DIGITAL MEDIA ASSOCIATION

ÉDITION
JANVIER 2021

LA FIN DES ÉCHANGES DE DONNÉES PERSONNELLES ENTRE L'EUROPE ET LES ÉTATS-UNIS?

Livre blanc sur les conséquences de certaines décisions juridiques récentes

ABORDONS LE PROBLÈME SOUS LE BON ANGLE

Depuis quelques années, la publicité en ligne n'a pas bonne presse. Non seulement son efficacité a été mise en doute (à tort), mais en outre les responsables politiques ont multiplié les interventions dans ce domaine. Si ces derniers ont incontestablement agi avec la meilleure intention du monde, il n'en demeure pas moins qu'ils ont créé un climat incertain et flou autour de la voie à suivre pour concilier efficacité et respect de la législation.

Ainsi, le 25 mai 2018 restera à jamais gravé dans nos mémoires comme le jour où le RGPD est devenu réalité. Les années qui ont précédé l'entrée en vigueur de ce règlement européen ont vu une situation sans précédent : les entreprises ont tenté à la hâte de saisir les tenants et aboutissants de cette nouvelle législation, ainsi que les conséquences en cas de non-respect.

Aujourd'hui, deux ans après son entrée en vigueur, nous constatons que le «consentement» n'a pas donné lieu aux situations dramatiques redoutées. Les consommateurs acceptent facilement de donner l'autorisation de traiter leurs données.

Toutefois, la publicité en ligne n'a pas encore quitté la zone de danger, car le taux de recours à un *adblocker* reste élevé. Un autre obstacle a par ailleurs fait son apparition, quoique de façon moins sensationnelle : un arrêt de la Cour européenne de justice met désormais des bâtons dans les roues en matière de transfert des données personnelles de l'Europe vers les États-Unis.

Et ce, alors que pratiquement tous les outils technologiques sont aux mains des Américains. De Google Analytics aux pixels de Facebook Connect, en passant par les adservers (qui assurent la diffusion des publicités en ligne et leur suivi) ou les DMP (plateformes où sont notamment stockées les données des campagnes publicitaires).

On peut donc se demander si nous envisageons le problème sous le bon angle. Savons-nous vraiment d'où viennent les défis que notre secteur doit relever? Notre rôle en tant que fédération est de démêler cet écheveau et d'apporter des solutions. Telle est également l'ambition du présent livre blanc.

Nous vous souhaitons une lecture inspirante!

Philippe Degueldre
Président de la DMA
Business Intelligence Director chez Pebble

L'ÉCHANGE DE DONNÉES À CARACTÈRE PERSONNEL ENTRE L'UE ET LES ÉTATS-UNIS DANS L'IMPASSE

Il n'y a probablement aucune entreprise en Europe qui puisse se passer d'outils tels qu'un CRM, Google Analytics ou Facebook Connect. Mais voilà que leur utilisation semble tout à coup illégale. Nous faisons le point sur la situation.

Commençons par un bref retour en arrière. Depuis 2018, le RGPD oblige les entreprises européennes à manipuler avec beaucoup plus de précautions les données personnelles de leurs clients, prospects et visiteurs de sites web. En clair, elles doivent requérir l'autorisation des consommateurs en vue de conserver leurs données, mais également veiller à ce que celles-ci ne quittent pas l'Europe à n'importe quelles conditions. En effet, certains pays ont adopté une législation moins stricte, laissant la porte ouverte à une utilisation abusive des données personnelles.

Or, à l'heure actuelle, il s'avère tout à fait impossible de conserver des données uniquement en Belgique ou en Europe. Presque toutes les entreprises travaillent avec des logiciels et des outils qui proviennent de pays très différents. Le recours à ces outils nécessite souvent l'échange de données (notamment à caractère personnel). Pensons notamment aux systèmes CRM prévoyant l'hébergement de toutes les données des clients dans le cloud. Ou encore à Google Analytics, Microsoft Azure et AWS, des services du cloud utilisés par presque toutes les entreprises. Dans le domaine de la publicité en ligne également, de nombreux outils utilisent couramment des données personnelles : DMP, DSP, ad-server, Facebook Connect, ...

LA SOLUTION ÉTAIT TEMPORAIRE...

