

La « Proposition 24 » en Californie, un faux renforcement du California Consumer Privacy Act

Description

Le 3 novembre 2020 en Californie, parmi les treize référendums soumis au vote des électeurs sur des questions diverses, deux intéressaient l'économie numérique : la « Proposition 22 » relative au statut de certains travailleurs de la *gig economy* et la « Proposition 24 » qui vient amender le California Consumer Privacy Act (CCPA).

L'organisation de ces référendums californiens s'appuie sur l'inscription au vote d'une mesure proposée à la suite d'une pétition à l'initiative de citoyens ou d'entreprises, ce qui est le cas pour la Proposition 22. Sans chercher à s'aligner sur le texte européen, la Proposition 24 avait pour objectif de corriger certaines insuffisances figurant dans le CCPA. Elle a finalement été adoptée à 56,23 % des suffrages. Certains analystes tendent néanmoins à dénoncer les effets pervers que pourraient engendrer ces modifications. En filigrane, ce vote ravive le débat relatif à la patrimonialité et la commercialisation des données personnelles ([voir La rem n°46-47, p.90](#)), qui n'est pas non plus éteint du côté de l'Union européenne.

Le CCPA, un cadre protecteur des données personnelles encore perfectible

Pour mémoire, le CCPA a été adopté en juin 2018 et est entré en vigueur le 1^{er} janvier 2020. Si l'on a pu opportunément le qualifier de « RGPD américain¹ », la comparaison avec le texte de l'Union européenne doit malgré tout être relativisée².

Le CCPA reste en effet empreint d'une logique consumériste ; les données personnelles des utilisateurs de services numériques y sont appréhendées dans leur dimension principalement économique et dans le seul cadre des relations avec les entreprises qui les exploitent³. Son champ d'application présente malgré tout l'avantage d'une certaine transversalité, alors que le droit des États-Unis était jusque-là caractérisé par une régulation sectorielle, les principales lois étant davantage pensées en fonction des types de données personnelles et des usages afférents. Sur le fond, le CCPA a octroyé de nouveaux droits essentiels aux consommateurs⁴.

Le plus important d'entre eux est le droit de s'opposer à la vente de données avec des entreprises tierces. À la différence du RGPD, le CCPA ne comporte pas de liste des bases légales de traitement des données personnelles ni ne prévoit d'obligation de recueillir le consentement des personnes préalablement à la collecte et/ou la vente des données (excepté lorsque ces actes portent sur les données de mineurs de moins de 16 ans). Seul un droit d'opposition, à exercice périodique (tous les douze mois), peut être exercé par les consommateurs qui souhaitent exprimer leur refus. Par ailleurs, si le texte interdit aux responsables de

traitement toute discrimination basée sur les choix des consommateurs, il les autorise malgré tout à proposer des avantages financiers, tels que des paiements, en compensation de la collecte de leurs données. Cette possibilité traduit explicitement la logique économique et patrimoniale qui anime le CCPA. Des droits d'accès et d'effacement ont également été conférés aux consommateurs. Ceux-ci bénéficient également d'une obligation d'information préalable à la charge des responsables de traitements.

On rappellera que le CCPA ne concerne qu'un nombre limité d'entreprises, en fonction de trois seuils de *minimis* alternatifs : générer plus de 50 millions de dollars de revenus bruts annuels ; traiter les données d'au moins 50 000 consommateurs, ménages ou objets connectés ; tirer 50 % de ses revenus annuels de la vente de données personnelles.

Aidé par le contexte états-unien, et notamment les suites du scandale Cambridge Analytica ([voir La rem n°48, p.90](#)), le CCPA inspire des initiatives dans d'autres États fédérés et nourrit les réflexions relatives à une législation fédérale⁵. Toutefois, si un progrès certain peut être relevé, force est de constater que ses standards restent pour l'instant inférieurs à ceux du RGPD.

Les principales mesures portées par la Proposition 24

La Proposition 24, également appelée *California Privacy Rights and Enforcement Act*, entend à la fois renforcer certains droits conférés aux consommateurs et créer une agence californienne de protection des données.

Les dispositions qui concernent les droits des consommateurs sont assez diverses. Tout d'abord, le droit d'opposition à la vente des données est étendu au simple « partage » de celles-ci avec des entreprises tierces. Si la définition de la vente était assez large dans la version initiale du CCPA et incluait notamment tout acte bénéficiant d'une contrepartie monétaire telle que la location, cet ajout étend la portée du droit d'opposition à des actes ne présentant pas nécessairement une telle compensation. Ainsi en est-il des croisements de données à des fins de publicité ciblée et comportementale. De la même manière, la portée du droit à l'information des consommateurs est étendue à ces types de traitement.

