

**Compte rendu du séminaire Nasse (14 octobre 2021) :**  
**« Protection de la vie privée et concurrence »**

Lors du séminaire Nasse organisé le 14 octobre 2021, **Winston Maxwell** - Directeur d'études Droit et Numérique à Télécom Paris, Institut polytechnique de Paris ; ancien associé du cabinet Hogan Lovells et avocat aux barreaux de New-York et de Paris et **Fabrice Rochelandet** - Docteur en économie, professeur à l'université Sorbonne Nouvelle Paris 3, ont débattu sur le sujet « protection de la vie privée et concurrence ». La séance a été animée par **Aymeric Pontvianne** - Conseiller finance et innovation à la CNIL.

Les présents propos n'engagent que leurs auteurs et ne sauraient être considérés comme constituant une prise de position officielle de leurs employeurs ou de la DG Trésor.

**Présentations des intervenants**

**Partie 1 : « Privacy » et concurrence : constats et concepts existants**

***Fabrice Rochelandet***

Le processus de plateformisation aboutit à une concentration des données, notamment par les GAFAM. Cette concentration des données s'est amplifiée par des mouvements d'acquisitions ainsi que par des formes de « répliquions déloyales »<sup>1</sup>. A cela s'ajoute la sophistication des algorithmes qui permet : aux utilisateurs finaux d'avoir une offre de service innovante, aux utilisateurs professionnels d'effectuer du profilage et de la prédiction de comportement, aux plateformes numériques de renforcer leur capacité de différenciation vis-à-vis des utilisateurs particuliers et professionnels. Si la collecte et l'exploitation des données peuvent être source d'innovations, de bien-être et de profits, elles sont également sources d'effets négatifs car elles peuvent porter atteinte à la vie privée, à l'autonomie individuelle (*i.e.*, dépendance aux médias sociaux), ou encore contribuer au renforcement et à l'abus de position dominante (*e.g.*, baisse de la qualité de service ou de l'innovation).

L'écosystème des données personnelles se compose du marché des services utilisateurs des données et du marché des données sur lequel sont échangées les données. Ces marchés sont interdépendants et connaissent des défaillances provenant de trois facteurs : (i) la valeur des données naît de leur combinaison ; (ii) l'existence d'effets de réseaux, car plus un opérateur de plateforme collecte des données, plus l'utilité, la valeur et le pouvoir de marché de la plateforme augmentent sur le marché des données ainsi que sur le marché des services numériques ; (iii) la collecte de données sans compensation monétaire directe car si le coût marginal de collecte des données est quasi-nul pour les plateformes, l'accès à des données supplémentaires est source de bénéfices, même minimes, lesquels, cumulés, renforce son pouvoir de marché.

Ces défaillances contribuent à accroître le pouvoir de marché des grandes plateformes, qui paraît disproportionné : les utilisateurs, verrouillés sur le marché des services, acceptent des conditions d'utilisation sur le marché des données ; par ailleurs, l'acquisition de données brutes à un prix quasi nul sur le marché des données renforce le pouvoir des plateformes numériques, ce qui leur permet d'améliorer leurs services et d'engranger des surprofits pour en financer de nouveaux ; ces nouveaux services permettront d'augmenter la dépendance des utilisateurs et des fournisseurs de contenu. A cela s'ajoute le « *privacy paradox* » : les utilisateurs sous-estiment la valeur de leur vie privée. Le

---

<sup>1</sup> Les « répliquions déloyales » désignent des situations dans lesquelles de nouveaux arrivants font concurrence aux géants du numérique et les géants font alors un « clonage de services », de sorte qu'ils collectent les mêmes types de données que les nouveaux entrants, sans avoir à les racheter.

pouvoir de marché des opérateurs de plateformes numériques et les dommages en termes de vie privée sont donc étroitement liés, d'où la nécessité et la difficulté à réguler ces acteurs.

### **Winston Maxwell**

Les données personnelles sont à la fois un droit fondamental (*i.e.*, une extension de la personne) et un bien économique (*i.e.*, l'un des objectifs du Règlement général sur la protection des données – RGPD - est de faciliter les flux libres des données au sein du marché unique).

Il existe différentes interprétations du RGPD. Certains considèrent que le RGPD renforce le pouvoir de marché des acteurs en place (Gal et Aviv, 2020), les actions d'une plateforme visant à renforcer la protection de ses utilisateurs pourraient devenir anticoncurrentielles. Ainsi, en 2018, l'Autorité de la concurrence a conclu que la législation sur les cookies pénalisait les éditeurs indépendants et favorisait les acteurs de plus grande taille. Récemment, la Commission européenne a lancé une enquête à propos du programme Google Privacy Sandbox<sup>2</sup>. La même problématique a été au cœur du procès entre LinkedIn et un acteur indépendant hiQ Labs aux Etats-Unis<sup>3</sup>. Pour d'autres, le RGPD serait pro-concurrentiel sur certains aspects tels que la portabilité des données, qui améliore la concurrence et la maîtrise des individus sur leurs données. D'après la littérature, l'impact de cette portabilité serait toutefois limité. Interpréter la protection des données comme critère de qualité pourrait également faire du RGPD un règlement pro-concurrentiel. Cependant, le fait que les individus accordent en pratique peu de valeur à la protection de leurs données personnelles empêche les entreprises de se différencier sur ce critère comme qualité de service.