Pour pouvoir continuer à utiliser ce type d'outils, l'Europe a prévu des exceptions à la règle. Lorsque les pays ont une législation au moins aussi stricte qu'en Europe (comme la Suisse, Israël et le Japon), la «libre circulation des données» reste autorisée. Pour les États-Unis (d'où proviennent la plupart des outils), c'est plus délicat, car ce pays a une tout autre vision en matière de confidentialité. En effet, les autorités américaines ont dans certains cas le droit de consulter les données personnelles stockées par les entreprises...

Pour les États-Unis, il ne s'agissait donc pas d'une règle générale, mais d'une exception accordée au cas par cas aux entreprises, moyennant le respect d'un certain nombre de conditions de sécurité, énumérées dans le Privacy Shield, un accord conclu entre l'UE et les États-Unis. La plupart des prestataires de services américains qui proposent également des services au sein de l'UE ont été certifiés et ont ainsi pu importer des données personnelles européennes sans condition supplémentaire.

Et même pour les entreprises non conformes ou basées en dehors des États-Unis, certaines possibilités existaient. La solution la plus courante consistait en des clauses contractuelles types, autrement dit des modèles de contrats de transfert de données personnelles adoptés par la Commission européenne.

Mais ces diverses mesures ont été remises en cause à l'été 2020. La Cour européenne de justice a alors décrété que le transfert de données personnelles de l'Europe vers les États-Unis n'était plus possible sans de sérieuses garanties. L'arrêt dit «Schrems II» va jusqu'à établir que ce transfert est illégal dans de nombreux cas. Le Privacy Shield subit ainsi le même sort que son prédécesseur, le Safe Harbor. Et ce, pour des raisons similaires. Retour à la case départ, donc.

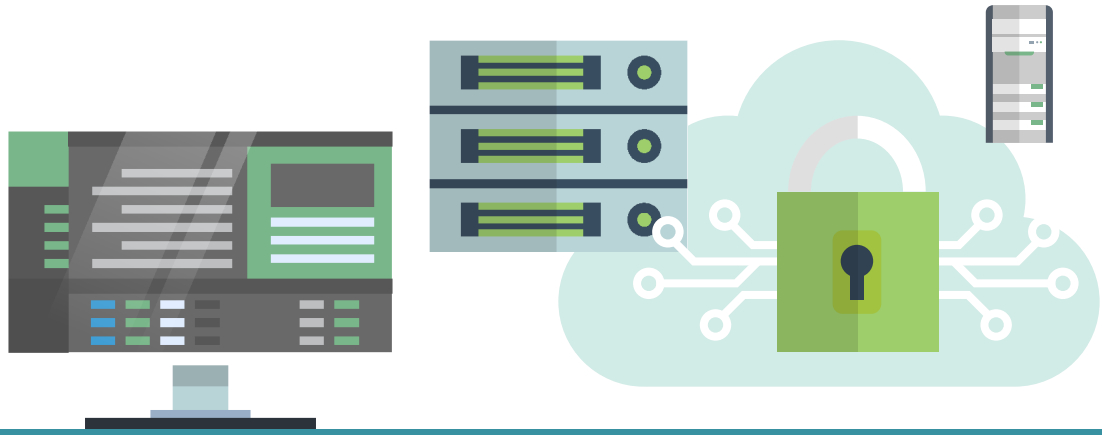
L'argumentation de la Cour? La collecte de données par les autorités américaines ne se limite pas au strict nécessaire (selon la logique européenne du RGPD) et, de plus, les Européens concernés ne disposent pas de recours juridiques suffisants pour s'y opposer (devant un tribunal américain).

… ET LE PROBLÈME RESSURGIT

La décision a eu l'effet d'un coup de tonnerre. Comme déjà signalé plus haut, interdire l'usage des outils couramment utilisés, surtout pour la publicité en ligne, revient à faire un bond de vingt ans en arrière …

Voilà pour les nouvelles, et elles ne sont donc pas réjouissantes. Début novembre, le Conseil européen de la protection des données a publié des lignes directrices très attendues qui fournissent une feuille de route claire, mais qui, dans la pratique, nécessite souvent des analyses complexes et des investissements importants.

Les entreprises en Europe se retrouvent par conséquent dans une zone grise : leur approche actuelle est peut-être illégale et les changements à apporter sont plutôt flous ou impossibles à mettre en œuvre à court terme. La modification du contrat – liant l'entreprise à son fournisseur américain – semble être la solution la plus évidente, mais les entreprises américaines ne peuvent bien sûr pas garantir que les autorités de ce pays ne demanderont pas à consulter les données. Bref, l'impasse est totale.



