

Objet : Consultation – Droit européen de la concurrence

Campus Cyber est défini sur votre site web comme suit :

« Projet initié par le président de République, le Campus Cyber est le lieu totem de la cybersécurité qui rassemble les principaux acteurs nationaux et internationaux du domaine. Il permet d'accueillir sur un même site des entreprises (grands groupes, PME), des services de l'État, des organismes de formation, des acteurs de la recherche et des associations. Le Campus Cyber met en place des actions visant à fédérer la communauté de la cybersécurité et à développer des synergies entre ces différents acteurs. Des partenariats entre le Campus national et des Campus territoriaux de cybersécurité seront développés dans les prochains mois. À ce jour, plus de 160 acteurs, issus d'une pluralité de secteurs d'activité, ont confirmé leur engagement. »

« Afin de répondre à la menace en matière de cybersécurité, le Campus Cyber prône la mutualisation des ressources. Dans ce cadre, il dispose d'un "Studio des Communs de la cyber" qui facilite la production de Communs de la cyber par les acteurs du Campus Cyber. »

« Les Groupes de Travail du Campus Cyber sont créés à l'initiative de notre écosystème et animés par le Studio des Communs, équipe dédiée à la collaboration des entités engagées auprès du Campus Cyber. La mission de ces groupes de travail est d'identifier les priorités Cyber des entreprises françaises, de mener une réflexion collective sur les réponses à apporter et de créer des livrables appelés "Communs" destinés à aider les entreprises françaises à mieux se protéger des risques cyber. »

Plusieurs exemples de communs sont donnés sur votre site web : *« production de connaissance, spécifications, jeux de données, briques technologiques »*.

Les Communs sont définis sur votre site web comme suit :

Les Communs sont donc, d'après ces descriptions, des contenus textuels, bases de données et logiciels, créés dans le cadre de groupes de travail (ci-après, les « Groupe de Travail »), destinés à aider les entreprises françaises à mieux se protéger des risques cyber.

Mon cabinet ayant été mandaté pour rédiger les licences pour l'exploitation des Communs, la présente étude se bornera à cet aspect de l'activité de Campus Cyber. La question qui se pose dans ce cadre est celle de savoir si le droit européen des ententes est applicable aux activités de recherches et développements des membres de Campus Cyber dans le cadre des Groupes de travail et à la mise à disposition des Communs.

Il s'agira ainsi dans un premier temps de déterminer le marché pertinent **(I)** avant d'analyser un par un les critères des ententes prohibées définis à article 101 §1 du TFUE **(II)**, puis d'étudier les conditions visées dans le règlement d'exemption UE n° 1217-2010 **(III)** et de l'article 101 § 3 du TFUE **(IV)** permettant d'échapper à l'interdiction des ententes.

Bien que la collaboration en matière de recherche et développement constitue l'activité la plus problématique au regard du droit européen des ententes, j'attire votre attention sur le fait que d'autres activités de Campus Cyber pourraient également constituer des activités caractérisant une entente. Une étude complémentaire devrait, selon nous, être réalisée pour vérifier globalement la conformité des activités de Campus Cyber au droit européen des ententes.

J'attire également votre attention sur le fait que les échanges d'informations au sein de structures telles que Campus Cyber font désormais l'objet de dispositions spécifiques dans la directive SRI 2 du 14 décembre 2022¹ :

Article 29 - Accords de partage d'informations en matière de cybersécurité

« 1. Les États membres veillent à ce que les entités relevant du champ d'application de la présente directive et, le cas échéant, les autres entités concernées ne relevant pas du champ d'application de la présente directive puissent échanger entre elles, à titre volontaire, des informations pertinentes en matière de cybersécurité, y compris des informations relatives aux cybermenaces, aux incidents évités, aux vulnérabilités, aux techniques et procédures, aux indicateurs de compromission, aux tactiques adverses, ainsi que des informations spécifiques sur les acteurs de la menace, des alertes de cybersécurité et des recommandations concernant la configuration des outils de cybersécurité pour détecter les cyberattaques, lorsque ce partage d'informations:

- a) vise à prévenir et à détecter les incidents, à y réagir, à s'en rétablir ou à atténuer leur impact;*
- b) renforce le niveau de cybersécurité, notamment en sensibilisant aux cybermenaces, en limitant ou en empêchant leur capacité de se propager, en soutenant une série de capacités de défense, en remédiant aux vulnérabilités et en les révélant, en mettant en œuvre des techniques de détection, d'endiguement et de prévention des menaces, des stratégies d'atténuation ou des étapes de réaction et de rétablissement, ou en encourageant la recherche collaborative en matière de cybermenaces entre les entités publiques et*

¹ Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (Texte présentant de l'intérêt pour l'EEE)

privées.

2. Les États membres veillent à ce que l'échange d'informations ait lieu au sein de communautés d'entités essentielles et importantes ainsi que, le cas échéant, de leurs fournisseurs ou prestataires de services. Cet échange est mis en œuvre au moyen d'accords de partage d'informations en matière de cybersécurité, compte tenu de la nature potentiellement sensible des informations partagées.

3. Les États membres facilitent la mise en place des accords de partage d'informations en matière de cybersécurité visés au paragraphe 2 du présent article. Ces accords peuvent préciser les éléments opérationnels, y compris l'utilisation de plateformes TIC spécialisées et d'outils d'automatisation, le contenu et les conditions des accords de partage d'informations. Lorsqu'ils précisent la participation des autorités publiques à ces accords, les États membres peuvent imposer des conditions en ce qui concerne les informations mises à disposition par les autorités compétentes ou les CSIRT. Les États membres offrent un soutien à l'application de ces accords conformément à leurs politiques visées à l'article 7, paragraphe 2, point h).

