Que sont le DMA et le DSA, les nouvelles règles européennes de régulation d'internet ?

Reprise avec quelques modification d'un article de Vincent Lequeux, publié le 24/04/2022

Ces deux textes d'ampleur doivent limiter la domination économique des grandes plateformes et la diffusion de contenus et produits illicites en ligne. Quelles sont les conséquences pour Augmented Security.

Plus de 10 000 plateformes en ligne opèrent aujourd'hui sur le marché européen du numérique, estime la Commission européenne. Pourtant, seule une toute petite partie d'entre elles capterait l'essentiel de la valeur générée par ces activités.

S'ils ne sont pas directement cités, les GAFAM (Google, Apple, Facebook, Amazon et Microsoft) et autres géants du secteur sont les principales cibles de ces deux textes : le règlement sur les marchés numériques (Digital Markets Act, ou DMA) et le règlement sur les services numériques (Digital Services Act, ou DSA).

Le premier vise à mieux encadrer les activités économiques des plus grandes plateformes. Celles-ci sont qualifiées par la Commission de "*contrôleurs d'accès*" pour indiquer qu'elles sont devenues des passages obligés afin de bénéficier des avantages d'internet. Elles sont accusées de rendre les entreprises et les consommateurs particulièrement dépendants de leurs services et d'empêcher la concurrence des autres sociétés.

Le second, qui doit moderniser une partie de la directive datant de l'an 2000 sur le commerce électronique jusque-là inchangée, s'attaque quant à lui aux contenus (haineux, pédopornographiques, terroristes…) et aux produits illicites (contrefaits ou dangereux) proposés en ligne. Il cherche notamment à harmoniser les législations nationales déjà en place dans les Etats membres en la matière et a pour mot d'ordre : *"ce qui est illégal hors ligne doit également être illégal en ligne".*

18 mois après la proposition de la Commission, les négociations sur le DMA ont abouti à un accord entre Parlement et Conseil le 24 mars 2022. Le texte doit encore être formellement adopté par ces deux institutions avant d'entrer en vigueur (sous 20 jours) et être appliqué 6 mois après, en principe dès le mois d'octobre 2022.

Un mois plus tard, le 23 avril dernier, c'est le DSA qui a fait l'objet d'un accord provisoire à son tour. Il s'appliquera en deux temps : 15 mois après son entrée en vigueur ou à partir du 1er janvier 2024 pour la plupart des plateformes, la date la plus tardive étant retenue ; et 4 mois après leur désignation pour les très grandes plateformes en ligne et les très grands moteurs de recherche.

Une fois adoptés définitivement, ces deux textes s'appliqueront à l'ensemble des pays de l'UE et des entreprises qui y opèrent.

Quelles sont les nouvelles règles prévues par le DMA ?

DMA et DSA ne répondent pas aux mêmes défis. La législation sur les marchés numériques (DMA) doit limiter les nombreux avantages grâce auxquels les contrôleurs d'accès peuvent conserver une position dominante sur le marché. Face à leurs pratiques parfois déloyales, le texte vise à imposer un certain nombre d'obligations ex ante : aujourd'hui, les amendes sanctionnant les infractions au droit de la concurrence interviennent souvent tard, ce qui n'incite pas les sociétés à modifier leur comportement en profondeur.

Avec le DMA, les contrôleurs d'accès n'ont plus le droit de favoriser leurs propres services et produits par rapport à ceux des entreprises qui les utilisent, ou d'exploiter les données de ces dernières pour les concurrencer. Ils ne peuvent pas imposer les logiciels les plus importants (comme les navigateurs ou les moteurs de recherche par exemple) par défaut à l'installation de leur système d'exploitation. Désinstaller des logiciels ou applications préinstallés sur son ordinateur, son téléphone ou sa tablette devient également possible dans la plupart des cas.

Le règlement garantit aussi la possibilité pour une entreprise utilisatrice de promouvoir son offre, conclure des contrats avec ses clients ou proposer ses propres services aux consommateurs hors d'une plateforme à laquelle elle est liée.

Afin de faire la promotion de ses produits et services concurrentiels, une entreprise, et notamment un vendeur de biens en ligne, peut demander l'accès aux données générées par ses activités (performance marketing…) et à celles liées aux annonces publicitaires qu'elle finance sur une plateforme.

L'accord du 24 mars ajoute plusieurs nouveautés au projet initial. Comme le souhaitait le Parlement européen, une plateforme ne pourra associer les données personnelles d'un utilisateur à des fins de publicité ciblée qu'en cas de consentement explicite.

