CONFRONTATIONS EUROPE

# Comment articuler le DMA et la régulation européenne en matière de protection des données personnelles ?

*Entretien avec Yann Padova*

## PRÉSENTATION

Dans un entretien accordé à Confrontations Europe, Yann Padova, associé du cabinet Baker McKenzie et ancien Secrétaire général de la CNIL, revient sur les enjeux structurants du DMA et de son articulation avec le RGPD. Propos recueillis par Thomas Dorget, Délégué général de Confrontations Europe.

**Thomas Dorget: Le projet de Digital Markets act (DMA) structure à la fois le mandat de la Commission européenne depuis sa première publication en décembre 2020, mais aussi le mandat français de Présidence du Conseil de l'UE comme un des objectifs à achever d'ici juin 2022. L'objectif du DMA est de réguler spécialement les plateformes systémiques venant de pays tiers, des Etats-Unis pour l'essentiel. Quel regard portez-vous sur cette proposition de la Commission, dans cette période de négociation entre les colégislateurs ?**

**Yann Padova:** Le DMA s'adresse aux plateformes dominantes et il est vrai que beaucoup d'entre elles aujourd'hui sont d'origine américaine. Mais en réalité, le DMA régule toutes les plateformes, notamment celles dites de « service essentiel » et parmi elles, celles que le texte qualifie de « contrôleur d'accès ». Cela s'adresse donc également à des entreprises européennes puisque le texte comptabilise une dizaine de milliers de plateformes au total, tout en identifiant qu'un nombre limité qui « dominent le marché » et qui sont parfois à l'origine de pratiques déloyales. Mon expertise portant sur le droit des données personnelles, mon objectif est de comprendre l'interaction entre cette régulation de marché et les obligations contenues dans le RGDP.

Cette interpénétration est importante car le DMA constate que l'instrument de pouvoir des plateformes essentielles qui dominent le marché vient de la collecte massive de données personnelles qui leur permet d'étendre leurs activités à une multitude de secteurs.

Le texte a pour objectif de réformer un point fondamental de la régulation de marché en s'appuyant sur le constat que le droit de la concurrence, dans son état actuel, n'est pas efficient car il intervient majoritairement ex-post. Or, l'essentiel de ces plateformes selon la Commission n'ont pas des pratiques qualifiables d'abus de positions dominantes. La conséquence de ce constat est la suivante : plutôt que de se concentrer sur l'ex-post où les autorités ne sont pas certains de pouvoir sanctionner les abus de position dominante et les comportements déloyaux ou illégaux, la Commission souhaite imposer aux plateformes des obligations ex-ante, en les contraignant à partager l'un de leurs instruments de pouvoir de marché : la donnée personnelle.

C'est pour cette raison que l'articulation entre DMA et RGPD est essentielle : garantir la circulation et le partage des données personnelles collectées par les plateformes contribuera, selon la Commission, à rétablir la contestabilité du marché. Pour assurer le succès de cette démarche, la Commission doit s'assurer que cette logique de concurrence s'articule correctement avec les autres réglementations s'adressant au traitement de données personnelles. C'est précisément à ce sujet que j'ai un certain nombre de craintes, car je trouve que cette articulation n'est pas parfaitement aboutie et peut ainsi conduire à l'émergence d'injonctions contradictoires pour les entreprises concernées.

**TD: A ce sujet vous avez publié le 20 décembre 2021, une tribune dans les Echos dans laquelle vous détaillez plus précisément l'articulation entre RGPD et DMA et pointez certaines incohérences dans cette articulation entre les deux textes. Vous mentionnez notamment la question des destinataires inconnus, l'usage compatible des données collectées, et la sécurité des données collectées. Pourriez-vous revenir sur ces trois points clefs ?**

**YP:** J'ai pointé un problème de transparence des finalités d'une part et un problème concernant les obligations de sécurité d'autre part. Le DMA prévoit que les gatekeepers (les « controleurs d'accès ») doivent mettre à disposition en temps réel, des données agrégées et non agrégées auprès des entreprises utilisatrices, afin que ces dernières puissent utiliser ces données pour le développement de leurs activités. Du point de vue du RGPD, cette injonction pose un problème dès lors que des données personnelles sont concernées. Pour rappel, une donnée personnelle est une donnée qui, indirectement ou directement, permet d'identifier une personne (adresse IP, nom, numéro de téléphone…). Le DMA en l'état demande donc aux gatekeepers de transmettre en temps réel, des données à caractère personnel à des destinataires pour un usage non réglementé. Or, le droit des données impose que la collecte soit réalisée avec une finalité précise et déterminée, afin d'éviter un usage abusif de cette collecte. De plus, le RGPD interdit les usages ultérieurs de données « incompatibles » avec les finalités initiales ayant présidé à leur collecte.