4. Les États membres veillent à ce que les entités essentielles et importantes notifient aux autorités compétentes leur participation aux accords de partage d'informations en matière de cybersécurité visés au paragraphe 2, lorsqu'elles concluent de tels accords ou, le cas échéant, lorsqu'elles se retirent de ces accords, une fois que le retrait prend effet.

5. L'ENISA fournit une assistance pour la mise en place des accords de partage d'informations en matière de cybersécurité visés au paragraphe 2 par l'échange de bonnes pratiques et l'apport d'orientations. »

Ces dispositions devront faire, à mon avis, l'objet d'une étude distincte de la présente consultation. Ces dispositions ne concernent en effet pas directement les activités de R&D, objets de la présente consultation. Cela démontre toutefois que l'Union européenne voit d'un bon œil la coopération entre entreprises concernant la cybersécurité et rend donc peu probable une action de la Commission européenne à l'encontre des membres de Campus Cyber du fait de leur collaboration au sein de Campus Cyber.

SOMMAIRE

| | |
|---|-----------|
| I. MARCHÉ PERTINENT | 7 |
| A. Nature du marché pertinent | 7 |
| 1. Solutions-logiciels de cybersécurité | 8 |
| 2. Contenus textuels de cybersécurité | 8 |
| B. Étendue géographique du marché | 9 |
| C. Caractéristiques du marché pertinent | 10 |
| | |
| II. APPLICABILITÉ DU DROIT EUROPÉEN DES ENTENTES..... | 11 |
| A. Accord de volontés entre entreprises..... | 11 |
| B. Accord susceptible d'affecter le commerce entre États membres | 12 |
| C. Accord ayant pour objet ou pour effet d'empêcher, de restreindre ou de fausser le jeu de la concurrence à l'intérieur du marché intérieur | 13 |
| 1. Objet anticoncurrentiel..... | 13 |
| 2. Effet anticoncurrentiel..... | 14 |
| | |
| III. APPLICABILITÉ DU RÈGLEMENT D'EXEMPTION UE N° 1217-2010 | 15 |
| A. Domaine d'application du règlement d'exemption | 16 |
| B. Conditions pour bénéficier du règlement européen | 17 |
| 1. Seuil de parts de marché et durée de l'exemption..... | 17 |
| 2. Absence de restrictions caractérisées | 19 |
| 3. Contraintes particulières | 21 |
| | |
| IV. APPLICABILITÉ SUBSIDIAIRE DE L'EXEMPTION DE L'ARTICLE 101 § 3..... | 23 |

CONCLUSION

1/ Le marché pertinent est présentement le marché mondial des solutions de cybersécurité, représentant un chiffre d'affaires mondial de 150,4 milliards de dollars en 2021.

2/ Le droit des ententes est applicable aux activités de recherches et développement et d'exploitation des Communs par les membres de Campus Cyber.

3/ Toutefois, l'entente entre les membres de Campus Cyber ne devrait pas être considérée comme une entente prohibée. En effet, le contrat-cadre à conclure entre les membres de Campus Cyber permettra de bénéficier de l'exemption prévue par le règlement d'exemption UE 1227-2010. De plus, l'exemption prévue à l'article 101 § 3 du Traité sur le fonctionnement de l'Union européenne pourrait également être invoquée à titre subsidiaire.

I. MARCHE PERTINENT

La définition du marché pertinent est considérée comme une condition préalable à la caractérisation d'une entente.

Dans son glossaire de 2002, la Commission européenne définit le marché pertinent en ce qu'il « *permet d'identifier et de définir le périmètre à l'intérieur duquel s'exerce la concurrence entre entreprises et qui permet d'établir le cadre dans lequel elle applique la politique de la concurrence* ». Son objet principal est ainsi d'identifier les contraintes que la concurrence fait peser sur les entreprises données. La définition du marché permet, entre autres, de calculer les parts de marché, ce qui un intérêt essentiel afin de bénéficier d'une exemption de recherches et développement.

Selon une définition largement admise, le marché pertinent comprend tous les produits et/ou services que le consommateur considère comme interchangeables ou substituables en raison de leurs caractéristiques, de leurs prix et de l'usage auxquels ils sont destinés (substituabilité au niveau de la demande). Il convient également de prendre en compte les produits et/ou les services qui pourraient être facilement commercialisés par d'autres producteurs sans coût de réorientation important, ou par des concurrents potentiels, à un coût raisonnable, et dans un laps de temps limité (substituabilité au niveau de l'offre).

Ce marché est délimité tant au niveau de la nature du marché (1) qu'au niveau de sa dimension géographique (2).

A. Nature du marché pertinent

Les Communs seront, d'après les indications du site internet de Cyber Campus, d'une part, des solutions-logiciels de cybersécurité, comportant des logiciels et des bases de données et, d'autre part, des contenus textuels en lien avec la cybersécurité.

1. Solutions-logiciels de cybersécurité

Les Communs ont vocation à devenir des solutions-logiciels de cybersécurité. La philosophie de Cyber Campus est en effet de mettre en commun des moyens, afin de produire des livrables de cybersécurité, sous la forme de solutions-logiciels permettant de sécuriser les systèmes d'information.

