Numéro 6 – Mai 2022 – Droit et numérique

Journal du DAA

Le J/DAA, votre revue étudiante en droit des affaires

A retrouver dans votre numéro sur le Droit et le numérique:

A la Une en droit des affaires

Le *Cyberscore*, nouvel outil de décision à la disposition du consommateur.

La mise en lumière des risques relatifs à la cybersécurité par la crise du Covid, ainsi que la préoccupation croissante des citoyens concernant leurs données personnelles[1] ont incité le législateur à accélérer la lutte contre les cyberattaques, qui portent atteinte aux données personnelles et à la souveraineté numérique. La loi n° 2022-309[2] a donc été promulguée le 3 mars 2022 dans le but d'informer le consommateur sur les risques qu'il encourt par l'utilisation de certaines plateformes et réseaux sociaux. L'effet de cette loi n'est pas de décourager le consommateur à avoir recours à ces outils numériques, mais bien de l'informer des risques qu'il prend en décidant de les utiliser.

Cette initiative s'inscrit dans une démarche européenne[3] et nationale[4] de protection de la sécurité dans le domaine numérique. En effet, ce texte se place dans la continuité de l'activité de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) en étendant les certifications mises en place par cette dernière aux outils numériques grand public et, surtout, en les rendant obligatoires[5]. Celle-ci entrera en vigueur le 1er octobre 2023[6].

Qui est concerné par ce nouveau texte ?

Seuls sont concernés certains acteurs qui répondent à deux critères. Tout d'abord, ils doivent être

[1] Rapport n° 38 (2020-2021) de Mme Anne-Catherine LOISIER, fait au nom de la commission des affaires économiques, déposé le 13 octobre 2020.
[2] Loi n° 2022-309 du 3 mars 2022 pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public.
[3] Mise en place de l'EU Cybersecurity Act (loi européenne sur la cybersécurité) ; règl. (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité).
[4] Développement de certifications de sécurité par l'ANSSI
[5] X. DELPECH, « Un audit de cybersécurité à la charge des grandes plateformes numériques », Dalloz Actualité, 15 mars 2022.
[6] Loi n° 2022-309 du 3 mars 2022, art 2.

qualifiés, soit d'opérateur de plateforme en ligne[1], soit de personne fournissant « des services de communications interpersonnelles non fondés sur la numérotation » (services de courriel ou messagerie électronique, de visioconférence), définis à l'article L32, 6° quater du Code des postes et des communications électroniques.

Par ailleurs, un décret précisera le seuil d'activité au-delà duquel les opérateurs seront soumis à cette obligation de transparence sur les risques de sécurité. Ces seuils sont mis en place afin de ne pas faire peser sur les petites plateformes des obligations qu'elles ne pourraient supporter (ou le pourraient difficilement). Cette limitation du champ d'application résulte, semble-t-il, d'un souci de mise en balance entre, d'une part, les coûts de mise en œuvre qui créeraient des barrières à l'entrée pour les opérateurs de petite taille et limiteraient l'innovation et, d'autre part, la nécessaire sécurisation de l'expérience numérique des consommateurs. Le choix a donc été fait d'imposer de « nouvelles obligations en matière de cybersécurité aux grandes plateformes numériques, aux messageries instantanées et aux sites de visioconférence les plus utilisés »[2].

Quelles sont les obligations imposées par cette loi ?

Le choix a été fait d'insérer un article L.111-7-3 dans un chapitre du Code de la consommation intitulé « obligation générale d'information précontractuelle ». L'objectif, clairement affiché, est donc la protection du consentement libre et éclairé du consommateur, qui bénéficie de plus en plus d'informations lui permettant de prendre des décisions économiques en pleine connaissance de cause.

Afin de satisfaire cet objectif de transparence accrue en faveur des consommateurs, le législateur a mis en place un Cyberscore, à l'image du Nutriscore inséré sur les emballages de produits alimentaires. En résumé, les entreprises devront faire figurer, sur leur site ou plateforme, un pictogramme coloré reflétant le degré de sécurité accordé aux données des utilisateurs.

Cette information requiert donc une double obligation. Tout d'abord, les acteurs concernés doivent réaliser un « audit de cybersécurité »[3]. Ce dernier est effectué par des « prestataires d'audit qualifiés par l'Agence nationale de la sécurité des systèmes d'information »[4] et porte sur « la sécurisation et la localisation des données qu'ils hébergent, directement ou par l'intermédiaire d'un tiers, et sur leur propre sécurisation »[5]. Les critères pris en compte par cet audit, ainsi que ses modalités de présentation et durée de validité sont précisés par arrêté.

Dans un second temps, une fois l'audit réalisé, son résultat doit être « présenté au consommateur de façon lisible, claire et compréhensible »[6] et un « système d'information coloriel »[7] doit l'accompagner. Le pictogramme du Cyberscore ne suffit donc pas. Les résultats de l'audit doivent également être présentés clairement au consommateur.

Notons que le législateur n'a pas souhaité limiter cet audit à la sécurisation des données personnelles des consommateurs. Ce dernier porte sur toutes les données que les opérateurs concernés hébergent. Le champ est donc élargi pour englober un grand nombre de données, donc un domaine large de sécurité.

Les plateformes et autres opérateurs qui manqueraient à cette obligation d'information s'exposent à la sanction précisée à l'article L.131-4 du Code de la consommation, à savoir « une amende administrative pouvant atteindre 75 000 € pour une personne physique et 375 000 € pour une personne morale ».

Les objectifs affichés par ce texte

L'objectif de cette loi est triple. D'une part, il s'agit de renforcer l'information du consommateur quant aux services qu'il utilise. Seulement, l'information ne porte plus sur les caractéristiques de ces services, mais bien sur le degré de sécurité qui est accordé aux données du consommateur lors de son utilisation. Cette information vise donc à ce que « les internautes puissent connaître la sécurisation de

[1] Au sens de l'article L.111-7 du Code de la consommation. Cela correspond aux plateformes proposant le classement, comme les moteurs de recherche, ou la mise en relation, comme les plateformes d'intermédiaire (Amazon, Blablacar, etc.).

[2] https://www.vie-publique.fr/loi/282626-loi-3-mars-2022-cyberscore-securite-des-plateformes-numeriques

[3] C. Cons., art. L.111-7-3, al. 1.

[4] C. Cons., art. L.111-7-3, al. 2.

[5] C. Cons., art. L.111-7-3, al. 1.

[6] C. Cons., art. L.111-7-3, al. 4

[7] *Ibid.*

leurs données sur les sites et réseaux sociaux qu'ils fréquentent »[1].

D'autre part, il est clair que l'un des enjeux est celui de la cybersécurité. En informant le public du degré de sécurité qui est assuré sur sa plateforme, l'opérateur mettra en lumière ses failles de sécurité et sera incité à y remédier. Le texte vise donc à lutter contre les failles de sécurité et le vol de données personnelles. Quoi qu'il en soit, le consommateur est informé de ces failles et des risques qu'il encourt et peut choisir de se tourner vers un service moins risqué. Il est désormais intéressé et sensibilisé aux questions qui touchent sa propre sécurité. Pour le législateur, il est « primordial de rendre accessibles au plus grand nombre les enjeux abscons de cybersécurité »[2]. Il s'agit donc d'un enjeu sous-jacent de sensibilisation des consommateurs à ces questions. Ce dernier est mis au premier plan en ce qui concerne la sécurité de ses données.

Enfin, un dernier objectif, directement lié au second, concerne la confiance dans le numérique. Objectif cher à l'Union Européenne[3], il permet de s'assurer de l'efficacité du marché numérique, qui est en très large expansion. Le consommateur confiant dans ce marché exerce des choix conscients, en connaissance des risques qu'il prend.

