machine.	Les informations doivent être envoyées dans un format portable et facilement utilisable, permettant leur transmission à des tiers.
RISQUES Système d'amendes Une notification de non-respect peut être rendue publique	
Sanction de 4% du chiffre d'affaires annuel dans la limite maximum de 20 millions d'Euros.	Pas de limite à l'amende. Prix forfaitaire allant de 2500$ à 7500$ lorsque l'intentionnalité est reconnue pour **chaque** violation constatée
	Possibilité d'actionner une procédure de recours collectif (« class action »).

À la lecture du tableau, on découvre de nombreuses similarités entre RGPD et CCPA, malheureusement mêlées à de nombreuses disparités. Si une société européenne implantée en Californie se pense protégée du fait de sa conformité au règlement européen, il n'en est rien. La société devra se conformer aux lois qui régissent tout acte commercial sur le territoire californien pour satisfaire aux obligations du CCPA. Il sera donc nécessaire de la part de l'entreprise de réaliser tout un travail d'adaptation de l'ensemble de sa documentation, de ses procédures internes ou encore des mentions d'information (citoyen ou consommateur) des personnes concernées.

Malgré des schémas légaux différents, l'Europe comme de nombreux États américains avancent dans la même direction : la protection des données personnelles. Avec l'idée de l'arrivée prochaine d'une loi fédérale américaine, un consensus commun pourrait être trouvé entre les États-Unis et l'Europe. Il reste donc à attendre la décision du Congrès américain exhorté par les dirigeants des 50 plus grandes entreprises américaines, de légiférer sur une loi fédérale à propos de la protection des données des consommateurs.

Jean-Noël Barneron est directeur de l'innovation chez Herow

Article écrit par Jean-Noël Barneron