INTERVIEW CROISÉE

DMA : les dés sont lancés…

Le règlement DMA (Digital Market Act) vise à lutter contre les pratiques anticoncurrentielles des géants d'internet et corriger les déséquilibres de leur domination sur le marché numérique européen. Il est progressivement applicable depuis le 2 mai 2023. Quels changements pratiques emporte-t-il pour les entreprises.

Le point avec Éric Barbry, associé du cabinet Racine, expert en droit du numérique, des nouvelles technologies et des données personnelles, et Guillaume Fabre, associé du cabinet Racine, expert en droit de la concurrence.

Que va changer le Digital Market Act?

ÉRIC BARBRY : Le Digital Market Act (DMA) vise à réguler ce qu'il est convenu d'appeler les « contrôleurs d'accès » (« gatekeepers »). Sont considérés comme des contrôleurs d'accès les « services de plateformes essentiels » qui répondent à certains seuils de matérialité. Sont considérés comme proposant un « service de plateforme essentiel » une kyrielle d'acteurs assez hétéroclites : services d'intermédiation en ligne, moteurs de recherche en ligne, services de réseaux sociaux en ligne, services de plateformes de partage de vidéos, services de communications interpersonnelles non fondés sur la numérotation, systèmes d'exploitation, navigateurs internet, assistants virtuels, services d'informatique en nuage, services de publicité en ligne, y compris tout réseau publicitaire, échange publicitaire et autre service d'intermédiation publicitaire, fournis par une entreprise qui met à disposition n'importe lequel des services de plateformes essentiels. Ces acteurs sont qualifiés de contrôleurs d'accès s'ils franchissent les seuils suivants : un chiffre d'affaires annuel de plus de 7,5 Mds€ au sein de l'Union européenne (UE) lors des trois derniers exercices ou une capitalisation boursière moyenne ou valeur marchande de 75 Mds€ lors du dernier exercice ; l'entreprise a compté au moins 45 millions d'utilisateurs finaux actifs dans l'UE lors du dernier exercice et au moins 10 000 entreprises utilisatrices actives par an, établis également dans l'UE. Ces seuils doivent avoir été atteints pendant les trois derniers exercices. Ces contrôleurs d'accès doivent se déclarer comme tels auprès de la Commission européenne d'ici au 2 juillet. La Commission devra procéder à la désignation des contrôleurs d'accès avant le 6 septembre 2023. Ils auront jusqu'au 6 mars 2024 pour mettre en œuvre des mesures et procédures appropriées, ce qui suscitera un travail important, notamment en termes d'audit interne et d'adaptation au second semestre 2023.

Quelles sont les obligations pour les entreprises ? Comment vont-elles pouvoir s'ajuster ?

ÉRIC BARBRY : Les obligations pour les contrôleurs d'accès sont nombreuses, les conduisant à revoir en profondeur leurs pratiques, leurs règles internes et leurs conditions contractuelles. Une partie de ces obligations constituent des restrictions en termes d'utilisation de données à caractère personnel. Les contrôleurs d'accès se voient interdire un certain nombre d'usages de ces données sauf consentement exprès des personnes concernées, conformément aux règles fixées par le RGPD. Ces obligations vont assez loin comme le fait de procéder à un audit indépendant de toutes mesures techniques de profilage des consommateurs. D'autres obligations s'expriment en termes d'interdictions ou d'obligations. On notera par exemple le fait d'interdire :

- les designs et interfaces trompeurs et truqués, à l'instar des dark patterns, ayant pour objet d'inciter un utilisateur à privilégier un choix plutôt qu'un autre ;
- le fait d'obliger les utilisateurs à recourir aux autres services du contrôleur d'accès ;
- le self-preferencing ou auto-préférence, consistant à désavantager ses concurrents par rapport à ses propres services. Par exemple, un comparateur ou un moteur de recherche qui mettrait en avant les annonces portant vers ses propres services plutôt que ceux de la concurrence.

Il existe aussi des obligations particulières « de faire », en termes de d'interopérabilité et de transparence à l'égard de la Commission européenne notamment, comme par exemple l'obligation de l'informer de toute acquisition pour qu'elle puisse identifier et réagir aux "killer acquisitions".

Quels sont les risques et les sanctions ?