Les limites du dispositif

Toutefois, si ce texte nourrit des espoirs fondés, il est à craindre qu'il ne suffise pas à saisir tous les enjeux dont il doit tenir compte. Au-delà de la tendance à l'infantilisation du consommateur, il semblerait que de nombreuses attentes doivent être prises en considération, au risque que l'effet inverse à celui souhaité se produise. En effet, une gommette de couleur suffit probablement au consommateur pour saisir les risques qu'il prend en consommant des denrées alimentaires. Ces risques concernent sa santé et celle de la planète. Mais connait-il vraiment les risques afférents à la cybersécurité ? Il semblerait que la réponse soit de plus en plus positive, le consommateur étant progressivement intéressé et sensibilisé aux risques afférents à la sécurité de ses données. Mais pour que ledit texte soit efficace, il faudra qu'il contribue pleinement à cette sensibilisation et, surtout, qu'il prenne en considération la faible connaissance du consommateur. Son application – et les décrets et arrêtés à venir – devra, par conséquent, permettre aux consommateurs d'être véritablement et clairement informés des risques. L'information ne doit pas seulement porter sur le manque de sécurisation, mais également sur les risques que celui-ci entraine concrètement. Il est donc nécessaire d'obliger les plateformes à donner une information claire et complète reposant sur des critères complets et cohérents.

En l'absence d'une telle sensibilisation, l'effet du texte pourrait être amoindri. En effet, le consommateur s'est habitué à l'utilisation de ces plateformes. Il ne renoncera donc pas à des services qu'il utilise quotidiennement et sur lesquels il garde toutes ses conversations simplement parce qu'une vignette rouge apparait. D'autant plus que pour avoir connaissance des risques pour sa sécurité, il devra lire le résultat des audits de chaque plateforme pour opérer son choix.

En outre, les comparaisons sont beaucoup moins aisées que dans le cadre du nutriscore sur les denrées alimentaires. En effet, il est possible de renoncer à une marque de pizzas pour prendre celle qui a obtenu le meilleur score. Dans le domaine du numérique, l'innovation est telle que les services ne sont pas comparables. Également, les plateformes ne sont pas interopérables, de sorte qu'il existe d'importantes contraintes pour renoncer à une plateforme et en utiliser une autre. Le consommateur ne sera donc pas confronté à un seul choix entre deux plateformes selon leur risque. Il devra, sans même avoir pleinement conscience de la traduction de ces risques, savoir s'il est prêt à abandonner ses habitudes et conversations stockées pour protéger ses propres données (dont il ne connait souvent pas la valeur).

Ainsi, si l'idée générale du texte parait être la bonne, celle-ci doit se traduire par une sensibilisation des consommateurs, leur permettant de comprendre en quoi il est primordial de renforcer leur sécurité lors de leur expérience numérique. Mais surtout, l'information doit être compréhensible et reposer sur des critères exigeants et cohérents. Une bonne connaissance de ces enjeux permettra au consommateur de faire des choix libres et éclairés.

Clara CAMPAGNE

[1] https://www.vie-publique.fr/loi/282626-loi-3-mars-2022-cyberscore-securite-des-plateformes-numeriques
[2] Doc. Sénat, n° 629, 15 juill. 2020, p. 3
[3] En témoignent les débats actuels sur les projets de Digital Market Act et Digital Services Act.

Data Act, cybersécurité, concurrence : quelle gouvernance pour les données ?

Luc-Marie AUGAGNEUR
–
Avocat associé
Cabinet Cornet Vincent Ségurel

Dans l'émergence d'un droit des données, dont on a beaucoup dit par facilité qu'elles seraient un carburant de l'économie numérique, le Règlement Général sur la Protection des données (RGPD) a largement focalisé l'attention au cours des dernières années. Mais, dans le même temps, d'autres enjeux juridiques sont apparus que ceux liés à la vie privée et à l'autodétermination informationnelle des personnes concernées. La recrudescence de cyberattaques, sous l'action de groupes de criminalité organisée et aggravée par le contexte géopolitique, a mis en évidence la nécessité d'appréhender les conditions de sécurité de l'hébergement des données de façon à prévenir les risques et de garantir la responsabilité. Au demeurant, les risques ne sont pas seulement externes à l'entreprise. Une partie non négligeable d'entre eux provient des possibilités de leur détournement par les personnes qui y ont accès. D'où la nécessité de définir des conditions d'accès limitatives et d'organiser la traçabilité et le cloisonnement.

Pour autant, les stratégies liées au cloud ne réduisent pas les problématiques à ces aspects. Outre les aspects patrimoniaux et financiers liés aux modalités de maîtrise des infrastructures techniques (cloud privé/cloud public), elles font apparaître des risques de dépendance technique à l'égard des fournisseurs. Cette situation appelle non seulement une anticipation contractuelle de la réversibilité pour assurer la continuité d'activité avec d'autres prestataires ; mais aussi une régulation concurrentielle pour éviter les phénomènes de captivité à l'égard des services essentiels du marché bénéficiant d'effets de réseau.

Par ailleurs, les données ont la caractéristique (au moins apparente) de n'être pas rivales (leur jouissance ne s'épuise pas quand on les transmet) ; de sorte que leur circulation (quasiment sans coût) se trouve favorisée. Or, les échanges d'information entre opérateurs économiques peuvent faire apparaître des risques de concurrence en réduisant l'incertitude dans laquelle leur autonomie décisionnelle suppose qu'ils se trouvent. Ce d'autant que l'économie numérique rebat largement les positions sur le marché, soit par des phénomènes d'intégration économique, soit par la vente en ligne qui met en concurrence la tête de réseau avec ses distributeurs (comme l'illustrent les problématiques liées à la distribution duale dans la révision du règlement d'exemption sur les accords verticaux), soit dans le contexte des marchés bifaces où les plateformes et leurs utilisateurs interagissent sur plusieurs marchés (phénomène de hub and spoke). Les entreprises sont donc amenées à prévenir les risques liés à l'accès et à la circulation des données par une politique de conformité préventive efficace si elles veulent éviter de se voir reprocher des pratiques anticoncurrentielles collusives.

L'ensemble de ces aspects fait apparaître la nécessité de définir et de mettre juridiquement en œuvre, tant au plan contractuel que de la régulation, une véritable gouvernance des données, qu'elles soient personnelles ou commerciales.

Dans ce contexte, le projet de Data Act, récemment dévoilé par la Commission européenne donne à cet gouvernance une dimension qui dépasse le cadre de chaque entreprise en l'étendant à un écosystème interdépendant. Puisque les données ne sont pas un bien rival, mais que leur accaparement pourrait produire des pertes d'efficacité, le Data Act a l'ambition de définir les droits et devoirs de chacune des parties prenantes dans la vie de la donnée. Depuis leur génération, leur enrichissement, leur valorisation et leur utilisation, ces données sont amenées à être partagées dans des cadres contractuels variés (vente d'objets connectés, services sous forme numérique, capteurs de l'industrie 4.0).

Plutôt qu'une propriété privée rivale et appropriable, les données apparaissent ainsi comme un bien commun, au sens où l'entendait Elinor Oström, auquel il faut réserver un accès équitable et des règles de gouvernance adaptées. La possibilité pour l'utilisateur d'avoir accès aux données qu'il génère, ou de désigner un tiers qui les valorisera pour lui, comme la levée des obstacles à l'interopérabilité tiennent ainsi une place importante dans le projet de Data Act. Pour autant, un accès inconditionnel à des données valorisées pourrait donner lieu à des stratégies opportunistes. Le Data Act essaye ainsi de concilier ouverture des données et protection des secrets d'affaires de ceux qui les ont enrichies.

Ces quelques lignes ne donneront certes qu'une idée réductrice de ce projet de règlement européen, lequel doit lui-même être lu à la lumière des autres projets en cours (notamment le projet de Digital Market Act). Mais la combinaison des enjeux évoqués ici montre à quel point leur agrégation rend centrale la gouvernance des données, tant dans l'entreprise que dans son écosystème. L'appréhension juridique du sujet y est décisive puisqu'il s'agit à la fois de transmettre des données, de distribuer les droits qui s'exercent sur elles, mais aussi réguler les comportements pour satisfaire à des buts essentiels. A n'en pas douter, le droit de la gouvernance des données a de beaux jours devant lui !

Luc-Marie AUGAGNEUR

Vous avez dit « influenceur » ?

