Haut Comité Juridique
de la Place financière de Paris

RAPPORT SUR LE CLOUD BANCAIRE : ÉTAT DES LIEUX ET PROPOSITIONS

du Haut Comité Juridique
de la Place Financière de Paris

Mai 2021

9 rue de Valois 75001 Paris - Tél.: 33 (0)1 42 92 20 00 - hautcomite@hcjp.fr - www.hcjp.fr

RAPPORT SUR LE CLOUD EN MATIÈRE BANCAIRE : ÉTAT DES LIEUX ET PROPOSITIONS DU HAUT COMITÉ JURIDIQUE DE LA PLACE FINANCIÈRE DE PARIS

Face à l'engouement des acteurs pour la technologie de l'informatique en nuage (plus connue sous le vocable anglais *Cloud computing*)[1] et aux enjeux que son utilisation présente pour l'industrie financière et, parmi elle, la profession bancaire, le Haut Comité Juridique de la Place Financière de Paris (HCJP) s'est saisi de ce sujet et a constitué à cet effet, en février 2020, un groupe de travail[2] chargé d'analyser ce phénomène au regard de l'architecture actuelle des règles applicables au secteur bancaire en matière prudentielle et de supervision. Initialement centré sur les questions liées au rapport de force contractuel entre les utilisateurs (les banques) et les fournisseurs de cette technologie (les prestataires informatiques), le groupe de travail a tenu compte des évolutions prochaines de la législation européenne dans le cadre de la nouvelle stratégie de la Commission européenne en matière de finance numérique pour le secteur financier de l'Union européenne,[3] et du train de mesures qui la met en œuvre. Parmi ces mesures, le groupe de travail a identifié le projet de règlement européen sur la résilience opérationnelle numérique du secteur financier (DORA), en cours de discussion au sein du Conseil,[4] comme répondant, en partie, aux principaux enjeux liés à l'utilisation du Cloud par les banques et dès lors a concentré ses efforts sur l'analyse de ce projet de règlement.

Le groupe de travail est bien conscient du caractère limité de l'exercice auquel il s'est livré.

D'une part, l'analyse a été conduite sous l'angle du seul secteur bancaire et ne prend donc pas en compte le point de vue d'autres acteurs du secteur financier au sens large (tels que les entreprises d'investissement, sociétés de gestion de portefeuille, entreprises d'assurance, etc.), qui tombent également, en qualité d'« entités financières »,[5] dans le champ du projet de règlement DORA, étant précisé, au surplus, que ce projet de texte n'est d'ailleurs pas confiné aux services de Cloud, mais embrasse tous les services de technologie de l'information et de la communication (TIC).

---

[1] *Voir la définition du Cloud en Annexe n° 2.*

[2] *La composition du groupe de travail figure en Annexe n° 1.*

[3] *Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions sur une stratégie en matière de finance numérique pour l'UE du 23 septembre 2020, COM(2020) 591.*

[4] *Au moment de la rédaction du présent rapport, sous la présidence portugaise (https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:52020PC0595).*

[5] *Voir à cet égard les contributions des acteurs des différentes industries sectorielles des services financiers reçues par la Commission européenne à propos du projet de règlement DORA.*

D'autre part, l'analyse ne porte pas sur les dispositions du règlement consacrées à la résilience opérationnelle des entités financières, qui en constituent l'un des piliers.

Enfin, pour pertinent qu'il soit, le projet de règlement DORA ne répond pas à tous les enjeux soulevés par l'utilisation du Cloud (et plus généralement, des TIC) par les acteurs du secteur financier, tels qu'ils sont décrits dans le présent rapport (voir la Section 1 - Enjeux liés au Cloud bancaire).[6] D'autres textes en vigueur et des projets législatifs en cours d'examen cherchent plus particulièrement à répondre à ces enjeux (tels que la directive NIS[7] qui est en cours de revue,[8] le RGPD, ainsi que les projets de règlements « *Digital Services Act* »[9] et « *Digital Market Act* »[10]).[11] Le groupe de travail a souhaité concentrer ses efforts sur le projet de règlement DORA compte tenu de la pertinence des sujets abordés par ce texte au regard de l'angle d'analyse qui a sous-tendu les travaux du groupe de travail et qui est décrit au début de cette introduction. Par conséquent, le groupe de travail n'a pas, pour l'heure, procédé à une analyse détaillée de ces textes ou projets de textes.[12]