Le marché des solutions-logiciels en matière de cybersécurité est subdivisé en plusieurs domaines :

| Market Segment | 2020 | 2021 | Growth (%) |
|-------------------------------------|----------------|----------------|-------------------|
| Application Security | 3,333 | 3,738 | 12.2 |
| Cloud Security | 595 | 841 | 41.2 |
| Data Security | 2,981 | 3,505 | 17.5 |
| Identity Access Management | 12,036 | 13,917 | 15.6 |
| Infrastructure Protection | 20,462 | 23,903 | 16.8 |
| Integrated Risk Management | 4,859 | 5,473 | 12.6 |
| Network Security Equipment | 15,626 | 17,020 | 8.9 |
| Other Information Security Software | 2,306 | 2,527 | 9.6 |
| Security Services | 65,070 | 72,497 | 11.4 |
| Consumer Security Software | 6,507 | 6,990 | 7.4 |
| Total | 133,776 | 150,409 | 12.4 |

Source: Gartner (May 2021)

2. Contenus textuels de cybersécurité

Les Communs sous forme de contenus textuels pourraient être considérés comme des produits destinés aux formations en matière de cybersécurité.

Nous préconisons cependant de ne pas retenir les contenus textuels dans la

définition du marché pertinent pour les raisons suivantes :

- Cyber Campus n'a pas *a priori* vocation à devenir un centre de formation en matière de cybersécurité. L'objectif est essentiellement de fournir des solutions-logiciels à des tiers pour assurer la sécurité des systèmes d'information.
- La diffusion en ligne d'informations sur la cybersécurité est souvent liée à l'exploitation de solutions-logiciels de cybersécurité. Ces informations peuvent constituer des préalables à l'utilisation de solutions-logiciels de cybersécurité, venir expliciter la manière d'utiliser ces solutions-logiciels ou encore être intégrées à des solutions-logiciels, comme c'est le cas en matière d'elearning. Dans ce cadre, les contenus textuels constituent des produits en lien avec les solutions-logiciels en matière de cybersécurité.
- L'activité liée à la formation en présentiel au sein de Campus Cyber devrait faire, comme indiqué plus haut, l'objet d'une étude séparée, afin de vérifier si, globalement, les activités de Campus Cyber sont susceptibles de caractériser une entente.
- Enfin, les échanges d'information sur la cybersécurité sont encadrés par l'article 29 de la directive SRI, si bien que ces échanges ne sont pas *a priori* susceptibles de constituer une entente prohibée.

Pour l'ensemble de ces raisons, le marché pertinent dans le cadre de la présente étude sera défini comme celui des solutions-logiciels en matière de cybersécurité.

B. Étendue géographique du marché

Le marché géographique en cause comprend le territoire sur lequel les entreprises concernées sont engagées dans l'offre des biens et des services donnés, sur lequel les conditions de concurrence sont suffisamment homogènes et qui peut être distingué de zones géographiques voisines parce que, en particulier, les conditions de concurrence y diffèrent de manière appréciable.

Plusieurs facteurs plaident pour la prise en compte d'un marché mondial :

- L'accès aux solutions-logiciels de cybersécurité se fait aujourd'hui en ligne, ce qui permet d'accéder de la même manière partout dans le monde aux solutions-logiciels.
- Les grands acteurs des solutions-logiciels de cybersécurité proposent aujourd'hui leurs produits partout dans le monde, sans se cantonner à un territoire national.
- Les analyses économiques évoquent aujourd'hui un marché mondial de la cybersécurité.

Ainsi, il y a lieu de considérer que les acteurs économiques des solutions-logiciels de cybersécurité sont engagés sur un marché mondial, globalement homogène.

C. Caractéristiques du marché pertinent

Selon la société américaine d'analyse économique Gartner, le marché des solutions-logiciels de cybersécurité 150,4 milliards de dollars en 2021, avec une croissance de 12,4% entre 2020 et 2021².

En conséquence, dans le cadre de la présente étude, nous considérerons que le marché pertinent est le marché mondial des solutions de cybersécurité, représentant un chiffre d'affaires mondial de 150,4 milliards de dollars en 2021.

À nouveau, je préconise de réaliser une étude globale des activités de Campus Cyber pour savoir à quel marché pertinent ces différentes activités peuvent être rattachées. Il serait judicieux, dans cette optique, de faire appel à un expert en économie de la concurrence, afin de faire une étude détaillée des marchés pertinents potentiellement impactés par les activités de Campus Cyber.

² Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed \$150 Billion in 2021, STAMFORD, Conn. May 17, 2021: <https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem>

II. APPLICABILITÉ DU DROIT EUROPÉEN DES ENTENTES

L'article 101 §1 du Traité sur le fonctionnement de l'Union européenne (« TFUE ») dispose que :

« Sont incompatibles avec le marché intérieur et interdits, tous accords entre entreprises, toutes décisions d'associations d'entreprises et toutes pratiques concertées, qui sont susceptibles d'affecter le commerce entre États membres et qui ont pour objet ou pour effet d'empêcher, de restreindre ou de fausser le jeu de la concurrence à l'intérieur du marché intérieur ».

Trois critères sont ainsi nécessaires pour qu'une entente soit prohibée en droit européen :

- Un accord de volonté entre entreprises
- Un accord susceptible d'affecter le commerce entre États membres
- Un accord ayant pour objet ou pour effet d'empêcher, de restreindre ou de fausser le jeu de la concurrence à l'intérieur du marché intérieur.