Les principaux services de messagerie (Whatsapp, Facebook Messenger, iMessage…) devront également être interopérables avec leurs concurrents plus modestes. Un utilisateur pourra ainsi envoyer des messages, des fichiers ou passer des appels vidéo depuis une application de messagerie vers une autre. Les réseaux sociaux pourraient eux aussi être concernés à l'avenir, ce qui devra être précisé par le Parlement européen et le Conseil. Enfin, les contrôleurs d'accès devront informer la Commission des acquisitions et fusions qu'ils réalisent.

Et par le DSA ?

La législation sur les services numériques (DSA) cherche de son côté à limiter la diffusion de contenus illicites (incitations à la haine ou à la violence, harcèlement, pédopornographie, apologie du terrorisme…) et la vente de produits illicites en ligne.

Afin de garantir ce principe, le DSA impose certaines obligations aux fournisseurs de services et notamment aux plateformes. Actuellement, les procédures de notification et de retrait de ces contenus et produits sont différentes d'un Etat membre à l'autre et ne permettent pas d'agir efficacement, les messages ou vidéos haineux étant par exemple supprimés longtemps après avoir été largement diffusés.

Si le DSA ne remet pas en cause la responsabilité limitée des plateformes vis-à-vis des contenus et produits illicites qu'elles hébergent (notion d'"hébergeur passif"), celles-ci devront en revanche proposer un outil permettant aux utilisateurs de les signaler. Une fois ce signalement effectué, elles devront alors retirer ces contenus et produits ou en désactiver rapidement l'accès.

Les plateformes auront l'obligation de coopérer avec des "signaleurs de confiance". Il s'agit d'organes, associations ou individus labellisés au sein de chaque Etat en vertu de leur expertise et qui verront leurs notifications traitées en priorité.

Le DSA interdit par ailleurs de cibler des personnes avec des publicités en ligne basées sur leur religion, leurs préférences sexuelles, des informations sur leur santé ou leurs convictions politiques. La publicité ciblée est également interdite vis-à-vis des mineurs.

La publicité ciblée et la politique de modération des plateformes sont soumises à des obligations de transparence. Les plateformes devront notamment expliquer le fonctionnement de leurs systèmes de recommandation, qui renforcent la visibilité de certains contenus pour un utilisateur en fonction de ses intérêts personnels. Les très grandes plateformes en ligne et les très grands moteurs de recherche auront également l'obligation de proposer aux utilisateurs un système de recommandation alternatif non fondé sur leur profilage.

Les "pièges à utilisateurs" ("dark patterns"), qui conduisent notamment les internautes à effectuer des actions non souhaitées sur un site au bénéfice de ce dernier, seront interdits.

Les très grandes plateformes, elles, seront par ailleurs tenues d'évaluer et de prendre des mesures pour atténuer les risques qui découlent de l'utilisation de leurs services : diffusion de contenus illicites, effets négatifs sur la vie privée et familiale, atteintes à la liberté d'expression… Elles devront réaliser chaque année cette analyse de réduction des risques sous le contrôle de la Commission européenne.

Les places de marché en ligne, qui réunissent des vendeurs et des consommateurs comme Amazon ou AirBnb, devront quant à elles afficher un certain nombre d'informations relatives aux produits et services qu'elles vendent, et détenir des informations permettant de tracer les vendeurs de biens et services illicites.

La Commission avait également proposé que le DSA impose à toutes les entreprises fournissant des services en ligne aux Européens de désigner un représentant légal dans un pays de l'UE. Celui-ci devrait par exemple, dans le cas des plateformes, obéir à toute demande de retrait de contenu ou de produit dangereux de la part de l'un des 27 Etats membres.

Toujours selon la proposition initiale de la Commission, un "coordinateur des services numériques" au sein de chaque Etat pourra également enquêter, saisir la justice s'il constate des irrégularités et même sanctionner directement une entreprise dans certaines situations. Les 27 coordinateurs coopèreront au sein d'un "comité des coordinateurs nationaux des services numériques" habilité à mener des enquêtes conjointes dans plusieurs Etats. Ce dernier pourra également recommander à la Commission européenne d'activer un mécanisme de crise lors d'événements particuliers pour lutter contre la désinformation en ligne.

Tandis que les Etats membres surveilleront les petites plateformes, la Commission disposera quant à elle d'un pouvoir exclusif de supervision des très grandes plateformes en ligne et des très grands moteurs de recherche, soit

une trentaine de sociétés. Une nouvelle responsabilité qui doit être financée par les plateformes elles-mêmes, en fonction de la taille de leur service et à hauteur de 0,05 % maximum de leur revenu net annuel mondial.