Après un rappel des enjeux liés au Cloud bancaire (Section 1 - Enjeux liés au Cloud bancaire) et du cadre réglementaire existant (Section 2 - L'appréhension du Cloud par la réglementation bancaire :

---

[6] *À savoir, en particulier, enjeux liés, d'une part, à la structure oligopolistique du marché de la prestation de services de cloud, d'autre part, à l'extraterritorialité des législations procédurales et répressives américaines et à la souveraineté de l'UE en matière de protection des données et, enfin, à la sécurité informatique.*

[7] *Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (Directive on Network and Information Security, ou « **Directive NIS** »). Cette directive définit une série d'exigences en matière de sécurité des réseaux et de l'information (notamment en matière de cybersécurité) qui s'appliquent aux « Fournisseurs de Services Numériques » (FSN) et aux « Opérateurs de services essentiels » (OSE). Cette directive concerne notamment les entreprises des secteurs de l'énergie, des transports, de la banque, des marchés financiers, de la santé, de la distribution d'eau potable et des infrastructures numériques. Elle est transposée en France par la loi n° 2018-133 du 26 février 2018 portant diverses dispositions n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, le décret d'application n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique, l'arrêté du 13 juin 2018 fixant les modalités de déclaration des incidents et, enfin, l'arrêté du 14 septembre 2018 fixant les règles de sécurité et les délais mentionnés à l'article 10 du décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique.*

[8] *https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union; proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (NIS II).*

[9] *Voir note de bas de page n° 86, en page 26.*

[10] *Voir note de bas de page n° 88, en page 26.*

[11] *De nombreux autres textes sont en préparation. Voir par exemple : E. Jouffin, La convergence des préoccupations dans la divergence des moyens, Banque & Droit n° 196 mars-avril 2021, p. 4, qui évoque un « brouhaha réglementaire ».*

[12] *Au surplus, il convient de noter que la Commission européenne a complété ses travaux en matière de résilience informatique spécifiquement dans le secteur financier avec la publication, le 24 septembre 2020, d'un nouveau projet de directive: proposal for a directive of the European Parliament and of the Council amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341 (COM(2020) 596 final), qui vise, notamment, à mettre en cohérence les directives précitées avec le Règlement DORA.*

entre morcellement et hétérogénéité), le présent rapport détaille les problématiques auxquelles les établissements sont aujourd'hui confrontés, dans le cadre de leur relation avec les Prestataires TIC. À ce titre, le présent rapport propose une analyse critique synthétique de certaines dispositions du projet de règlement DORA et formule des propositions de modification (Section 3 - Vers un nouveau paradigme réglementaire en matière d'externalisation informatique dans le secteur financier : le Règlement DORA).

SYNTHÈSE DES CONCLUSIONS DU GROUPE DE TRAVAIL

Enjeux liés au Cloud bancaire

Le Cloud est un mode d'organisation et de gestion informatique des entreprises permettant l'accès et l'utilisation, à distance, par ces entreprises, de services informatiques standardisés qui leur sont fournis par des prestataires de services informatiques. La technologie du Cloud permet à ces prestataires de mettre à disposition de leurs clients des services de fourniture d'infrastructures, de plateforme informatique ou encore d'applications ou de logiciels. Elle s'est progressivement déployée dans le secteur bancaire et financier mondial, d'abord dans les fonctions « support », puis marginalement dans les fonctions ou services relevant du cœur des métiers bancaires, accompagnant le développement des néo banques et des acteurs de l'*open banking*, où elle prend une place grandissante dans le parcours client. Il en résulte une tendance irréversible de transformation numérique des banques au moyen des solutions de Cloud et en raison des bénéfices qui en résultent, tant pour les banques en termes de gestion de leurs ressources techniques, que pour la clientèle.

Toutefois, leur déploiement à grande échelle au cœur même des métiers bancaires et financiers, qui implique la transmission à des tiers non soumis à supervision d'informations et données sensibles concernant les clients, se heurte à plusieurs difficultés qui mettent en exergue la situation de dépendance croissante des banques à l'égard d'un faible nombre de Prestataires de Cloud, essentiellement américains et asiatiques, auxquels la réglementation de la profession bancaire ne s'applique pas, par définition. Ainsi, la structure oligopolistique du marché du Cloud, doublée d'une dépendance technologique des banques vis-à-vis de l'expertise des Prestataires de Cloud, entraîne une profonde interconnexion avec l'ensemble du système financier et est susceptible d'inverser la relation de pouvoir traditionnelle entre le client et le prestataire de services. Ce phénomène de concentration du marché du Cloud met également en lumière l'existence de risques de comportements anticoncurrentiels sur les marchés numériques. Plusieurs projets de réforme du droit de la concurrence sur ce sujet ont été initiés ou sont en discussion dans les différents territoires concernés : la Commission européenne a publié récemment le *Digital Services Act* et le *Digital Market Act* qui ont pour objectif d'assurer un environnement concurrentiel équitable dans le secteur des services numériques.