A. Accord de volontés entre entreprises

Concernant l'accord de volontés entre entreprises, le Tribunal de l'Union européenne rappelle que l'accord, au sens de l'article 101 du TFUE, suppose uniquement que les entreprises en cause aient exprimé leur volonté commune de se comporter sur le marché d'une manière déterminée.

En l'espèce, il existe plusieurs accords de volonté entre les membres de Cyber Campus :

- Les statuts de Campus Cyber constituent un accord de volontés entre entreprises. Ces statuts encadrent l'ensemble des activités de Campus Cyber. Ils ne nous intéressent ici que dans la mesure où ils prévoient la réalisation d'activités de recherches et développement et la création de Communs.

- Le contrat-cadre à rédiger afin d'encadrer la formation des Groupes de travail, le travail en leur sein et l'exploitation des résultats.

B. Accord susceptible d'affecter le commerce entre États membres

Concernant l'atteinte à la concurrence, selon un principe bien établi, une entente ne tombe sous le coup des interdictions du Traité **que si elle produit des effets d'une certaine ampleur sur la concurrence (effet sensible)**. La Commission européenne, dans la décision *Völk-Vervaecke* du 9 juillet 1969, a pu considérer que :

« Pour être susceptible d'affecter le commerce entre États membres, l'accord doit, sur la base d'un ensemble d'éléments objectifs de droit ou de fait, permettre d'envisager avec un degré de probabilité suffisant qu'il puisse exercer une influence directe ou indirecte, actuelle ou potentielle sur les courants d'échange entre États membres dans un sens qui pourrait nuire à la réalisation des objectifs d'un marché unique entre États ; que pour le surplus, la prohibition de l'article 101, § 1 du TFUE ne peut s'appliquer qu'à la condition que l'accord en cause ait pour objet ou pour effet d'empêcher, de restreindre ou de fausser le jeu de la concurrence dans le marché commun. »

Dans sa communication du 27 avril 2004, la Commission a établi une présomption positive selon laquelle les accords ou pratiques qui, de par leur nature même, sont susceptibles d'affecter le commerce entre États membres, par exemple parce qu'ils concernent des importations ou des exportations, ou mettent en cause plusieurs États membres, affectent le commerce de façon sensible, dès lors que le chiffre d'affaires réalisé par les parties avec les produits contractuels **excède un seuil de 40 millions d'euros, ou que leur part de marché est supérieure au seuil de 5 %**.

En l'espèce, Campus Cyber rassemble la plupart des grandes entreprises françaises et l'État pour permettre une activité commune de recherche et développement dans le domaine de la cyber. Au regard de l'importance des acteurs membres de Campus Cyber (notamment Air-France, Airbus, Axa, BNP Paribas, Bolloré, Bouygues, SNCF, Total Energies...), cette condition est largement remplie en ce que seulement Total Energies possède un chiffre d'affaire estimé à 250 000 millions d'euros pour 2021.

Le manifeste de Campus Cyber indique d'ailleurs clairement que le groupement vise à « *protéger la société et faire rayonner l'excellence française en réunissant les acteurs de la sécurité numérique autour d'un lieu totem.* » L'idée de rayonner implique ici un effet hors du territoire strictement français.

Les membres de Campus Cyber ont ainsi conclu un accord susceptible d'affecter le commerce entre États membres.

C. Accord ayant pour objet ou pour effet d'empêcher, de restreindre ou de fausser le jeu de la concurrence à l'intérieur du marché intérieur

La troisième et dernière condition concerne l'objet ou l'effet restrictif de concurrence (effet anticoncurrentiel). Aux termes du paragraphe 1 de l'article 101 du TFUE, les ententes prohibées sont celles qui ont pour objet ou pour effet de porter atteinte à la concurrence. Il y a là une alternative, comme il résulte de la conjonction « ou », si bien qu'il suffit que l'entente ait soit pour objet, soit pour effet de porter atteinte à la concurrence pour être condamnable.

L'objet restrictif de concurrence est relatif à l'intention, par les parties, de fausser le jeu de la concurrence en concluant l'entente, il n'est pas nécessaire d'attendre qu'elle ait produit quelque effet concret, ni même d'établir la réalité de cet effet une fois qu'il s'est produit.

1. Objet anticoncurrentiel

En l'espèce, les statuts de Campus Cyber indiquent que l'organisation vise à :

« Fédérer les acteurs publics et privés de la sécurité des systèmes d'information et de favoriser les échanges dans le cadre de projets dans le domaine de la sécurité des systèmes d'information au sein d'un lieu baptisé campus cyber dans une culture commune d'innovation ouverte. »

« La gestion d'un incubateur dans le domaine de la sécurité des systèmes d'information »

« Le développement de la sécurité des systèmes d'information grâce à des travaux de recherches et développement »

« L'émergence de ressources ouvertes dans le domaine de la sécurité des systèmes d'information »

« Le soutien de la réunion de toute personne (acteurs industriels, institutions publiques, instituts de formation et laboratoires de recherche, PME et start-ups, etc.) souhaitant être active dans l'Union européenne dans le domaine de la sécurité des systèmes d'information, souhaitant mettre en commun ses connaissances, ses ressources ou ses activités, y compris dans un but autre que le partage de bénéfices financiers, afin de favoriser l'émergence et l'adoption opérationnelle de Communs. »

« La contribution à la création et au développement des Communs autour de la sécurité des systèmes d'information au travers de modèles ouverts. »

L'objet de Campus Cyber est ainsi anticoncurrentiel : l'organisation vise clairement à rassembler des acteurs de différents marchés, et notamment celui du marché des solutions-logiciels de cybersécurité, afin de travailler en commun pour la création de Communs.