Christiane FÉRAL-SCHUHL
–
Avocate associé
Fondatrice cabinet FÉRAL
Médiatrice
Ex-présidente du CNB
Ex-bâtonnière de Paris

« Quel est votre métier ? »

« Influenceur ! » « influenceuse » !

En bref, « leader d'opinion sur les réseaux sociaux ».

Ces acteurs sont de plus en plus nombreux à opérer sur YouTube, Instagram, Twitch… au moyen de vidéos et visuels, avec pour mission d'influencer les choix des consommateurs, tous domaines confondus, qu'il s'agisse de sport, de cinéma, de musique, de mode, de voyages, de restaurants... ou encore pour défendre des causes comme la lutte contre les discriminations ou la protection de l'environnement.

Véritables stars du web, leurs cibles peuvent se compter en plusieurs milliers, voire millions de fans, à l'exemple de Cyprien (humoriste), Squeezie (gamer) ou encore Chiara Ferragni (influenceuse mode).

L'objectif ? Il s'agit le plus souvent d'accroitre la notoriété et la visibilité des marques dans le cadre de campagnes promotionnelles.

Comment ? En exposant publiquement leurs avis et leurs choix sur tel ou tel produit ou service. Ils peuvent ainsi le promouvoir (ou le détrôner), ou encore favoriser tel ou tel placement, faire le succès d'une opération publicitaire.

Ils sont désormais au cœur de la stratégie marketing des entreprises.

Ils sont courtisés, adulés, monétisés avec des cachets qui peuvent donner le vertige, les montants pouvant varier en fonction de l'audience.

Un concept étrange où l'influenceur / l'influenceuse offre une visibilité quasi permanente, cultivant « l'exposition de soi », n'hésitant pas à se dévoiler, parfois en toute impudeur ! La frontière entre sa vie privée et sa vie publique semble se dissoudre jusqu'à disparaitre. Mais après tout, il faut admettre que la vie privée est une notion fluctuante. Comme le rappelle le professeur Beignier[1], au XVII[e] siècle, les Parisiens se baignaient nus dans la Seine, la Reine de France accouchait en public et dans les habitations, il régnait une promiscuité que nous jugerions intolérable….

Désormais, l'influenceur ou l'influenceuse est un modèle, référence, guide, mentor… auprès d'un auditoire qui le suit, le scrute pour copier sa manière d'être, de penser, d'agir.

Alors, forcément, on en arrive ainsi très vite à la question de sa responsabilité, car on peut deviner les dégâts considérables que pourraient provoquer certains propos ou prises de position, relayés et partagés par des millions de fans.

Les règles de la responsabilité civile ont bien sûr vocation à s'appliquer. De même, la responsabilité pénale peut être engagée en présence, par exemple, de propos incitant à la haine ou jugés attentatoires à un groupe de personne déterminé.

L'obligation la plus essentielle pour un influenceur est certainement celle d'agir en transparence. La loi du 21 juin 2004 pour la confiance dans l'économie numérique prévoit en effet que « *toute publicité, sous quelque*

[1] B. Beignier, « La protection de la vie privée », *in* R. Cabrillac, M.A. Frison-Roche, T. Revet (dir.), *Libertés et droits fondamentaux*, 23[e] éd, 2017, Dalloz, p. 224.

forme que ce soit, accessible par un service de communication au public en ligne, doit pouvoir être clairement identifiée comme telle. »

Aussi, lorsqu'un influenceur ou une influenceuse est rémunéré(e) pour faire la promotion de produits et qu'il ou elle ne le précise pas, cela est de la publicité déguisée. C'est ce que la direction générale de la concurrence, de la consommation et de la répression des fraudes a indiqué à l'influenceuse Nabilla[1] qui avait publié sur son compte Snapchat une « story » faisant la promotion de services boursiers, sans mentionner à sa communauté qu'elle était rémunérée. En tant que professionnelle rémunérée, elle avait aussi l'obligation de ne pas induire en erreur les consommateurs sur les caractéristiques du service et les résultats attendus de son utilisation. Or, elle avait communiqué à tort sur la gratuité du service proposé ou encore la récupération systématique des sommes investies. Son comportement a été jugé trompeur[2].

Faut-il aller plus loin et envisager un statut spécifique pour l'activité d'influenceur ?

En fait, la vraie question est celle de savoir si la responsabilité de l'influenceur ou de l'influenceuse est la même lorsqu'il ou elle s'adresse à 10 suiveurs ou à plusieurs centaines de milliers de suiveurs ? Monsieur tout le monde aurait-il le même niveau de responsabilité que le *streamer* ZeratoR, qui organise depuis 4 ans des *live* caritatifs permettant de lever des fonds pour Amnesty International ? Quid lorsqu'il s'agit de plusieurs dizaines de millions de suiveurs ?

Ne serait-il pas temps de prévoir un code de conduite sur le web ?

Après tout, dans le monde réel, il existe un code de la route et il faut un permis pour pouvoir conduire une moto, une voiture, une camionnette, un poids lourd… un permis catégoriel en fonction du véhicule concerné, sauf pour les vélos, les trottinettes…

L'association RespectZone[3] qui lutte contre le cyberharcèlement propose que *« 20% des comptes les plus "influents" des utilisateurs inscrits en France suivre une formation spécifique au respect numérique et à la modération respectueuse (…) »* ?

Une idée intéressante à explorer et à généraliser.

En attendant, pourquoi ne pas exiger de chaque influenceur / influence, la signature d'une charte éthique dès qu'il franchit un seuil de « suiveurs » ? Une manière de le rappeler à ses responsabilités et d'encourager le respect de la cyberéthique.

Christiane FÉRAL-SCHUHL

[1] https://www.economie.gouv.fr/dgccrf/paiement-dune-amende-de-20-000eu-par-linfluenceuse-nabilla-benattia-vergara-pour-pratiques

[2] L'article L. 121-3 du Code de la consommation qualifie de trompeuse la pratique qui *« omet, dissimule ou fournit de façon inintelligible, ambiguë ou à contretemps une information substantielle ou lorsqu'elle n'indique pas sa véritable intention commerciale dès lors que celle-ci ne ressort pas déjà du contexte ».*

[3] https://www.respectzone.org/lassociation/

L'interview métier

Les métiers de la tech et le droit

Anis AYARI

Lead Data Scientist
Entrepreneur
Youtuber et Twitcher Tech

https://www.youtube.com/c/DefendIntelligence-tech?app=desktop
https://www.twitch.tv/defendintelligence

I - Présentation du métier

- **Pourriez-vous nous présenter votre métier ?**

Je suis Data Scientist, mais je préfère me définir en tant qu'ingénieur en Intelligence Artificielle, parce que je suis ingénieur et parce que j'ai plus une démarche d'ingénieur que de Data Scientist, qui est devenu un terme un peu "fourre-tout". Ce sont surtout des métiers de la donnée.

Concernant ma formation, j'ai une licence de physique. J'ai découvert l'analyse de données par le prisme de la physique. Puis, j'ai fait une grande école d'ingénieur, Télécom (École nationale supérieure des télécommunications et École supérieure de télégraphie). Je suis ensuite entré dans le machine learning par le prisme des télécommunications spéciales en partant à San Francisco à la sortie de l'École. De retour en France, j'ai travaillé dans des grandes boîtes de conseil. Ensuite, j'ai travaillé en Freelance, dans un label d'Universal Music avec des projets sur de la data et de l'intelligence artificielle. Ensuite, j'ai travaillé comme lead Data Science dans la Data factory d'Intermarché. Enfin, j'ai rejoint une startup il y a trois semaines.

La métier de Data Scientist est le métier central de la donnée en entreprise. C'est un métier assez jeune, qui est né environ en 2012. La plupart des Data Scientists ont commencé à être diplômés il y a peu. Je fais partie des premières promotions et j'ai été diplômé en 2016.
Les compétences reposent surtout sur l'informatique. Le traitement des données demande également de bonnes compétences en mathématiques, parce que l'on applique des théories probabilistes tous les jours.