Comme évoqué ci-dessus, les principaux Prestataires de Cloud ne sont pas européens. Or, leur soumission à des législations ne relevant pas du droit de l'Union européenne (UE) ou de celui des États membres, interroge sur l'application de dispositions légales ou réglementaires étrangères, notamment américaines avec l'exemple du CLOUD Act, entrant en conflit avec le droit de l'UE ou celui de ses États membres, telles que, notamment, le règlement général sur la protection des données (RGPD) ou, en France, la loi de blocage de 1968 ou encore le secret bancaire. Ce constat

soulève plusieurs enjeux stratégiques notamment en matière de contrôle de l'accès et de l'utilisation des données, de la préservation de leur confidentialité, sécurité et intégrité, mais, également de manière plus générale, en termes de sécurité informatique. En pratique, on observe traditionnellement un risque de captation des données aux fins d'activités de « surveillance » légitimées par application de règlementations extraterritoriales.

Enfin, une autre conséquence inévitable de la forte concentration des Prestataires de Cloud réside dans l'introduction d'un certain déséquilibre dans le rapport de force contractuel, non seulement du fait d'enjeux commerciaux, mais surtout en raison de l'externalisation auprès de ces prestataires de fonctions critiques ou importantes. Or l'absence ou le défaut de conformité de certaines clauses dans les contrats d'externalisation de prestations de services ou d'autres tâches opérationnelles essentielles ou importantes expose les banques à un risque de sanction administrative, voire de mise en jeu de leur responsabilité, notamment à l'égard de leurs clients. À l'inverse, les Prestataires de Cloud, comme généralement, la plupart des sous-traitants de banques, ne sont pas assujettis aux règles imposées au secteur bancaire.

Ces observations mettent en exergue les lacunes de l'encadrement contractuel des relations entre les acteurs bancaires et leurs Prestataires de Cloud et plus généralement, les limites atteintes par la réglementation bancaire actuellement en vigueur.

L'appréhension du Cloud par la réglementation bancaire

Le sujet de l'externalisation des services liés aux activités bancaires vers le Cloud – pas uniquement bancaires soit-dit en passant – a suscité des réactions de superviseurs, comme l'ACPR, dès le début des années 2010, jusqu'à susciter la création d'un régime spécifique. Toutefois, l'appréhension de ce phénomène par la réglementation, au niveau national et européen, s'est révélée lacunaire et hétérogène.

Au niveau européen, le superviseur bancaire a marqué son attention au développement de l'externalisation, qui a donné lieu en Europe à des lignes directrices du Comité Européen des Superviseurs Bancaires (CESB), comité consultatif dépourvu de tout pouvoir normatif ou de supervision, puis des recommandations de l'Autorité Bancaire Européenne (ABE), autorité européenne de supervision ayant succédé au CESB, lesquelles ont précisé les orientations du CESB. Elles concernaient, en particulier, l'évaluation du caractère critique des activités externalisées, la notification au superviseur national compétent des activités externalisées pertinentes et la mise à disposition d'un registre des dispositifs d'externalisation, la localisation et la conformité du traitement des données, la sécurité des systèmes d'information, la prise en compte des risques et l'encadrement contractuel de l'externalisation en chaîne, la mise en œuvre contractuelle d'un droit d'audit effectif au bénéfice de l'établissement supervisé et des autorités compétentes sur les prestataires de services de Cloud et, enfin, l'application de plans de continuité de l'activité et de plans de réversibilité. Le traitement spécifique réservé au Cloud fut toutefois de courte durée. En

effet, l'ABE décida finalement d'intégrer le Cloud au régime général de l'externalisation à l'occasion de l'élaboration d'orientations relatives à l'externalisation, entrées en vigueur le 30 septembre 2019 (les Orientations sur l'Externalisation).