La Proposition 24 définit également de façon autonome les données dites « sensibles », en des termes assez proches de ceux du RGPD, alors que celles-ci n'étaient qu'implicitement visées auparavant. Un droit à l'information spécifique à ces données est créé dans la continuité de cette définition, les consommateurs devant être au courant des finalités pour lesquelles ces informations sont collectées et stockées ainsi que de leur durée de conservation. De même, un droit d'opposition séparé leur permettra d'interdire tout acte de vente et/ou de partage de ces données avec des entreprises tierces aux responsables de traitement. Le droit d'accès se voit prolongé par un droit de rectification des données qui s'avèrent inexacts ou obsolètes. En cela, les défenseurs du texte insistent sur sa capacité à rétablir un certain contrôle des données par les consommateurs.

La Proposition 24 vient également préciser les obligations des responsables de traitement, ainsi que le

régime des sanctions qui peuvent leur être infligées en cas de manquement. Le texte dispose notamment que les entreprises ne pourront procéder qu'à des collectes de données nécessaires et proportionnées aux objectifs indiqués, ce qui rappelle le principe de minimisation des données. Quant aux sanctions, le CCPA laissait initialement aux entreprises un délai de 30 jours pour corriger toute faille de sécurité ou remédier à un accès frauduleux, faute de quoi elles encouraient des sanctions allant de 2 500 à 7 500 euros par manquement. Les nouvelles dispositions adoptées le 3 novembre 2020 suppriment désormais ce délai.

Enfin, et c'est là un point remarquable de la proposition, une nouvelle autorité de régulation est créée au sein de l'État de Californie pour veiller au respect des dispositions du CCPA modifié. Dénommée California Privacy Protection Agency et bénéficiant d'un budget annuel de 10 millions de dollars, cette autorité est dotée de pouvoirs d'investigation, de recommandation et de sanction à l'égard des responsables de traitement. Son conseil de direction sera composé de cinq membres nommés par le gouverneur et le procureur général de l'État, ainsi que par les deux chambres du Parlement californien.

Critiques américaines

Malgré les intentions affichées, le texte de la Proposition 24 a été fermement critiqué par plusieurs organisations américaines, telles que l'American Civil Liberties Union⁶ ou l'Electronic Frontier Foundation⁷. Celles-ci reprochent au texte de ne pas aller assez loin dans la logique de protection de la vie privée des consommateurs et de d'induire des risques de discrimination.

De façon générale, les ajouts apportés au CCPA par la proposition se révèlent essentiellement « cosmétiques » et ne changent pas radicalement son esprit, qui reste basé sur la patrimonialité et la commercialisation des données. Une réelle avancée en la matière aurait été d'instaurer un véritable principe de respect de la vie privée par défaut, fondé sur le consentement des consommateurs, plutôt que sur une faculté d'opposition qui paraît illusoire. À ce titre, les critiques insistent sur l'effet pratique des nouvelles dispositions. S'il paraît effectivement salubre de délivrer une information préalable aux consommateurs, celle-ci peut s'avérer peu lisible et dissuasive au vu des nombreuses exigences du texte. Par ailleurs, le CCPA n'interdit pas les réglages par défaut basés sur l'*opt-out* et les cases pré-cochées. Il y a donc fort à parier que les consommateurs soient peu enclins à exercer leurs droits d'opposition dans de telles conditions, comme cela a souvent été constaté. On relèvera malgré tout que la Proposition 24 prohibe le recours aux *dark patterns* (interfaces trompeuses) et précise qu'aucun consentement valable ne saurait être obtenu grâce à l'emploi d'un tel procédé. Elle encadre également les conditions de présentation des conditions d'utilisation en exigeant une certaine lisibilité ainsi qu'une ergonomie facilitant l'exercice des droits.

D'autres reproches portent sur l'insuffisance de certaines définitions. Celle des données « sensibles » visées par le texte serait en effet incomplète en ce qu'elle néglige notamment les données relatives au statut d'immigration. Il en est de même pour les dispositions relatives à la proportionnalité des collectes de données, qui restent déterminées par le(s) objectif(s) annoncé(s) par les responsables de traitement, ou celles qui portent sur le droit d'opposition au partage de données, et qui ne visent que la publicité

comportementale alors qu'il existe d'autres pratiques de croisement des données. Enfin, les moyens alloués à l'autorité de régulation paraissent largement insuffisants au regard du nombre de personnes concernées et du nombre potentiels de manquements dont les responsables de traitement peuvent se rendre coupables.

Surtout, la Proposition 24 a entériné dans le CCPA des exceptions qui risquent fort bien de renforcer la marchandisation des données. Outre le fait que les entreprises peuvent toujours proposer des avantages financiers aux consommateurs, le texte comporte une nouvelle exception à l'interdiction des pratiques discriminatoires, créée au profit des programmes de fidélité. Les responsables de traitement pourront donc proposer leurs services à des tarifs différents selon les choix de leurs utilisateurs. Les offres les moins chères ou gratuites seront naturellement compensées par des collectes plus intrusives et massives. Loin du *privacy by default*, c'est donc la logique du *pay for privacy* qui est consacrée implicitement par le nouveau texte.