ÉRIC BARBRY : À l'instar du RGPD et son principe d'accountability, les contrôleurs d'accès devront être en mesure de démontrer leur conformité aux obligations issues du DMA. Dans les six mois de sa désignation par la Commission, le contrôleur d'accès remet à la Commission un rapport décrivant de manière détaillée et transparente les mesures prises. Ce rapport est mis à jour annuellement. Une synthèse est diffusée en ligne. Le contrôleur de données devrait donc disposer d'un ensemble d'éléments (documents et procédures) de nature à démontrer cette conformité. La Commission apparait comme le régu-


Guillaume Fabre


Éric Barbry

lateur en charge du respect du DMA. L'article 26 précise que *« la Commission prend les mesures nécessaires pour contrôler la mise en œuvre et le respect effectif des obligations du règlement »*. Ses pouvoirs sont très importants. Par exemple, elle peut exiger la communication de toute information qu'elle estimera nécessaire *i.e.* sur les algorithmes. Elle dispose d'un droit d'audition et d'inspection, et peut imposer des mesures provisoires, nonobstant la mise en œuvre d'une procédure de nature contentieuse. Elle peut constater et sanctionner le non-respect du DMA. La plupart des obligations sont sanctionnées d'une amende pouvant atteindre 10 % du chiffre d'affaires mondial en cas de non-respect et 20 % en cas de récidive s'agissant des obligations les plus importantes. L'ensemble des entreprises, contrôleuses d'accès ou non, peuvent se voir infliger une amende de 1 % du chiffre d'affaires mondial, principalement, mais pas uniquement, en cas de manquement aux obligations de collaboration et d'information à l'égard de la Commission. À ces sanctions s'ajoutent des astreintes pouvant atteindre 5 % du chiffre d'affaires journalier moyen. Les autorités françaises peuvent aussi intervenir. D'une part, un projet de loi envisage notamment que l'Autorité de la concurrence et Bercy puissent enquêter sur le non-respect du DMA, tout constat et sanction d'une violation étant réservé à la Commission. D'autre part, les juridictions nationales pourraient engager la responsabilité délictuelle des contrôleurs d'accès.

Quels sont les enjeux pour l'Union Européenne au niveau mondial ?

GUILLAUME FABRE : L'Union européenne a souhaité s'affirmer comme un précurseur mondial s'agissant de la réglementation économique des marchés numériques. Pourtant, les entreprises les plus évidemment visées par ce texte sont Américaines. Certains outre-Atlantique ont déploré ce texte qui menacerait des "American jobs". Dans le même temps, l'Union européenne a adopté un règlement pour contrôler les subventions étrangères, y compris celles qui pourraient découler de l'Inflation Reduction Act américain. Et l'Union européenne vient d'annoncer vouloir règlementer l'intelligence artificielle, très rapidement après l'apparition de produits grands publics tels que ChatGPT. En d'autres termes, le DMA semble s'inscrire dans un mouvement consistant pour l'Union européenne à tenter de se constituer un avantage compétitif (certains diront, à réduire son manque de compétitivité) par la voie règlementaire, en particulier par rapport aux entreprises américaines. Certains déploreront ce qu'ils verront comme des contraintes réglementaires freinant l'innovation, comme ceux qui notent que l'émergence de ChatGPT n'aurait pu survenir en Europe en raison de l'application du RGPD. D'autres se féliciteront des opportunités que cela pourrait créer sur le marché.

Quels sont les effets sur les Gafam ?

GUILLAUME FABRE : Ces acteurs ne sont pas nécessairement les seuls concernés, même s'ils étaient les principaux visés. Un certain nombre d'acteurs européens pourraient être contrôleurs d'accès – la Commission publiera la liste en septembre prochain. Tout commentaire sur l'effectivité des règles peut apparaître prématuré. D'une part, les obligations créées apparaissent importantes, avec des sanctions dissuasives. D'autre part, l'innovation est généralement rapide dans le secteur numérique (*i.e.*, l'IA n'est pas concernée) et les consommateurs peuvent avoir des habitudes bien ancrées. Enfin et surtout, l'interprétation des règles, par la Commission et, dans une moindre mesure, les juridictions nationales et l'Autorité de la concurrence, pourrait être décisive. Le texte soulève un certain nombre de questions et nos clients nous sollicitent déjà, nous donnant l'occasion de réunir des équipes pluridisciplinaires pour les accompagner. D'autres questions surgiront nécessairement à mesure de l'évolution du marché et de l'application du DMA.

Le maintien de règles différentes pour l'Europe par rapport au reste du monde est-il tenable sur la durée ?

GUILLAUME FABRE : Lorsque l'Union européenne s'est dotée du RGPD, la même question s'est posée. D'autres juridictions ont fini par lui emboîter le pas, telle que la Californie depuis janvier 2020. On ne peut totalement exclure l'apparition d'autres textes de ce type. D'ailleurs, les Américains ont leurs propres initiatives concernant le secteur numérique. Une autre hypothèse serait que les contrôleurs d'accès décident de limiter le champ d'application des obligations issues du DMA au marché européen. Si cela devait priver les Européens de produits innovants, ou les exposer à certains risques de sécurité qui n'existerait pas hors UE, cela pourrait créer une forme de pression pour réformer le DMA. ■