Il existe tout de même des points de convergence entre le RGPD et le droit de la concurrence : les deux visent à améliorer le bien-être du consommateur, et sont centrés sur le concept de loyauté (« *fairness* »). En Allemagne, le contentieux Facebook<sup>4</sup> amène à s'interroger sur la spécialité des instruments législatifs (*i.e.* en cas de violation observée, faut-il privilégier une législation spécifique, plutôt que le droit de la concurrence ?) et le principe de *non bis in idem* (interdiction de condamner deux fois pour le même acte).

## **Partie 2 : Quels sont les besoins de régulation, faut-il aller plus loin que le droit existant ?**

### **Winston Maxwell**

Au niveau européen, différentes initiatives sont en cours avec le *Digital Market Act* (DMA), le *Data Act*, l'expérience de service digital pour les services de paiements (DSP2),... afin de prévoir de nouveaux textes réglementaires sur le sujet des données. Les autorités de données à caractère personnel en Europe n'ont pas les mêmes possibilités que les autorités de concurrence.

La proposition de règlement sur la gouvernance européenne des données créerait des intermédiaires neutres de confiance afin de favoriser le partage des données entre individus. Comment ce système pourrait-il émerger sans incitation pour les individus (*e.g.*, idée de monétisation des données) ? Aux Etats-Unis, des sénateurs ont proposé d'obliger les plateformes à publier la valeur des données

---

<sup>2</sup> Ce programme, qui avait pour objectif d'améliorer la protection de la vie privée des internautes en limitant la présence de cookies externes, a été décrié par les concurrents comme étant anticoncurrentiel et visant à renforcer le pouvoir de Google.

<sup>3</sup> LinkedIn a interdit l'accès de ses données à hiQ Labs car ce dernier ne respectait par son règlement sur la protection des données des utilisateurs. HiQ Labs a remporté le procès au motif que l'acte de lui couper l'accès était anti-concurrentiel.

<sup>4</sup> En 2019, l'Autorité de la concurrence allemande, a ordonné à Facebook de cesser la collecte de données relatives à des sites extérieurs à Facebook en estimant que cette collecte était excessive et que le consentement n'était pas valable car non librement donné (abus de position dominante). La Cour d'appel de Düsseldorf a suspendu l'ordonnance car elle considérait que l'effet sur la concurrence n'avait pas été suffisamment démontré. En 2020, la Cour fédérale a cassé l'arrêt de la Cour d'appel, au motif que la réduction du choix des consommateurs a un impact sur la concurrence.

individuelles par utilisateur. Une telle mesure permettrait notamment aux individus de prendre conscience de l'argent généré par leurs données.

### **Fabrice Rochelandet**

Il serait intéressant d'évaluer l'efficacité des régulations déjà en place. Le droit à la portabilité a des effets ambigus : coût élevé de mise en œuvre pour les consommateurs et potentiels effets anti-innovation (une plateforme ne souhaite pas partager ses données avec les autres acteurs du marché) ; pour autant, ce droit à la portabilité peut avoir des effets concurrentiels et vertueux, par exemple pour les plateformes de contenu (*e.g.*, un utilisateur non satisfait de Spotify pourrait se tourner vers Deezer). Cela est moins évident dans le cas des GAFAM, du fait du peu de concurrence auquel ils font face.

Une idée pour monétiser les données serait de créer des communs, en s'inspirant de ce qui se fait pour les droits d'auteur, en mettant en place des formes de sociétés de gestion collective : les individus étant exclus du marché des données, une solution pourrait être de les faire entrer en tant que propriétaires de données. Mais cela pose différentes interrogations : quelle est la valeur de ces données brutes, s'agit-il des données des utilisateurs ou des données combinées entre elles ?

## Interactions avec le public

### ***Monétisation des données personnelles et possibilités d'inversion des modèles « données contre service » à prix monétaire nuls :***

Cela dépend des droits de propriété que l'on pourrait donner aux individus. Cette monétisation devrait-elle avoir lieu *ex ante* (*e.g.*, prix à négocier avec la plateforme) ou *ex post* (*e.g.*, droit à compensation) ? Un des défauts serait qu'il s'agit de négociations collectives peu évolutives. *Cf.* également des situations où des « *class actions* » réclameraient une compensation. Des tentatives ont eu lieu aux Etats-Unis mais pour le moment, les tribunaux n'acceptent pas d'attribuer une valeur monétaire à un dommage virtuel de « *privacy* ».

### ***Amélioration des modèles d'affaires en prenant davantage en compte la protection des données personnelles :***

Du point de vue du RGPD, ces améliorations sont louables et vont dans le sens du renforcement de la « *privacy* ». Cependant, pour les concurrents de plus petite taille, cela peut être vu comme une barrière d'exclusion. Dans le cas où les plateformes accepteraient de réduire leur profit et de mettre en place des systèmes de « *privacy* » concurrentiels, se poserait toujours la question de la connaissance du consommateur quant au devenir concret de ses données.

### ***Vol de données personnelles, par exemple dans la santé : à qui cela profite-t-il, comment améliorer la régulation ?***

Comment corriger le dommage *ex post* ? Comment inciter les acteurs à investir dans la sécurité des bases de données ? Aux Etats-Unis, le dommage réputationnel considérable crée une incitation à investir pour les acteurs (principe de « *name and shame* »).

### ***Concernant l'incitation au partage des données, quelle serait la meilleure approche réglementaire (horizontale ou sectorielle) ?***

En télécommunications, on ne peut pas se passer d'une approche sectorielle pour déterminer ce que signifie l'accès ou quelle partie du service peut avoir tel ou tel accès.