2. Effet anticoncurrentiel

Pour qu'un accord soit restrictif par ses effets, il doit affecter la concurrence réelle ou potentielle à un point tel qu'il soit possible de prévoir avec quelque vraisemblance qu'il aura, sur le marché en cause, des effets négatifs sur les prix, la production, l'innovation, la diversité ou la qualité des produits ou service. Des effets défavorables sur la concurrence peuvent encore être relevés lorsque les parties, individuellement ou conjointement, possèdent ou obtiennent un certain pouvoir de marché et que l'accord contribue à la création, au maintien ou au renforcement de ce pouvoir, ou

permet aux parties de l'exploiter³.

En l'espèce, même si les membres de Campus Cyber n'ont pas pour objectif de fausser la concurrence, la création et la mise à disposition de Communs sont susceptibles de produire des effets anticoncurrentiels. Étant donné la taille et le nombre des acteurs déjà membres de Campus Cyber, la simple création et publication des Communs par les membres pour leur propre cyber sécurité aura un effet non négligeable sur le marché de la cybersécurité.

L'accord conclu entre les membres de Cyber Campus a donc pour objet actuel et pour effet potentiel d'empêcher, de restreindre ou de fausser le jeu de la concurrence à l'intérieur du marché intérieur.

Les trois conditions de l'article 101 §1 du TFUE étant réunies, les activités de recherches et développement de Cyber Campus constituent une entente.

Toutefois, si Campus Cyber respecte le règlement d'exemption relatif aux activités de recherches et développement, alors cette entente ne sera pas prohibée.

III. APPLICABILITÉ DU RÈGLEMENT D'EXEMPTION UE N° 1217-2010

Le droit européen des ententes admet – fort heureusement – la possibilité pour plusieurs entreprises de se regrouper, afin de mener ensemble des activités liées à la recherche et au développement. Dès lors que ces activités entrent dans le champ d'application du règlement d'exemption UE n° 1217-2010 (A) et répondent à ses conditions de mises en œuvre (B), alors l'entente n'est pas prohibée⁴.

J'attire votre attention sur le fait que le règlement d'exemption UE n° 1217-2010

³ *Comm. CE, communication n° 2004/C 101/08, 27 avr. 2004, pt 25*

⁴ En principe, l'application du droit français des ententes et du droit européen des ententes est cumulative. Cependant, le § 2 de l'article 3, Règlement n° 1/2003, tempère quelque peu les effets de l'application cumulative, au moins en matière d'entente. En effet, il y est précisé que « l'application du droit national de la concurrence ne peut pas entraîner l'interdiction d'accords, de décisions d'associations d'entreprises ou de pratiques concertées qui sont susceptibles d'affecter le commerce entre États membres, mais qui n'ont pas pour effet de restreindre la concurrence au sens de l'article 81, § 1 du Traité, ou qui satisfont aux conditions énoncées à l'article 81, § 3, du Traité ou qui sont couverts par un règlement ayant pour objet l'application de l'article 81, § 3 du Traité ». Le droit français ne peut donc pas rendre l'entente en question illicite alors qu'elle entre dans le champ d'application et

expirera en principe le 30 juin 2023. Il devrait en principe être remplacé par un nouveau règlement d'exemption, reprenant en les améliorant, les dispositions du règlement d'exemption actuel. Il conviendra à ce moment-là de réaliser une étude complémentaire pour savoir s'il est nécessaire de modifier les stipulations du contrat-cadre.

A. Domaine d'application du règlement d'exemption

Le règlement d'exemption créé une exemption au profit des accords de recherches et de développement lorsque les parties assurent des activités conjointes de recherche et de développement de produits ou de technologies et une exploitation en commun de leurs résultats ou assurent l'une ou l'autre de ces activités isolément.

Ainsi, les accords visés par l'exemption sont très diversifiés, puisqu'il s'agit des accords dans lesquels les parties assurent :

- soit des activités conjointes de recherche et de développement de produits ou de technologies contractuels ainsi que l'exploitation en commun de leurs résultats (art. 1er, a, i),
- soit l'exploitation en commun des résultats issus de la recherche et du développement de produits ou de technologies contractuels effectués conjointement en vertu d'un accord conclu antérieurement par les mêmes parties (art. 1er, a, ii),
- soit des activités conjointes de recherche et de développement de produits ou de technologies contractuels, à l'exclusion de l'exploitation en commun de leurs résultats (art. 1er, a, iii),
- soit des activités rémunérées de recherche et de développement de produits ou de technologies contractuels ainsi que l'exploitation en commun de leurs résultats (art. 1er, a, iv),
- soit l'exploitation en commun des résultats issus de la recherche et du développement rémunéré de produits ou de technologies contractuels en vertu d'un accord conclu antérieurement par les mêmes parties (art. 1er, a, v),
- soit enfin des activités rémunérées de recherche et de développement de produits ou de technologies contractuels, à l'exclusion de l'exploitation en

répond aux conditions du règlement d'exemption.

commun de leurs résultats (art. 1er, a, vi).