Un important différentiel dans le droit au respect de la vie privée, qui est pourtant garanti par la Constitution californienne, pourrait donc se dessiner en application du nouveau CCPA, les populations les plus défavorisées ayant à en pâtir les premières.

Perspectives européennes

Le débat sur la patrimonialité et la marchandisation des données personnelles paraissait plus lointain en Union européenne depuis l'entrée en vigueur du RGPD. Il a pourtant resurgi à l'occasion de l'adoption de la directive du 20 mai 2019, relative aux contrats de fourniture de contenus numériques et de services numériques⁸.

Si celle-ci porte essentiellement sur des questions de responsabilité et de conformité des contenus et services délivrés à l'utilisateur, la détermination de son champ d'application, à l'article 3, n'a pas manqué d'attirer l'attention. Les contrats auxquels elle est censée s'appliquer sont en effet définis comme ceux pour lesquels le consommateur « *s'acquitte ou s'engage à s'acquitter d'un prix* » ou « *fournit ou s'engage à fournir des données à caractère personnel* » au professionnel en contrepartie des contenus ou services demandés. Autrement dit, les données personnelles peuvent bien être substituées au prix que pourrait payer l'utilisateur, la valeur provenant naturellement des actes de traitement auxquels pourront se prêter ces informations. Bien que cette option ait été condamnée par le Contrôleur européen de la protection des données⁹, elle revient à admettre que l'on puisse « payer » avec ses données personnelles. On rappellera que les tribunaux français avaient déjà implicitement admis ce raisonnement pour requalifier les conditions générales d'utilisation de plusieurs réseaux sociaux « gratuits » ([voir La rem n°48, p.26](#), et [n°50-51, p.16](#)), de même que l'Autorité de la concurrence italienne ([voir La rem n°49, p.19](#)).

On a dès lors pu s'interroger sur la base du traitement de données autorisé par la directive précitée au sens de l'article 6 du RGPD¹⁰. Celle-ci excluant explicitement les données nécessaires à l'exécution du contrat et les conditions exigées pour recueillir un consentement éclairé et « libre » n'étant pas réunies, seul l'intérêt légitime du responsable de traitement paraît justifier une telle opération sur le plan juridique. Le RGPD devra certes primer en cas de contradiction entre les deux textes, et les traitements afférents devront dans

tous les cas en respecter les dispositions. Toutefois, l'alternative ouverte par la directive renvoie en pratique à celle que permet le CCPA, tel que modifié par la Proposition 24. En effet, elle laisse la possibilité aux entreprises de différencier leurs tarifs en fonction des choix des consommateurs quant à leurs données personnelles. De la même manière qu'en Californie, l'adhésion à un programme de fidélité gratuit pourra justifier commercialement l'option proposée par le responsable de traitement. Et il y a fort à parier que les consommateurs soient davantage tentés (ou forcés selon leur situation financière) d'accepter une offre gratuite pour bénéficier de contenus ou services numériques.

Malgré les apparences, une certaine convergence de logiques se fait jour de part et d'autre de l'Atlantique quant à la marchandisation des données. Alors que le droit californien tente d'inspirer les autres États fédérés en bridant la logique consumériste qui avait droit de cité jusqu'alors, le droit de l'Union européenne semble contraint d'admettre des interstices de marchandisation des données.

Sources :

1. S. Le Strujon, « Le *California Consumer Privacy Act* : premier pas vers un RGPD américain ? », *Rev. UE*, 2020, p.41 ; voir également : S.L. Pardau, « The California Consumer Privacy Act : Towards a European-Style Privacy Regime in the United States », *J. Tech. L. & Pol'y*, Vol. 23, Issue 1 (2018), p.68-114.
2. A. Debet, « Quelle législation pour la protection des données aux États-Unis (1^{re} partie) ? », *CCE*, mai 2019, p.34-36.
3. C. Castets-Renard, « *Schrems II* et invalidation du *Privacy Shield*, un goût de « déjà vu »... », *D.*, 2020, p.2432.
4. P. Kamina, « Un an de droit anglo-américain », *CCE*, février 2020, p.21.
5. A. Debet, « Quelle législation pour la protection des données aux États-Unis (2^e partie) ? », *CCE*, juin 2019, p. 31-35.
6. J. Snow et S. Conley, « Californians Should Vote No on Prop 24 », *ACLU Northern California*, October 16, 2020.
7. L. Tien, A. Schwartz et H. Tsukayama, « Why EFF Doesn't Support California Proposition 24 », *Electronic Frontier Foundation*, July 19, 2020.
8. Directive n°2019/770 du Parlement et du Conseil du 20 mai 2019, relative à certains aspects concernant les contrats de fourniture de contenus numériques et de services numériques.
9. Avis n°4/2017 sur la proposition de directive concernant certains aspects des contrats de fourniture de contenu numérique, 14 mars 2017, 32 p.
10. T. Leonard, « Peut-on payer avec ses données personnelles ? », *Droit & Technologies*, 19 septembre 2019.

Categorie

1. Ailleurs

date créée

17 juin 2021

Auteur

philippemouron