Plusieurs dispositions du DSA visent à contrebalancer les mesures de contrôle des contenus afin de garantir le respect de la liberté expression : l'auteur d'un contenu illicite devra être informé avant le retrait de ce dernier. Il pourra contester gratuitement cette décision auprès de la plateforme (en plus de la justice) et demander une compensation financière à l'entreprise si celle-ci ne respecte pas le texte.

Si la législation sur les services numériques (DSA) vise à encourager la suppression des contenus illicites, les contenus préjudiciables (désinformation, canulars, manipulation…) licites ne sont pas concernés au même plan. Le texte vise à limiter leur propagation non par leur suppression, qui serait contraire à la liberté d'expression, mais en exigeant des plateformes qu'elles revoient les mécanismes (algorithmes) permettant leur amplification.

Ces contenus préjudiciables font également l'objet aujourd'hui d'une régulation européenne non contraignante, notamment via le code de bonnes pratiques contre la désinformation, signé par plusieurs grandes entreprises du numérique.

Quelles sont les sanctions prévues ?

Si elle estime qu'un contrôleur d'accès ne respecte pas ses obligations prévues par le DMA, la Commission peut lui indiquer des mesures concrètes à mettre en œuvre. Si celui-ci persiste, il peut se voir infliger des amendes allant jusqu'à 10 % de son chiffre d'affaires mondial total. En cas de récidive, cette amende peut aller jusqu'à 20 % de ce chiffre d'affaires.

En cas de non-respect systématique du DMA (règles enfreintes au moins 3 fois en 8 ans), la Commission peut ouvrir une enquête de marché et, si nécessaire, imposer des mesures telles que l'interdiction d'acquérir d'autres entreprises pendant une période donnée.

La Commission européenne est responsable de la bonne application du règlement par les contrôleurs d'accès qu'elle aura désignés, ainsi que des éventuelles sanctions. Les autorités nationales de concurrence des Etats membres peuvent quant à elles ouvrir des enquêtes sur des infractions présumées et transmettre leurs conclusions à l'exécutif européen.

Dans le cadre du DSA, chaque Etat membre déterminera les sanctions applicables dans la limite de 6 % du revenu ou du chiffre d'affaires annuel de la société (plafond abaissé à 1 % en cas d'informations incorrectes ou de refus d'enquête sur place). Les astreintes seront limitées à 5 % du chiffre d'affaires quotidien. Pour les très grandes plateformes, la Commission pourra contrôler elle-même le respect de la législation. Les entreprises qui ne respecteraient pas les règles de manière répétée pourront être interdites.

Quelles conséquences pour Augmented Security ?

Notre savoir- faire consiste à simplifier la signature renforcée, une obligation dans la Communauté Européenne, que ces deux textes en filigrane, évoque. Cela évite les manœuvres illicites de pénétration, de vols et autres actions illégales.

Directement nous ne sommes pas concernés par les textes entourant le DMA. En rechange nous avons tout notre rôle au sein du DSA. Ne serait-ce que nos clients démontrent leur volonté de « bon citoyen européen ».

Indirectement, ces textes participent à valoriser Augmented Security qui se retrouve encore plus que d'habitude au cœur du moteur.

Justement, et l'automobile dans tout cela ?

Augmented Security alerte les constructeurs et les tiers one sur les dangers inhérents à la prévalence du cloud dans tous les véhicules. Vols, suivi illégal, accidents. Un nouveau VWgate potentiel.

Or tous les constructeurs automobiles souhaitent devenir des acteurs importants du Net confére de nombreux articles tels que *« La filiale Stellantis & You veut capter 25 % des clients sur Internet » « L'expérience digitale à bord des futurs véhicules de Stellantis sera signée Amazon ».. » Renault se tourne vers le Snapdragon Digital Chassis de Qualcomm*" etc..

Ces acteurs seront soumis dès la fin 2022 aux textes DMA et certainement ceux du DSA. Une opportunité importante pour Augmented Security, dont le brevet Européen participe à sécuriser et faciliter l'utilisation légale du DSP2.

De plus, lors du Forum Europe : vers un espace numérique Européen organisé conjointement par la CCI Paris Ile de France et par *entreprise europe network*,[1] il a clairement été évoqué que les USA et les principaux pays industriels suivaient avec intérêt les avancées européennes à fin d'implémentation dans leurs propres zones d'influence.

[1] Entreprise europe network dépend de la Commission Européenne et a pour objectif « d'aider les entreprises à innover et à se développer à l'international Réseau Entreprise Europe (europa.eu)