Sous réserve des entretiens à réaliser avec les membres de Campus Cyber, la collaboration envisagée par les statuts de Campus Cyber aux fins de R&D et la mise à disposition de Communs entrent bien dans le champ d'application du règlement d'exemption.

B. Conditions pour bénéficier du règlement d'exemption

Les conditions de l'exemption sont : le non-franchissement d'un certain seuil établi en parts de marché (1), l'absence de restrictions caractérisées (2) et diverses contraintes particulières propres à ce type d'accord (3).

1. Seuil de parts de marché et durée de l'exemption

a. Absence d'entreprises concurrentes dans le Groupe de Travail

L'article 4.1 du règlement d'exemption dispose que :

« Lorsque les parties ne sont pas des entreprises concurrentes, l'exemption prévue à l'article 2 s'applique pendant toute la durée de la recherche et du développement. En cas d'exploitation en commun des résultats, l'exemption continue de s'appliquer pendant une période de sept ans à compter de la date de la première mise sur le marché des produits ou des technologies contractuels au sein du marché intérieur. »

L'article 4.3 du règlement d'exemption dispose que :

« À l'issue de la période visée au paragraphe 1, l'exemption continue de s'appliquer tant que la part de marché cumulée des parties n'est pas supérieure à 25 % du marché du produit ou de la technologie en cause. »

L'article 7 du règlement d'exemption dispose que :

« d) Si la part de marché visée à l'article 4, paragraphe 3, est initialement inférieure ou égale à 25 % mais franchit ensuite ce seuil sans dépasser 30 %, l'exemption prévue à l'article 2 continue de s'appliquer pendant deux années civiles consécutives suivant l'année au cours de laquelle le seuil de 25 % a été dépassé pour la première fois

e) si la part de marché visée à l'article 4, paragraphe 3, est initialement inférieure ou égale à 25 % mais dépasse ensuite 30 %, l'exemption prévue à l'article 2 continue à s'appliquer pendant une année civile suivant l'année au cours de laquelle le niveau de 30 % a été dépassé pour la première fois ».

Ainsi, lorsqu'il n'y a pas d'entreprises concurrentes dans le même Groupe de Travail, il sera nécessaire de distinguer selon deux situations :

- Si le Commun est simplement placé sous une licence libre en ligne, cette mise à disposition doit s'analyser a priori comme une renonciation à exercer les droits de propriété intellectuelle. Dans ce cas, il n'y a pas à proprement parler d'exploitation du résultat. L'exemption s'applique ainsi pendant la durée de la R&D, puis n'a plus vocation à s'appliquer, le Commun étant libre de droits et librement utilisable, sans qu'une collaboration entre les parties persiste.
- Si, en revanche, le Commun n'est pas placé sous licence libre en ligne ou s'il est placé sous licence libre en ligne mais que les membres réalisent des actes de maintenance, une collaboration persistera entre les membres pour l'exploitation du Commun. Dans ce cas, l'exemption s'appliquera pendant la durée de la R&D et :
 - o pendant une durée de 7 ans à compter du début de l'exploitation du Commun si les parts de marché cumulées des membres du Groupe de Travail sur le marché de solutions-logiciels de cybersécurité dépassent 25% ;
 - o sans limite de durée si les parts de marché cumulées des membres du Groupe de Travail sur le marché mondial de solutions-logiciels de cybersécurité restent inférieures à 25%. En cas de dépassement du seuil de 25%, l'exemption est encore valable 2 ans tant que les parts de

marché restent inférieures à 30%. En cas de dépassement du seuil de 30%, l'exemption reste valable 1 an.

b. Présence d'entreprises concurrentes dans le Groupe de Travail

L'article 4.3 du règlement d'exemption dispose que :

« Lorsque deux ou plusieurs parties sont des entreprises concurrentes, l'exemption prévue à l'article 2 s'applique pendant la période visée au paragraphe 1 du présent article, à condition qu'à la date de conclusion de l'accord de recherche et de développement,

a) la part de marché cumulée des parties ne dépasse pas 25 % du marché du produit ou de la technologie en cause, lorsqu'il s'agit des accords de recherche et de développement visés à l'article 1er, paragraphe 1, point a) i), ii) ou iii); ou
b) la part de marché cumulée de la partie qui finance et de l'ensemble des parties avec lesquelles la partie qui finance a conclu des accords de recherche et de développement concernant les mêmes produits ou technologies contractuels ne dépasse pas 25 % du marché du produit ou de la technologie en cause, lorsqu'il s'agit des accords de recherche et de développement visés à l'article 1er, paragraphe 1, point a) iv), v) ou vi). »

Sans entrer dans le détail à ce stade, retenons que, lorsque des entreprises concurrentes sont dans le même Groupe de Travail, elles ne pourront bénéficier de l'exemption, pendant la durée de la R&D et jusqu'à 7 ans après de début de l'exploitation, que si leur part de marché sur le marché mondial de solutions-logiciels de cybersécurité est inférieure à 25% au moment de la formation du Groupe de Travail.