- **Dans les propositions que vous avez faites pour le numérique pour le prochain quinquennat[1], vous avez évoqué l'image des métiers de la tech. Selon vous, comment est-ce qu'on pourrait faire connaître ces métiers et les rendre attractifs ?**

On ne peut pas dire qu'ils ne sont pas attractifs. Ils le sont pour une petite partie de la population, c'est-à-dire souvent des hommes qui passent leur temps sur leur ordinateur et qui se dirigent vers les métiers de la tech.

Nous sommes nombreux à défendre l'image des métiers de la tech et à essayer de casser cette vision au maximum. Nous essayons de démocratiser ces métiers pour attirer d'autres populations, notamment les femmes. Souvent, les femmes qui veulent faire du code sont désincitées. Elles pensent que ce n'est pas pour elles, parce qu'il n'y a que des hommes. C'est frustrant de savoir que des personnes se restreignent non par envie, mais parce qu'elles pensent que ce n'est pas pour elles. Cela veut dire qu'il y a un vrai problème de communication et de représentation. Je pense qu'il faut faire une campagne pour rendre ces métiers plus attractifs.

Nos métiers se trouvent parmi les mieux lotis : nous pouvons travailler où nous voulons, nous sommes très bien payés, nous pouvons très facilement changer de travail parce que ces compétences sont très recherchées. Très peu de personnes ont ce luxe de travail. Il faut s'affranchir des préjugés concernant ces métiers. Ils ne doivent pas être réservés à des hommes qui aiment les jeux vidéo.

[1] https://twitter.com/DFintelligence/status/1509115136514088960

Dans mon équipe tech, j'ai toujours essayé de tendre vers la parité. Le problème n'est pas dans la sélection, mais dans la représentation des candidats. Il n'y a que 20 ou 30% de femmes dans les équipes tech, mais le vrai problème est qu'il n'y a que 20 ou 30% de femmes dans les écoles d'ingénieur. Le problème est la formation et l'orientation des jeunes, mais aussi des handicapés, etc. Tout le monde a sa place dans ce milieu.

Surtout, nous avons besoin de personnes qui ne viennent pas du milieu de la tech, ce qui est peu connu. Par exemple, je travaille tout le temps avec des DPO (Data Protection Officer), des juristes, des designers, etc. Travailler dans la tech ne veut pas forcément dire faire du code, surtout avec les problématiques de protection des données, d'intelligence artificielle, de big data, etc. Nous avons besoin de juristes capables d'appréhender ces sujets relatifs au droit, que l'on rencontre tous les jours.

- **Avez-vous reçu une formation juridique et une sensibilisation aux questions juridiques dans vos études ?**

Je n'ai pas fait de droit dans ma formation, parce qu'il n'y avait pas encore ces sujets, mais actuellement, les formations sont davantage tournées vers le droit.

II - Les métiers de la donnée

- **Quelle a été l'influence du RGPD (Règlement Général sur la Protection des Données) sur votre métier ?**

Je pense que ce texte va dans le bon sens. Je crée du contenu vidéo dans lequel je mets l'intérêt des données utilisateurs au centre des enjeux, donc je pense que c'est positif.
D'un point de vue professionnel, cela nous a ralenti, dans le sens où cela nous met des barrières en plus. Par exemple, en travaillant sur un système de recommandation pour lequel j'avais besoin de données personnelles, le responsable de traitement nous a demandé de remplir un papier pour lister les données utilisées, pour combien de temps, pour faire quoi, etc. Cela rend les choses très complexes, demande plus de temps de travail et ajoute des process. Mais ces processus sont sains et utiles. Cela ajoute du travail, mais les enjeux sont importants.

- **Est-ce que les entreprises sont investies dans cette protection ?**

Je travaillais en conseil quand le RGPD a été voté, donc j'ai eu beaucoup de missions de conseil pour mettre les entreprises en adéquation avec le RGPD. C'était vu comme quelque chose d'obligatoire, mais contraignant. Cela ajoute de la charge de travail, donc logiquement, elles ont été réticentes. C'est devenu un sujet de société et, en plus, c'est obligatoire, donc elles le respectent, mais elles ne feront pas plus que ce qui est demandé.

III - Les métiers d'algorithmes

- **Est-ce possible d'intégrer les règles de protection des données dans un algorithme ? Est ce qu'il ne risque pas de créer des biais et aboutir à une situation de traitement illégal ?**

L'algorithme apprend à partir de données qu'on lui donne en entrée. Par exemple, si l'on souhaite faire appliquer une règle d'anonymisation des données, soit on fournit à l'algorithme des données déjà anonymisées, soit l'algorithme se charge de le faire. Cependant, l'algorithme ne va pas appliquer lui-même une règle de protection des données. Il s'agit simplement du produit d'un entraînement à partir de bases de données. Le but du machine learning n'est pas de donner de règle à l'algorithme, c'est l'algorithme qui trouve ses propres règles.

En revanche, il peut trouver des règles biaisées. Par exemple, il y a eu un algorithme créé aux Etats-Unis qui s'est entraîné pour prédire la durée d'occupation d'un lit des patients hospitalisés. L'algorithme avait tendance à favoriser les hommes et les femmes blanches par rapport aux personnes noires. Les personnes blanches avaient donc des durées d'hospitalisation plus longues que les personnes noires. En l'occurrence c'est un choix biaisé car deux humains atteints de la même maladie devraient en théorie avoir les mêmes chances de survie qu'importe leur couleur de peau. Ce biais est apparu car les données à partir desquelles s'entraînait l'algorithme

faisaient ressortir que les personnes blanches se soignaient mieux que les personnes noires aux Etats-Unis. Dès lors, l'algorithme en déduisait qu'ils avaient plus de chance de survie car ils se soignaient mieux, et avaient plus de moyens financiers pour le faire. Ce biais racial a été créé du fait d'un défaut d'études approfondies des données sur lesquelles s'entraînait l'algorithme.
Le problème réside donc dans les données d'entrée qui représentent des faits sociétaux.

- **Dans vos propositions sur le droit du numérique pour le prochain quinquennat, vous évoquez une obligation d'explicabilité algorithmique ? Cela correspond-il à une plus grande transparence de l'algorithme ?**

En effet, cela se réfère à une loi sur la transparence algorithmique. C'est un champ de recherche en pleine expansion aujourd'hui concernant l'intelligence artificielle qui s'appelle le XAI (explainable artificial intelligence ou applicabilité de l'intelligence artificielle) qui a pour but d'expliquer les décisions faites par un algorithme.
Par exemple, le secteur qui est impacté par excellence c'est celui de l'assurance ou du prêt. Quand une personne contacte son banquier pour obtenir un prêt, il va calculer des modèles de risque à partir d'algorithmes. L'idée c'est de pouvoir expliquer au client sur quels critères s'est basé l'algorithme pour lui refuser l'octroi d'un prêt par exemple. Cette transparence permet de comprendre les choix de l'algorithme. Cela demande d'intégrer cette transparence dès la conception de l'algorithme. L'idée serait donc d'imposer une loi qui exigerait que toutes les décisions prises par les algorithmes qui impactent directement les utilisateurs soient transparentes.

- **Comment pourrait-on articuler ce devoir de transparence avec d'autres lois telles que le secret d'affaires ?**

Aujourd'hui, on a l'impression que lorsqu'il s'agit d'algorithmes et de liberté d'expression sur internet, il y a une zone de "gris". Il faut toujours trouver un juste équilibre entre le droit au blasphème, à la satire, le droit à la propriété intellectuelle, le droit à l'image, le droit à la vie privée. Il faut également prendre en compte le manque de connaissance et de sensibilisation des juges à l'ensemble des problématiques liées aux nouvelles technologies.

- **Avec l'arrivée des textes européens DSA et DMA, est ce qu'il est possible d'intégrer ces questions de responsabilités directement dans le code ?**

Non car aucune instance ne viendra auditer ou contrôler le code.