Nous sommes ici au cœur du problème : la plateforme a collecté la donnée pour un certain usage et va la transmettre à une autre entreprise pour un usage dont elle ignore la finalité. Le destinataire lui, au regard du RGPD, va devoir s'assurer que la finalité qu'il en fait est compatible avec la finalité initiale de la collecte. Cet examen de la compatibilité des finalités en droit est assez délicat, il y a des critères dans le RGPD et des recommandations des autorités de protection des données mais ce contrôle impliquera des surcoûts de ressources juridiques dont la plupart des PME ne disposent pas. Par ailleurs, le non-respect du principe de finalité fait encourir des sanctions administratives très élevées (4% du chiffre d'affaires) et constitue aussi un délit pénal en droit français.

Le second point soulevé dans mon précédent article concerne le principe de sécurité des données. En effet, le RGPD oblige l'entreprise qui traite des données personnelles, à en assurer la protection, la sécurité tout au long du « cycle de vie » des données. Ce n'est pas une simple obligation de moyens qui concernerait des aspects de pure technique, il s'agit d'un principe fondamental, au même niveau que celui de transparence ou de finalité que nous venons d'évoquer. Une fois encore, le gatekeeper a l'obligation de partager en temps réel des données, dont certaines potentiellement à caractère personnel, mais il ne connait pas le niveau de sécurité de l'entreprise qui les reçoit. Cette situation soulève de nouvelles questions : va-t-il falloir privilégier le partage des données, au risque de leur sécurité ? Là encore, en cas de violation de ce principe de sécurité, l'entreprise encoure une sanction élevée du point de vue du RGPD (4% du chiffre d'affaires), et également un risque pénal en droit français. Mais laquelle sera responsable ? Celle ayant partagé les données ou celle les ayant reçues ?

**TD: Les débats autour du DMA se focalisent également sur un l'enjeu fondamental de la gouvernance : quel régulateur pour le marché du numérique en Europe ?**

**YP:** C'est une question essentielle ! En matière de données personnelles il y a également des discussions en ce moment sur l'architecture du RGPD et sa gouvernance qui n'est pas pleinement satisfaisante : faut-il recentraliser la supervision vers la Commission ou garder une logique décentralisée avec des autorités nationales qui coopèrent et la Commission en appui ? Traditionnellement, la Commission est très puissante en matière de concurrence mais dispose-t-elle

en l'espèce de la bande passante nécessaire pour couvrir l'intégralité des sujets abordés par le DMA ? C'est une vraie question politique ! Est-ce que la Commission en est capable avec toute l'expertise technologique que cela nécessite ? Quel sera le rôle des autorités nationales de protection des données ? La question de la gouvernance permet essentiellement de s'assurer qu'au-delà de la cathédrale juridique, le fonctionnement soit efficient sur le terrain.

Cet enjeu de la gouvernance me permet de revenir plus précisément sur d'autres incohérences dans l'articulation entre les deux textes, notamment concernant la construction des bases légales pour procéder à la combinaison des données.

En effet, le DMA prévoit que les gatekeepers ont l'obligation de partager en temps réel les données agrégées et non agrégées. Mais cette notion de donnée agrégée et non agrégée n'existe pas en droit des données personnelles qui distingue entre données personnelles et données non personnelles. Ce flou crée ainsi une incertitude pour les entreprises soumises à ces obligations sur le terrain juridique applicable : doivent-elles vraiment partager des données agrégées à caractère personnel ou non ? Rien n'est dit à ce sujet car le DMA ne définit pas ces notions et ne propose pas d'articulation satisfaisante avec des définitions qui existent dans d'autres textes, comme le RGPD.