2. Absence de restrictions caractérisées

L'article 5 du règlement d'exemption prévoit que l'exemption ne s'applique pas en cas de restrictions caractérisées, concernant notamment la fixation des prix et l'obligation de ne pas réaliser de ventes actives :

« L'exemption prévue à l'article 2 ne s'applique pas aux accords de recherche et de développement qui, directement ou indirectement, isolément ou cumulés avec d'autres facteurs sous le contrôle des parties, ont pour objet:

c) la fixation des prix pour la vente du produit contractuel à des tiers ou du montant de la licence sur les technologies contractuelles octroyée à des tiers, à l'exception de la fixation des prix appliqués aux clients directs ou de la fixation du montant de la licence appliqué aux preneurs directs de licences lorsque l'exploitation en commun des résultats s'étend à la distribution conjointe des produits contractuels ou à la concession conjointe de licences relatives aux technologies contractuelles au sens de l'article 1^{er}, paragraphe 1, point m) i) ou ii);

e) l'obligation de ne pas réaliser de ventes actives des produits ou des technologies contractuels, ou de les limiter, sur les territoires ou à la clientèle qui n'ont pas été attribués exclusivement à l'une des parties par voie de spécialisation dans l'exploitation ».

a. Fixation des prix

La liberté de fixation des prix par les opérateurs du marché est un principe cardinal du droit économique européen. Il est traduit ici dans l'interdiction, dans l'accord entre les entreprises, de fixer le montant auquel le produit ou la technologie issus des activités de R&D sera commercialisé par les revendeurs. Rien n'interdit en revanche aux membres du Groupe de Travail de se mettre d'accord entre eux sur le prix de commercialisation par les membres du Groupe de Travail eux-mêmes du produit ou de la technologie à leurs clients directs.

Dans le cas présent, la mise à disposition gratuite en ligne du Commun pourrait s'analyser comme une fixation du prix. Toutefois, cette fixation n'est valable que pour les membres du Groupe de Travail. Rien n'interdit à un tiers de vendre le Commun, par exemple en faisant payer son accès pour le téléchargement en ligne ou en forçant l'internaute à télécharger le Commun avec un autre produit ou une autre technologie.

Les licences libres ne devront donc pas avoir pour effet de restreindre la possibilité, pour les personnes qui accèdent au Commun, de librement fixer le prix de la revente.

b. Obligation de ne pas réaliser de ventes actives

La philosophie du règlement d'exemption tient au fait que les ententes, qui sont en principe prohibées, car elles ont un effet néfaste pour le consommateur final, peuvent être bénéfiques si elles permettent au consommateur de bénéficier de R&D pour accéder à de nouveaux produits ou à des produits améliorés.

L'interdiction de prévoir, dans l'accord entre entreprises, l'obligation de ne pas réaliser de ventes actives des produits ou des technologies contractuelles doit être comprise dans cette optique. Le produit et la technologie doivent pouvoir être accessibles pour les consommateurs sur le marché en cause pour justifier l'entente.

Or, dans le cas présent, si le Commun est mis à libre disposition en ligne, cet objectif est bien rempli. Le terme de « vente » de l'article 5 e) du règlement d'exemption devrait donc être compris, selon nous, non pas comme une opération nécessairement payante, mais comme une mise à disposition sur le marché au profit des consommateurs.

L'article 5 e) du règlement d'exemption ne fait donc pas obstacle, selon l'interprétation proposée, à la mise à disposition gratuite en ligne des Communs.

3. Contraintes particulières

Les obligations mentionnées ci-dessus devront être retranscrites en détail dans le contrat-cadre selon les options définies après discussion avec les membres. À ce stade de la réflexion, nous en retiendrons les idées essentielles.

a. Accès aux résultats

Les résultats sont définis par le règlement d'exemption comme les technologies contractuelles (technologies ou procédés issu(e)s des activités conjointes de recherche et de développement), les produits contractuels (produits issus des activités conjointes de recherche et de développement, ou fabriqués ou fournis en utilisant les technologies contractuelles), ainsi que les droits de propriété intellectuelle sur ces technologies et produits.

L'article 3.2 du règlement d'exemption dispose que :

« L'accord de recherche et de développement doit stipuler que toutes les parties ont un accès illimité aux résultats finaux des travaux conjoints ou rémunérés de recherche et de développement, y compris aux droits de propriété intellectuelle et au savoir-faire qui en découlent, à des fins d'activités de recherche et de développement ou d'exploitation complémentaires, dès qu'ils sont disponibles. Lorsque les parties limitent leurs droits d'exploitation des résultats, conformément au présent règlement, en particulier lorsqu'elles se spécialisent dans l'exploitation, l'accès aux résultats dans un but d'exploitation peut être limité en conséquence. Les instituts de recherche, les centres universitaires ou les entreprises qui exécutent des travaux de recherche et de développement sur une base commerciale sans normalement participer à l'exploitation des résultats, peuvent en outre convenir de limiter leur utilisation desdits résultats à des fins de recherches complémentaires. L'accord de recherche et de développement peut prévoir que les parties s'indemnisent pour l'accès consenti aux résultats dans un but de travaux de recherche complémentaires ou d'exploitation, mais le montant de l'indemnisation ne doit pas être tel qu'il empêche en réalité l'accès à ces résultats. »

Cette disposition impose que le contrat-cadre à rédiger permette à tous les membres du Groupe de Travail d'avoir accès aux résultats obtenus dans le cadre des travaux de ce Groupe de Travail dans le but de mener des travaux de recherche complémentaire ou de réaliser une exploitation complémentaire des résultats.

b. Accès au savoir-faire

Le savoir-faire est défini par le règlement d'exemption comme « un ensemble secret, substantiel et identifié d'informations pratiques non brevetées, résultant de l'expérience et testées. »