Interview par Hélène BURLET et Clara CAMPAGNE

Vers un encadrement international plus performant de la fiscalité des activités numériques

À l'ère de la transformation numérique, de nouveaux enjeux font leur apparition dans différents domaines du droit et la fiscalité n'y échappe pas. Qu'il s'agisse de questions portant sur l'imposition des activités numériques, ou encore la coopération entre États et l'équilibre des systèmes fiscaux dans leur globalité, il parait plus que nécessaire que le cadre réglementaire évolue afin d'appréhender de manière efficiente et rationnalisée un secteur de l'économie en perpétuelle croissance qui représente plus de 11 500 milliards de dollars en 2016[1], estimé aujourd'hui à 15,5 % du PIB mondial selon les dernières estimations[2].

Pourtant et de manière surprenante, de nombreux millionnaires à la tête de plateformes bien connues[3] demandent à payer plus d'impôts. Bien que cette volonté s'inscrit, peut-être, dans un esprit de communication afin d'améliorer leur image, il n'en reste pas moins que les plateformes numériques supportent une charge fiscal bien moindre que les entreprises évoluant dans des secteurs traditionnels. Il semble donc nécessaire, afin de préserver l'équilibre entre les États, que chaque entreprise évoluant sur des secteurs différenciés de l'économie paie une taxe proportionnelle à son activité, les plateformes et entreprises numériques ne pouvant y faire exception.

Bien qu'Internet ait transformé notre quotidien, le droit, comme bien souvent, n'a pas évolué au même rythme. Les règles actuelles de la fiscalité internationale, parfois centenaires, s'avèrent n'être plus adaptées à l'époque contemporaine avec une application des règles fiscales subordonnant la taxation à des critères physiques là où les entreprises innovantes n'ont qu'une présence virtuelle sur des territoires où elles exercent pourtant une grande partie de leur activité et d'où elles tirent une partie non négligeable de leur chiffre d'affaires. En la matière, les critères actuels de taxation se trouvent souvent dépassés pour appréhender l'ensemble de la valeur économique qui résulte des activités du numérique.

L'Union européenne s'est saisie du problème et en parallèle de nombreuses discussions ont eu lieu au sein de l'Organisme de Coopération et de Développement Économique (OCDE). Les ministres des Finances des principaux pays membres de cet organisme ont adopté, le 27 novembre 2020 des conclusions détaillées afin de faire émerger une réglementation fiscale adaptée à l'ère du numérique et des nouvelles technologies.

Le 8 octobre 2020, après d'intenses négociations, 136 juridictions sur les 140 membres du projet OCDE/G20 sur l'érosion de la base d'imposition et le transfert de bénéfices (BEPS) ont adhéré, non sans mal, à la « Déclaration sur la Solution reposant sur deux piliers pour résoudre les défis fiscaux soulevés par la numérisation de l'économie ». Cette déclaration repose sur l'émergence de deux piliers.

Le Pilier Un accorde une répartition plus égalitaire des revenus imposables des entreprises multinationales les plus rentables du XXIe siècle. Cette mesure permettra concrètement de contrecarrer l'actuel critère physique d'imposition afin de permettre aux juridictions de marché d'avoir des droits d'impositions. Par exemple, il sera désormais possible pour l'État français d'appréhender une part de l'imposition des plateformes numériques en fonction de la part des utilisateurs français vis-à-vis des utilisateurs du monde entier.

Le Pilier Deux, quant à lui, introduit un taux minimum d'imposition mondial de 15 % ce qui permettra de réattribuer les bénéfices de ces grands groupes. Ce nouveau taux d'imposition minimum s'appliquera aux entreprises qui réalisent un chiffre d'affaires d'au moins 750 millions d'euros et devrait générer chaque année environ 150 milliards de dollars de recettes fiscales supplémentaires à l'échelle mondiale[4]. Cette mesure permettra concrètement une redistribution plus juste des recettes fiscales et permettra de lutter contre la fraude fiscale. Cette solution se fondera notamment sur la détermination d'un résultat fiscal unique, définies selon

[1] Rapport sur le développement du numérique de la Banque mondiale de 2016
[2] Rapport sur l'économie numérique – UNCTAD – mis à jour fin 2021
[3] The guardian, 18 Janvier 2022 « Millionaires call on governments worldwide to 'tax us now'»
[4] Estimation de l'OCDE

les règles GloBE et déterminées à partir des données de la consolidation comptable de l'entreprise multinationale.

PRINCIPAUX ÉLÉMENTS DE LA SOLUTION REPOSANT SUR DEUX PILIERS

Pilier Un	Pilier Deux
Les droits d'imposition au-delà de 25 % du bénéfice résiduel des EMN les plus grandes et les plus rentables seraient réattribués aux juridictions dans lesquelles les clients et les utilisateurs de ces EMN se situent	Les règles GloBE prévoient un impôt minimum mondial de 15 % sur toutes les EMN qui réalisent un chiffre d'affaires annuel supérieur à 750 millions EUR
Sécurité juridique en matière fiscale grâce à un mécanisme obligatoire et contraignant de règlement des différends, associé à un régime facultatif pour tenir compte des besoins de certains pays à faibles capacités	Obligation pour toutes les juridictions qui appliquent un taux nominal d'imposition des bénéfices des sociétés inférieur à 9 % aux intérêts, aux redevances et à un ensemble défini d'autres paiements d'adopter une « règle d'assujettissement à l'impôt » dans leurs conventions bilatérales avec les pays en développement membres du Cadre inclusif qui le demandent, afin que leurs conventions fiscales ne puissent pas faire l'objet d'une utilisation abusive.
Suppression des taxes sur les services numériques et des autres mesures similaires pertinentes et instauration du statu quo	Exception pour prendre en compte les incitations fiscales en faveur d'activités économiques substantielles
Mise en place d'une approche simplifiée et rationalisée pour l'application du principe de pleine concurrence dans des circonstances spécifiques, en mettant tout particulièrement l'accent sur les besoins des pays à faibles capacités.	

OCDE, schéma explicatif des deux nouveaux piliers[1]

Cette avancée majeure constitue pour le Secrétaire général de l'OCDE, Mathias Corman, « une grande victoire à mettre au crédit d'un multilatéralisme efficace et équilibré. Cet accord ambitieux garantit que notre système fiscal international est adapté aux réalités de l'économie numérique et mondialisé d'aujourd'hui ».

Toutefois, quelques pays restent réfractaires à cette mesure et il sera nécessaire de faire preuve de célérité pour la mise en œuvre effective de ces nouvelles mesures, le droit devant s'adapter le plus rapidement possible dans un système en perpétuelle mutation. Il faudra attendre quelques années après l'entrée en vigueur afin de confirmer avec certitudes si ce nouveau système répond aux enjeux actuels. Il est déjà toutefois prévisible que ce nouvel instrument de calcul nécessitera des calibrages pour être pleinement optimal.

En effet, ce système fait preuve d'une grande complexité et nécessitera une interconnexion exacerbée entre les systèmes fiscaux du monde entier. Cet échange d'informations s'inscrit toutefois dans le mouvement actuel de mondialisation avec des échanges de plus en plus rapides à l'ère du numérique, échanges transcendants les frontières comme le rappelle la récente guerre des Pixels sur Reddit[2]. Cet exemple illustre l'interconnexion croissante entre utilisateurs sur Internet et l'importance du numérique dans nos sociétés.

Enfin le calendrier de mise en œuvre de ces nouvelles mesures semble ambitieux avec une transposition initialement prévue en 2022 pour une entrée en vigueur effective en 2023. Outre les potentiels blocages politiques, comme l'illustre le récent refus de la Pologne de transposer la directive mettant en œuvre le pilier 2[3], la mise en place de cet instrument impliquera un vrai travail de préparation de l'administration fiscale mais également des multinationales. Ces dernières devront veiller au respect de ces obligations et à la bonne application des nouvelles normes par la mise en place de procédures internes spécifiques. Il faudra notamment que les services de consolidation participent aux calculs du résultat fiscal et à l'identification de tous les retraitements dans le monde entier.