CINQ FAÇONS DE FAIRE FACE À CETTE SITUATION

Heureusement, nous disposons de plusieurs leviers pour réagir à cette décision car il faut absolument mettre un terme à ce flou juridique en prenant les bonnes mesures. Voici nos cinq recommandations.

1

CARTOGRAPHIEZ LA SITUATION DE VOTRE ENTREPRISE

Il s'agit de la première étape logique. Vérifiez les contrats conclus qui peuvent être impactés par cet arrêt. Avez-vous des contrats avec des prestataires de services américains ? Ou bien des contrats en vertu desquels un prestataire de services américain intervient comme sous-traitant ? Pensez par exemple à votre agence média qui utilise les services de Facebook ou de Google, ou à une agence de publicité travaillant avec une solution dans le cloud.

Il est important de vérifier en détail quelles données à caractère personnel sont traitées dans le cadre d'un tel contrat, selon quel mode opératoire, les conditions de transfert aux États-Unis… Bref : faites l'inventaire de votre situation personnelle.

Un détail non négligeable : même si les données sont stockées sur des serveurs européens, il peut également être question de transfert de données si leur consultation est possible à partir d'un pays non européen (par exemple pour des raisons techniques).

2

VÉRIFIEZ LES ACTIONS ENTREPRISES PAR VOS PRESTATAIRES DE SERVICES

Bien entendu, les prestataires de services américains sont également conscients de cette situation juridique incertaine. Ils peuvent prendre un certain nombre de mesures proactives pour réglementer le transfert de données à caractère personnel. Par exemple, ils peuvent traiter les données personnelles uniquement en Europe, en évitant que celles-ci soient transférées aux États-Unis.

N'attendez donc pas pour prendre contact avec vos partenaires. Vérifiez s'ils passent à l'action et si vous pouvez adapter les contrats conclus avec eux.

3

SUSPENDEZ LES CONTRATS SI NÉCESSAIRE

Si vous avez certains contrats qui ne sont plus légaux ou si votre prestataire de services américain ne planche pas sur des solutions à court terme, suspendez le contrat en question et cessez temporairement la coopération. Au besoin (par exemple si la situation ne change pas rapidement), vous devrez également faire annuler le contrat en vertu de la décision juridique susmentionnée.

4

CHERCHEZ DES ALTERNATIVES EUROPÉENNES OU REPORTEZ LA CONCLUSION DE NOUVEAUX CONTRATS

Il va sans dire que ce n'est pas le moment idéal pour conclure un nouveau contrat avec un prestataire de services américain. La situation juridique est trop incertaine à l'heure actuelle.

Si, dans le cadre d'un tel contrat, le transfert de données vers les États-Unis s'avère difficile voire impossible à exclure, nous vous recommandons de reporter sa signature jusqu'à ce que la situation ait été clarifiée.

Une autre solution consiste bien sûr à vous tourner vers un partenaire européen. Vous bénéficierez ainsi d'une plus grande sécurité juridique.

5

ADAPTEZ VOUS-MÊME VOTRE CONTRAT

Heureusement, vous pouvez aussi prendre les choses en main. Les juristes travaillent d'arrache-pied pour adapter les contrats afin de supprimer tout risque. Pour ce faire, ils utilisent les clauses contractuelles types de la Commission européenne, complétées par un certain nombre de mesures techniques, organisationnelles et juridiques, conformément aux directives récentes du Conseil européen de la protection des données.

Vous l'avez compris : nul doute que la situation va encore évoluer dans les mois à venir. C'est pourquoi nous vous conseillons de consulter un juriste pour savoir où en seront les choses à ce moment-là.

DIGITAL MEDIA ASSOCIATION

La DMA s'est assigné la mission de suivre de près l'actualité du marché et d'en clarifier les enjeux. Nous espérons que ce livre blanc y aura contribué. Nous continuerons à suivre la situation de très près.

Ce livre blanc a été réalisé par la DMA (Digital Media Association), fédération qui regroupe les éditeurs et les régies belges actifs dans la publicité en ligne.

www.dma-belgium.be

DMA asbl
Schaliënhoevedreef 20C
2800 Malines