Enfin, le DMA fait souvent référence au RGPD de façon très sélective et partielle. L'analyse de départ est que les gatekeeper peuvent combiner de grands volumes de données, leur permettant ainsi de dominer le marché. Le DMA vise par conséquent à restreindre la combinaison des données : la plateforme ne doit pas pouvoir y procéder à moins d'avoir obtenu le consentement de la personne concernée. Toutefois, la combinaison de données personnelles est très fréquente pour lutter contre fraude ou garantir la sécurité des données. Le RGPD dispose donc de plusieurs bases légales possibles pour collecter des données, notamment le consentement de la personne, l'exécution du contrat (accepter les conditions générales d'utilisation d'un site), l'intérêt légitime d'une entreprise, une obligation légale… en bref le RGPD met dans le même article, plusieurs fondements légaux pour pouvoir traiter et collecter les données personnelles. En effet, le consentement n'est pas toujours la bonne base, notamment pour la lutte contre la fraude et pour la sécurité informatique. Il faudrait que le texte du DMA soit plus fin sur cette question, en distinguant selon les finalités de la combinaison de données. Au surplus, chacun perçoit qu'à force de solliciter le consentement des personnes, l'effet devient contreproductif. Le fait de « sur-solliciter » les personnes par l'intermédiaire de de demandes de consentement à répétition n'apporte pas davantage de du contrôle aux personnes mais introduit plutôt ce que nous appelons, « la fatigue du consentement », les personnes se lassent et cliquent sans regarder.

**TD: Comment le DMA peut soutenir le développement des PME européennes innovantes ? Pensez-vous que le texte réponde dans ses dispositions actuelles, à l'objectif de création de champions européens du numérique ?**

**YP:** Il y a un aspect d'économie industrielle derrière le texte qui n'est pas ma spécialité… Toutefois, nous voyons bien effectivement que le DMA, comme le DSA, le DGA, le Data Act ou le règlement sur l'intelligence artificielle ont en commun cette volonté d'affirmer la souveraineté numérique de l'UE. Le partage des données permettra peut-être l'émergence de champions européens dans des secteurs nouveaux. Le DMA, s'il est bien conçu sur le plan juridique,

constituera un puissant outil.

Concernant les PME, le DMA est clairement fait pour faciliter l'accroissement de l'innovation, notamment via le partage des données pour des entreprises qui n'ont pas accès à cette ressource. La législation vise ainsi les PME, les startups et même des entreprises plus installées. Il est clair que ce texte est conçu pour faciliter l'émergence de champions européens, peut-être des licornes, en leur donnant accès à des données auxquelles elles ne pourraient pas disposer, ou pas dans les meilleures conditions. Toutefois, pour que le texte joue pleinement son rôle auprès des PME, il faut absolument résoudre les injonctions contradictoires évoquées précédemment pour éviter des surcoûts juridiques importants. Si le DMA transmet une surcharge juridique, technologique ou de sécurité vis-à-vis des PME, ma crainte est que le texte rate son objectif.

Ainsi, pour faciliter l'accès aux données pour les PME il faudrait plutôt réfléchir à des codes de conduite qui seraient certifiés par le régulateur. Le RGPD prévoit que des codes de conduite puissent être élaborés par des secteurs d'activité et « labellisés » par le régulateur. De tels codes de conduite pourraient, par exemple, définir des finalités compatibles afin de faciliter le partage des données dans la sécurité juridique.

**TD: Cela fait le pont vers la dernière question: quelles sont les solutions à envisager ?**

**YP:** Le code de conduite est effectivement l'une des solutions qui peut permettre de répondre aux questions de la finalité, de la sécurité, éventuellement celle de la transparence (comment on informe les usagers des nouveaux usages ?). Cela peut être aussi un moyen de régler la question de la base légale. Toutefois, l'élaboration d'un code de conduite est un processus long : il faut mettre d'accord une profession ou un secteur d'activité, et il faut ensuite que le régulateur interagisse pour arriver à un accord. C'est un outil de droit souple efficace mais lent dans sa genèse.

# CONFRONTATIONS EUROPE


**Confrontations - Paris**
**29 avenue de Villiers**
**75017 Paris**

**Confrontations - Bruxelles**
**Rue du Luxembourg 19**
**1000 Bruxelles**

communication@confrontations.org

https//:confrontations.org

@confrontations

@ConfrontationsEurope