[1] À consulter sur : https://www.oecd.org/fr/fiscalite/beps/brochure-relever-les-defis-fiscaux-souleves-par-la-numerisation-de-l-economie-octobre-2021.pdf

[2] La « guerre des pixels » lancés sur Redit le 1er avril 2022 a consisté pour des internautes du monde entier connectés simultanément à placer des millions de Pixels sur une vaste toile virtuelle, il s'agissait d'une initiative collaboratrice permettant à différentes « communautés » numériques de montrer leur influence. Cet évènement n'a fait que démontrer la place d'internet dans nos sociétés et la connexion exacerbée entre utilisateurs du monde entier.

[3] https://www.pwcavocats.com/fr/ealertes/ealertes-france/2022/04/absence-unanimite-proposition-directive-mettant-en-oeuvre-pilier-2-conseil-ecofin-5-avril-2022.html

Finalement, le numérique conduit à redéfinir le marché sur lequel va s'exercer l'imposition. Le critère de présence physique tend à disparaitre pour les entreprises du numérique afin d'être remplacé par la notion de juridiction de marché, c'est-à-dire aux États où se situent les consommateurs et qui semble plus performante. Cette redéfinition du marché n'est pas propre au droit fiscal et intervient également en droit de la concurrence[1] avec la notion de marché pertinent. En effet le marché pertinent « permet d'identifier et de définir le périmètre à l'intérieur duquel s'exerce la concurrence entre entreprises et permet de délimiter le cadre dans lequel la Commission européenne exerce sa politique de concurrence »[2]. À l'ère du numérique le critère traditionnel semble être en déclin, ne permettant plus de répondre aux nouvelles interrogations du droit de la concurrence face au numérique. Ainsi, un rapport préconise de porter une attention particulière à l'identification des préjudices et aux stratégies anticoncurrentielles plutôt qu'à cette définition dépassée du marché pertinent.[3]

Le groupe de travail sur le projet BEPS (*base erosion and profit shifting*) a également identifié, parmi ses quatre grandes catégories de défis pour la fiscalité du numérique l'impérativité de redéfinir plusieurs notions clés du droit fiscal tel que le concept du « nexus », le lien entre une entreprise et un territoire, ou celle de l'établissement stable. Certaines branches du droit, tel que le droit de la consommation sont encore allées plus loin en ne redéfinissant pas seulement les concepts clés à l'ère du numérique mais en définissant directement ce qu'il faut entendre par numérique. A titre d'exemple l'article liminaire du Code de la consommation a été modifié et comporte désormais une liste de nouvelles définitions en lien avec le numérique comme au paragraphe 6 « Bien comportant des éléments numériques » ou encore au paragraphe 7 « Contenu numérique ».

L'ensemble de ces illustrations en dehors du champ du droit fiscal montre que le développement du numérique pose des problèmes à l'ensemble des branches du droit, en raison notamment de l'incapacité des qualifications traditionnelles à saisir ces phénomènes et comportements nouveaux. Il semble nécessaire d'aller outre l'adaptabilité de la législation et d'enclencher une modification globale et profonde du système dans nos sociétés 2.0 en proie à une digitalisation de plus en plus importante.

Perrine ALBERT

[1] Voir l'article d'Alex NICOLLET et Thomas FRANCIA intitulé « la technologie blockchain, une nouvelle menace pour la concurrence ? », paru dans ce numéro.
[2] Définition du marché pertinent – communication de la Commission publiée au JOEU ((97/C 372/03)
[3] Rapport du 4 avril 2019 de la Commission européenne sur la politique de concurrence à l'ère du numérique

La technologie *blockchain*, une nouvelle menace pour la concurrence ?

En 2018, Isabelle de Silva – alors présidente de l'Autorité de la concurrence – constatait l'existence d'une « forte imprégnation de l'économie par le numérique, qui bouleverse les modèles d'affaires traditionnels »[1].
Lorsque l'on parle de numérique, d'innovation et de bouleversements, cela fait immédiatement penser à la *blockchain*. Cette technologie et les applications qui en découlent sont aujourd'hui au cœur de l'actualité, principalement avec les cryptomonnaies, les NFT, etc.
Si l'utilisation de la *blockchain* dans un cadre financier est de plus en plus analysée, l'étude des implications de cette technologie en matière de concurrence semble délaissée. À cet égard, certains dénoncent la trop grande attention portée aux pratiques anticoncurrentielles – principalement les ententes – basées sur les algorithmes, alors que la réelle menace pour le marché résiderait dans la *blockchain*[2]. En ce sens, l'Autorité de la concurrence elle-même relève qu'il existe des risques concurrentiels susceptibles de découler de l'utilisation de la technologie *blockchain*[3].

Pour beaucoup cette dernière demeure une notion mystérieuse et mal comprise. Ainsi, l'objet du présent article sera de tenter d'expliquer clairement ce qu'est la *blockchain*, afin de déterminer le rôle que celle-ci pourrait jouer dans la mise en œuvre de pratiques anticoncurrentielles. Enfin, il conviendra d'évoquer la capacité du droit de la concurrence à se saisir des potentielles atteintes au marché reposant sur la technologie *blockchain*.

I. Définitions

Alors, qu'est-ce que la ***blockchain*** ? L'Autorité de la concurrence l'a définie dans un avis d'avril 2021 comme une « technologie de stockage et de transmission d'informations, enregistrées sur des blocs et relatives aux transactions effectuées par les utilisateurs du réseau, qui permet de constituer un registre dans lequel l'information est simultanément distribuée entre tous les utilisateurs »[4]. En un mot, la *blockchain* est un registre d'informations.

Ce registre revêt plusieurs caractéristiques : il est transparent, sécurisé et décentralisé[5].
Transparent – Les transactions enregistrées sur la *blockchain* sont accessibles et visibles pour tous les utilisateurs.
Sécurisé – Les informations relatives aux transactions sont groupées au sein de blocs, lesquels sont horodatés, vérifiés par des mineurs[6], puis inscrits dans la *blockchain*. A partir du moment où le bloc intègre la chaîne de blocs, celui-ci ne peut plus être modifié et les informations qu'il contient deviennent donc quasi-immuables.
Décentralisé – Il faut comprendre que la *blockchain* vit au travers des utilisateurs du réseau. Ce sont eux qui assurent son fonctionnement, notamment en vérifiant la véracité des informations contenues dans les blocs avant que ceux-ci n'intègrent la chaîne de blocs. La *blockchain* n'est ainsi ni détenue ni contrôlée par un opérateur unique ou un petit groupe d'opérateurs. Elle n'appartient à personne sinon à la collectivité de ses utilisateurs. Dès lors, en principe aucun opérateur n'a d'emprise sur le système de la *blockchain*.

Cette dernière affirmation est cependant à nuancer. La décentralisation est effectivement un des caractères de la *blockchain* telle qu'entendue dans un sens commun et que l'on peut qualifier de *blockchain* publique.

[1] Interview d'Isabelle de Silva, Dalloz IP/IT 2017, p.488.
[2] T. Schrepel, « Ententes algorithmiques et ententes par blockchain », Recueil Dalloz 2020, p.1244.
[3] Autorité de la concurrence, Avis n° 21-A-05 du 29 avril 2021 portant sur le secteur des nouvelles technologies appliquées aux activités de paiement, p. 5.
[4] *Ibid*, p. 90.
[5] L. Bettoni, « Problématiques soulevées par la blockchain en droit de la concurrence », Contrats-Concurrence-Consommation, n°2, février 2020, Étude 3.
[6] Utilisateurs de la blockchain chargés de vérifier la véracité des transactions effectuées par les utilisateurs du réseau et regroupées au sein d'un bloc, afin que celui-ci puisse être ajouté à la chaîne de blocs. Cette vérification passe par la résolution d'un problème mathématique.