L'article 3.3 du règlement d'exemption dispose que :

« Sans préjudice du paragraphe 2, si l'accord de recherche et de développement ne concerne que les activités conjointes ou rémunérées de recherche et de développement, il doit stipuler que chacune des parties doit avoir accès au savoir-faire préexistant des autres parties si ce savoir-faire lui est indispensable aux fins de l'exploitation des résultats. L'accord de recherche et de développement peut prévoir que les parties s'indemnisent pour l'accès consenti à leur savoir-faire préexistant, mais le montant de l'indemnisation ne doit pas être tel qu'il empêche en réalité l'accès à ce savoir-faire. »

Cette disposition impose que le contrat-cadre à rédiger permette à tous les membres du Groupe de Travail d'avoir accès aux savoir-faires préexistants des autres parties, si l'accès à ces savoir-faire est indispensable pour l'exploitation des résultats, c'est-à-dire la production ou la distribution des produits contractuels et/ou l'utilisation des technologies contractuelles.

IV. APPLICABILITÉ SUBSIDIAIRE DE L'EXEMPTION DE L'ARTICLE 101 § 3

Dans l'hypothèse où le règlement d'exemption ne s'appliquerait pas, Campus Cyber pourrait alors bénéficier d'une sorte de filet de secours. L'article 101 §3 du TFUE assortit le principe de prohibition des ententes anticoncurrentielles d'une possibilité d'exemption générale fondée sur la contribution au progrès économique.

Selon l'article 101 §3 du TFUE :

« Les dispositions du paragraphe 1 peuvent être déclarées inapplicables à tout accord ou catégorie d'accords entre entreprises, à toute décision ou catégorie de décisions d'associations d'entreprises et à toute pratique concertée ou catégorie de pratiques concertées qui contribuent à améliorer la production ou la distribution des produits et à promouvoir le progrès technique ou économique, tout en réservant aux utilisateurs une partie équitable du profit qui en résulte, sans imposer aux entreprises intéressées des restrictions qui ne sont pas indispensables pour atteindre ces objectifs, ni donner à des entreprises la possibilité, pour une partie des produits en cause, d'éliminer la concurrence ».

Quatre conditions cumulatives sont nécessaires pour que l'exemption puisse jouer. Ces conditions sont cumulatives⁵ :

1. Il faut d'abord démontrer que l'accord, la décision ou la pratique contribue à améliorer la production ou la distribution des produits ou à promouvoir le progrès technique ou économique. Ce progrès doit produire des effets objectifs et doit présenter une portée européenne. L'amélioration peut se traduire par une fabrication de meilleure qualité, grâce notamment à des accords de licence de brevet permettant la généralisation de techniques nouvelles⁶, ou à des accords de recherche en commun favorisant l'invention ou la mise au point de produits nouveaux⁷.

2. Il faut ensuite que cela soit réalisé tout en réservant aux utilisateurs une partie équitable du profit qui en résulte. La jurisprudence considère que l'entente qui apporte un avantage réel au public remplit cette condition ; elle pourra donc être exemptée sur le fondement de « l'intérêt public ».

3. Il ne faut pas imposer aux entreprises intéressées des restrictions qui ne sont pas indispensables pour atteindre ces objectifs. Les restrictions imposées

⁵ Comm. CE, communication n° 2004/C 101/07, pt 46

⁶ Comm. CE, déc. n° 72/237/CE, 9 juin 1972, Davidson-Rubber, aff. IV/17.545 et a. : JOCE n° L 143, 23 juin 1972

⁷ Comm. CE, déc. 17 juill. 1968, ACEC-Berliet : JOCE n° L 201, 12 août 1968. – Comm. CE, déc. 22 déc. 1987, Rich Products Jus-Rol : JOCE n° L 69, 15 mars 1988, p. 21, préc., n° 126, à propos des gains d'efficacité dus à une licence de savoir-faire

aux entreprises n'outrepassent pas les limites de l'indispensable pour obtenir les résultats escomptés. Les restrictions de concurrence imposées doivent être limitées au strict nécessaire pour atteindre l'objectif visé.

4. Il ne faut pas, enfin, donner à des entreprises la possibilité, pour une partie substantielle des produits en cause, d'éliminer la concurrence. Cette condition implique l'appréciation du degré de concurrence qui existait avant l'accord et l'incidence de ce dernier sur la concurrence. En d'autres termes, il convient de mesurer la réduction de concurrence induite par l'accord.

Sans entrer ici dans le détail de chacune de ces conditions, on notera que la mise à disposition sous licence libre de Commun de la cybersécurité correspond bien à la philosophie de l'article 101 § 3 du TFUE. Il s'agit bien, en effet de promouvoir le progrès technique (1) au profit d'utilisateur partout dans le monde (2) sans imposer aux entreprises de restriction étrangère à l'objectif de cybersécurité (3) et sans risque a priori d'éliminer la concurrence sur le marché mondial de la cybersécurité (4).

Dans l'hypothèse où, malgré les efforts de Campus Cyber pour satisfaire au règlement d'exemption en matière de R&D, certaines conditions ne seraient pas remplies, les membres Campus Cyber pourraient invoquer les dispositions de l'article 101 § 3 du TFUE afin de démontrer que l'entente entre eux ne constitue pas une entente prohibée.

Je me tiens à votre disposition pour évoquer oralement la présente consultation.

Bien cordialement,

Étienne Deshoulières
Avocat au barreau de Paris