Néanmoins, elle ne décrit pas la réalité d'une *blockchain* privée. Il convient donc de distinguer ces deux notions.
La ***blockchain* publique** correspond à la définition donnée précédemment. C'est la chaîne de blocs accessible et visible par tous. N'importe qui muni d'un ordinateur peut devenir utilisateur du réseau et ainsi visualiser l'ensemble du contenu des blocs composant la chaîne.
La ***blockchain* privée** est quant à elle administrée par un opérateur (ou un groupe d'opérateurs) qui en définit les règles d'entrée et de fonctionnement. L'accès à la chaîne de blocs, et donc aux informations contenues par ceux-ci, est alors soumis à une autorisation préalable. En outre, la possibilité offerte à l'utilisateur de visualiser les informations contenues dans les blocs peut être restreinte.
L'utilité de ces deux types de *blockchain* diffère, tout comme leur potentiel rôle dans la mise en œuvre de pratiques anticoncurrentielles.
Pour la suite de cet article, le terme *blockchain* renverra indistinctement aux blockchains privées et publiques. Il sera spécifié lorsque seulement l'une d'entre elle sera évoquée.

En outre, il est nécessaire de définir une dernière notion, celle de ***smart-contracts***.
Littéralement « contrats intelligents », ce sont des « programmes informatiques permettant de vérifier ou d'exécuter automatiquement les termes d'un contrat {...} lorsque les conditions requises sont remplies »[1]. Ils s'appuient sur les données de la *blockchain* afin d'exécuter automatiquement certaines clauses contractuelles. A titre d'illustration, on peut imaginer le cas d'une location d'appartement. La mise à disposition du bien, observable informatiquement par le déverrouillage d'une serrure numérique par le client, engendrera automatiquement le paiement du loyer au propriétaire[2].

Les contours de la technologie *blockchain* ayant été précisés, il convient de s'interroger sur l'impact que celle-ci pourrait avoir en matière de concurrence, en étudiant ses potentiels effets pro-concurrentiels ainsi que les risques de développement de pratiques anticoncurrentielles.

II. Les potentiels effets pro-concurrentiels de la *blockchain*

Le postulat est que les entreprises enregistrent les transactions qu'elles réalisent avec leurs clients sur une *blockchain* publique. Comme évoqué précédemment, cette technologie induit de la transparence, laquelle va rejaillir sur le marché et bénéficier tant aux concurrents qu'aux consommateurs.
Ainsi, dans un tel cadre les opérateurs auront une connaissance plus fine du marché (des concurrents et des clients potentiels). Les entreprises utilisatrices auront la possibilité de visualiser les transactions qui ont été réalisées (pseudonyme des parties, date et heure, contenu transféré, prix…). Ces informations pourraient leur permettre de mieux cerner les besoins des consommateurs, leur disponibilité à payer et d'adapter leurs stratégies commerciales en conséquence. En ce sens, les données issues de la *blockchain* leur permettront notamment d'ajuster leurs offres à la demande et ainsi d'approcher un « prix optimal »[3].
Dans le même temps, cette transparence bénéficiera également aux consommateurs. Comme les entreprises utilisatrices, ceux-ci pourront visualiser l'ensemble des transactions effectuées et les informations y afférentes. Ainsi, ils auront une vision globale du marché (prix retenus pour des transactions équivalentes…). Cette meilleure connaissance du marché leur permettra de comparer les offres présentes sur celui-ci.
La concurrence entre opérateurs devrait ainsi sortir renforcée.

Cependant, ces potentiels effets pro-concurrentiels ne doivent pas éclipser le risque d'utilisation de la *blockchain* à des fins anticoncurrentielles.

[1] Autorité de la concurrence, Avis n° 21-A-05 du 29 avril 2021, précité, p. 86, pt. 415.
[2] V. en ce sens, L. De la Raudière et J-M. Mis, « Rapport d'information déposé par la mission d'information commune de l'Assemblée nationale sur les chaînes de blocs (*blockchains*) », décembre 2018, p. 35.
[3] L. Bettoni, « Problématiques soulevées par la blockchain en droit de la concurrence », précité.

III. Le risque de comportements anticoncurrentiels reposant sur l'utilisation de la *blockchain*

A l'instar de la distinction retenue par l'Autorité dans son avis de 2021[1], les risques concurrentiels seront envisagés en fonction des acteurs de la *blockchain* susceptibles de les mettre en œuvre : les personnes contrôlant l'accès à la *blockchain* ; les utilisateurs du réseau ; et les mineurs.

A) Les opérateurs contrôlant la *blockchain*

L'un des premiers comportements qui peut être envisagé concerne la situation dans laquelle l'opérateur contrôlant la *blockchain* utiliserait celle-ci afin d'évincer ses concurrents du marché.
Si l'on prend en considération une *blockchain* publique, il ne peut exister d'abus d'éviction. Par définition celle-ci est décentralisée, elle n'est donc pas contrôlée par un opérateur ou un petit groupe d'opérateurs.
Cependant, le risque d'abus d'éviction ressurgit lorsque l'on envisage la question sous l'angle d'une *blockchain* privée. Pour rappel, dans ce cas les règles d'accès, de fonctionnement et d'utilisation de la *blockchain* sont fixées par le développeur et l'accès à celle-ci est soumis à autorisation.
La *blockchain* est une source de données potentiellement stratégiques pour les entreprises opérant sur un marché. L'opérateur contrôlant la chaîne de blocs pourrait alors être tenté de restreindre l'accès à celle-ci afin d'empêcher ses concurrents – à tout le moins certains d'entre eux – d'accéder aux données qu'elle contient.
Si l'opérateur en question est en position dominante sur le marché, et selon la nature des données contenues dans la *blockchain*, il se peut que cette pratique constitue un abus de position dominante. Le refus sera abusif dans deux hypothèses[2] :

- Si les données en cause peuvent être qualifiées d'infrastructures essentielles : il faudra alors établir que celles-ci sont indispensables à l'exercice de l'activité des concurrents et l'absence de justification objective du refus d'accès.
- S'il est établi que le refus d'accès est discriminatoire et qu'il fausse le jeu de la libre concurrence (notamment en érigeant des barrières à l'entrée sur le marché).

Un abus de position dominante serait ainsi caractérisé.

Si le refus d'accès provient de la décision commune de plusieurs opérateurs s'entendant afin d'empêcher un concurrent d'accéder aux informations de la *blockchain*, il semble que celui-ci puisse être appréhendé sous l'angle de la prohibition des ententes entre concurrents.

L'Autorité de la concurrence pointe également le risque qu'un opérateur subordonne l'accès à une blockchain privée à des conditions susceptibles d'être qualifiées de pratiques de couplage, de ventes liées ou d'exclusivité[3] et donc d'abus de position dominante si l'opérateur occupe une telle position sur le marché.

B) Les utilisateurs de la *blockchain*

Tel qu'évoqué précédemment, la *blockchain* est un registre de données et la transparence qu'elle induit permet aux opérateurs d'avoir une meilleure connaissance du marché. Partant, celle-ci pourrait être utilisée par les opérateurs pour mettre en place une personnalisation tarifaire à l'égard des consommateurs, notamment à l'aide d'algorithmes ayant pour mission de fixer les prix.
Ce comportement peut correspondre à une pratique de discrimination tarifaire, consistant à fixer un prix différent pour un même produit en fonction de la propension du consommateur à acquérir ledit produit. En clair, pour des clients avec une faible disponibilité à payer, le prix est diminué. La perte de profit consécutive est alors compensée par une augmentation du prix du produit proposé à un consommateur ayant une plus forte disponibilité à payer.
La *blockchain* serait alors la source de données permettant à l'algorithme tarifaire de fonctionner et de fixer les prix de manière dynamique selon la disponibilité à payer du client.
Cette méthode de fixation des prix permet à l'entreprise d'accaparer la totalité du surplus du consommateur.

---

[1] Autorité de la concurrence, Avis n° 21-A-05 du 29 avril 2021, précité.
[2] Autorité de la concurrence, Avis n° 21-A-05 du 29 avril 2021, précité, pt. 402.
[3] *Ibid*, pt. 403.

Un autre risque lié à l'utilisation de la *blockchain* serait que des concurrents l'utilisent comme mode de communication indirecte afin de mettre en œuvre une entente.
Les concurrents se baseraient alors sur les informations contenues dans la *blockchain* pour aligner leurs comportements et aboutir à un équilibre collusif. Comme le relève Lucas Bettoni[1], cette pratique pourrait reposer sur des algorithmes intelligents, chargés de fixer les prix des différentes entreprises en se basant sur les données de la *blockchain*.
Se pose dès lors la question de la capacité du droit des ententes à saisir un tel comportement. En l'absence de preuve d'un accord de volonté explicite ou d'une décision d'association d'entreprises, il conviendrait de démontrer l'existence d'une pratique concertée entre entreprises. La caractérisation de cette dernière suppose la réunion de trois conditions cumulatives : une concertation entre concurrents ; un parallélisme de comportements ; et un lien de causalité entre ces deux éléments[2]. A cet égard, l'une des difficultés pour les autorités de concurrence résidera dans le fait que les informations contenues dans la *blockchain* sont publiques et donc accessibles à tous. La communication sera donc d'autant plus difficile à établir.
Ainsi, outre le parallélisme, il conviendra de relever plusieurs indices positifs (*plus factors*), corroborant l'existence d'une concertation entre concurrents et donc d'une entente.

Enfin, l'utilisation de la *blockchain* et des *smart contracts* pourrait être un vecteur de stabilisation des ententes entre concurrents.
Le recours aux *smart contracts* permettrait d'automatiser la gouvernance des ententes[3], ceux-ci exécutant de manière automatique les ordres prédéterminés et illicites des parties à l'accord.
Cela aurait pour conséquence d'éliminer les biais humains dans leur mise en œuvre.
En outre, cela réduirait considérablement le risque de déviation unilatérale des opérateurs. En effet, les *smart contracts* pourront détecter les déviations et les sanctionner de manière ciblée. L'effet dissuasif lié à cette sanction automatique via les *smart contracts*, couplé à la rapidité de détection qu'ils induisent, diminuera grandement les profits de déviation et donc *in fine* l'incitation à dévier de l'accord illicite.

C) Les mineurs de la *blockchain*

Concernant les mineurs, leur capacité à vérifier les transactions dépend pour une large part de leur puissance énergétique et informatique. Ainsi, les risques concurrentiels sont minimes lorsqu'ils agissent indépendamment.
Cependant, les mineurs se regroupent parfois en *pools*, afin de maximiser leur capacité de vérification et donc leurs profits. Cela a pour conséquence directe d'engendrer « une concentration du pouvoir de marché autour d'un ou plusieurs de ces groupements »[4].
Cette concentration confère à ces pools de mineurs une forme de pouvoir de contrôle sur la *blockchain*, duquel s'infère nécessairement un risque accru d'émergence de pratiques anticoncurrentielles (barrières à l'entrée, entente entre pools de mineurs…).

Ces problématiques sont renforcées lorsque les mécanismes de vérification des blocs donnent une prime aux mineurs les plus expérimentés ou avec une plus grosse puissance de calcul… L'incitation à se regrouper s'en trouve augmentée, tout comme la concentration du marché et du même coup les risques concurrentiels sont accrus.

[1] L. Bettoni, « Problématiques soulevées par la blockchain en droit de la concurrence », précité.
[2] Arrêts de la Cour de justice du 21 janvier 2016, Eturas, aff. C-74/14, pt. 42, et du 19 mars 2015, Dole Food et Dole Fresh Fruit Europe/Commission, aff. C-286/13 P, pt. 126.
[3] T. Schrepel, « Collusion by blockchain and smart contracts », Harvard Journal of Law & Technology, Volume 33, Number 1 Fall 2019, p.142 et s.
[4] Autorité de la concurrence, Avis n° 21-A-05 du 29 avril 2021, précité, pt. 414.

IV. Les pratiques reposant sur la *blockchain*, un obstacle à l'application du droit des marchés concurrentiels ?

Le trait commun des comportements évoqués précédemment est que la blockchain n'est qu'un outil permettant de faciliter la mise en œuvre de pratiques anticoncurrentielles connues. Que les pratiques émanent d'opérateurs contrôlant une *blockchain* privée, d'utilisateurs de la blockchain ou bien encore de mineurs, il semble que les qualifications classiques du droit des pratiques anticoncurrentielles soient aptes à saisir et sanctionner ces atteintes au marché.
Sur le fond, la principale difficulté identifiée précédemment concernait le cas où la blockchain était associée à un algorithme. Mais si l'on prend la *blockchain* en tant que telle, elle est un simple registre d'informations, dont l'utilisation par les entreprises peut engendrer des atteintes au marché, lesquelles peuvent être appréhendées par le droit de la concurrence.
Internet, les algorithmes… la *blockchain* n'est que la dernière innovation en date et la plasticité naturelle du droit des marchés concurrentiels lui permet d'appréhender celle-ci sans qu'une évolution textuelle ne soit nécessaire.

Il semble que les principales problématiques liées à la *blockchain* soient des difficultés de nature probatoire pour les autorités de concurrence[1]. Il y a un effet d'opacité pour les tiers à la chaîne de blocs[2], lequel se traduit de deux manières.
D'abord, certains auteurs mettent en avant les difficultés liées aux pseudonymes[3]. En effet, les utilisateurs de la *blockchain* opérant sous pseudonyme, cela complexifierait la tâche des autorités pour remonter aux auteurs de la pratique. Cependant, cette affirmation semble devoir être nuancée. En effet, l'intervention des autorités est liée à la constatation d'une pratique et de ses effets sur un marché. Les auteurs de celle-ci seront donc identifiés sans que le recours à la *blockchain* ne pose réellement de nouvelles difficultés et sans que la question des pseudonymes n'entre en ligne de compte à ce stade.
C'est ensuite la preuve de l'accord de volonté qui semble plus difficile à rapporter lorsque celui-ci est dissimulé par l'utilisation d'une blockchain. Si la *blockchain* est publique, elle pourrait servir de mode de communication indirecte entre concurrents tel que développé précédemment. Dans le cadre de la *blockchain* privée, seuls les utilisateurs autorisés peuvent avoir accès aux informations. Par définition, les autorités de concurrence en sont donc exclues.
Néanmoins – si l'on se concentre sur la question des ententes entre concurrents – la preuve d'un accord de volonté dissimulé via la *blockchain* ne semble pas plus compliquée à rapporter que celle d'une réunion secrète entre concurrents. D'autant plus qu'une *blockchain* privée laissera une trace de l'entente, ce qui pourrait *in fine* faciliter la preuve par les autorités.
Les écueils précités n'apparaissent donc pas insurmontables. En un mot, il semble que les pouvoirs d'enquête attribués aux autorités de concurrence soient à même de parer à ces difficultés.

Si la *blockchain* n'apparait pas comme posant de réel problème au regard du droit de la concurrence, il semble qu'il faille s'inquiéter d'une autre innovation : le « métavers ».
Ce dernier se veut être un monde parallèle, dont le but est de représenter le monde physique de manière virtuelle en y instaurant une capacité créatrice qui n'aura de limite que l'imagination. Ainsi, les deux mondes ayant pour objectifs d'être connectés, on ne peut s'empêcher de voir poindre de nouveaux défis juridiques lorsque des enseignes de la grande distribution, comme Carrefour, achètent pour une somme de 120 Ethereum, soit environs 300 000€, des parcelles de terrain sur The Sandbox, surface virtuelle permettant aux utilisateurs (joueurs), de créer, utiliser mais encore de monétiser leur propre NFT.
On peut dès lors se demander si les règles du droit de la concurrence seront aptes à saisir les pratiques dématérialisées et virtualisées qui ne manqueront pas de découler de l'utilisation du métavers. En clair, le métavers sera-t-il une énième innovation appréhendée sans difficulté par la plasticité du droit de la concurrence, ou celui-ci devra-t-il évoluer ?

Thomas FRANCIA et Alex NICOLLET

[1] V. en ce sens, L. Bettoni, « Problématiques soulevées par la blockchain en droit de la concurrence », précité.
[2] T. Schrepel, « Collusion by blockchain and smart contracts, Harvard Journal of Law & Technology », précité.
[3] V. en ce sens, L. Bettoni, « Problématiques soulevées par la blockchain en droit de la concurrence », précité.