Au niveau des États membres, le cadre réglementaire demeure hétérogène. En France, il existe un régime juridiquement contraignant de l'externalisation des activités bancaires.[13] À partir de 2013, l'ACPR s'est préoccupée officiellement du sujet du Cloud au travers d'une consultation de place, qui a conclu que le recours à certaines prestations informatiques externes devrait être considéré comme une externalisation de prestations de services ou d'autres tâches opérationnelles essentielles ou importantes tombant dans le régime de l'externalisation. Dans les autres États membres, des textes de portées juridiques différentes, généralement non contraignants, ont été adoptés. De manière plus récente, la plupart des autorités de supervision des États membres ont déclaré à l'ABE se conformer à ses orientations sur l'externalisation, à l'exception de l'Espagne et de la Pologne. Il n'en demeure pas moins que le cadre réglementaire des différents États membres régissant le recours au Cloud par des établissements bancaires reste encore très hétérogène, certains étant perçus comme plus contraignants que d'autres, comme le relève la Commission européenne dans son étude d'impact en prélude au projet de règlement DORA.

En conséquence, l'approche consistant à appréhender le Cloud bancaire au travers des règles encadrant l'externalisation des fonctions critiques ou importantes, si elle n'est pas propre au modèle européen, a atteint ses limites particulièrement dans l'environnement juridique européen. Les Orientations sur l'Externalisation n'intègrent pas le rôle grandissant des prestataires de technologies de l'information et de la communication en général (et des prestataires de services de Cloud en particulier) et ne reflètent pas l'inversion du rapport de force entre la banque et ses sous-traitants.

Un changement de paradigme devait donc s'opérer : c'est tout l'enjeu du projet DORA présenté par la Commission européenne en septembre 2020, qui agrège, d'une part, le cadre réglementaire existant, en particulier les Orientations sur l'Externalisation, et, d'autre part, le changement de dimension qui vise à soumettre ces prestataires à la surveillance d'un superviseur financier.

Vers un nouveau paradigme réglementaire en matière d'externalisation informatique dans le secteur financier : le projet de règlement DORA

Le projet de règlement DORA (pour « *digital operational resilience regulation* ») prévoit des exigences harmonisées afin d'accroitre et de sauvegarder la résilience opérationnelle des établissements et

[13] *Initialement, le règlement 97-02, remplacé par l'arrêté sur le contrôle interne du 3 novembre 2014.*

professionnels réglementés de la banque, des marchés financiers, de l'assurance notamment. Il a notamment pour objet de répondre aux enjeux relatifs à l'exposition et à la dépendance croissante des professionnels réglementés à l'égard des Prestataires TIC (incluant les Prestataires de Cloud), à l'absence d'un cadre harmonisé pour la maîtrise des risques associés aux TIC et à l'insuffisance du cadre réglementaire actuel concernant l'externalisation au regard du déséquilibre constaté dans la relation entre ces prestataires et les entités financières.

Ce projet de règlement européen d'application directe dans les États membres s'articule autour de deux piliers :

• les obligations applicables aux entités financières traitant avec les Prestataires TIC, à mettre en œuvre sur la base d'un principe de proportionnalité et dans une perspective de maîtrise des risques liés aux TIC ; et

• la surveillance des Prestataires TIC établis au sein de l'UE qui sont considérés comme « critiques » par les autorités européennes de supervision, sur la base de critères définis.

À cet égard, le groupe de travail s'est attaché à mettre en lumière les apports du projet de règlement DORA qui sont pertinents dans le cadre du présent rapport et à formuler des recommandations pour pallier les difficultés rencontrées concernant les thèmes suivants :

• supervision des Prestataires TIC critiques : conditions tenant au rattachement géographique au territoire de l'Union des prestataires critiques, à la détermination de leur caractère critique, et sanctions des manquements des Prestataires TIC critiques ;

• aménagement de l'interdiction pour les entités financières de faire appel à des Prestataires TIC critiques qui ne sont pas établis dans l'UE, notamment en termes d'application de la loi dans le temps et de l'évolution du caractère critique du Prestataire TIC ;

• exclusion des Prestataires TIC Intragroupes du champ d'application *ratione personae* de la surveillance des AES et de celui de l'interdiction de recourir à des Prestataires TIC Pays Tiers critiques, à certaines conditions ; et

• renforcement des obligations des Prestataires TIC en matière contractuelle.

TABLE DES MATIÈRES

INTRODUCTION

Qu'est-ce que le Cloud ?

Pluralité de définitions – Le *Cloud computing*, qui se traduit en français par l'expression l'« informatique en nuage »[14], fait l'objet de plusieurs définitions données par divers organismes officiels, dont celle-ci : « *Mode de traitement des données d'un client, dont l'exploitation s'effectue par l'internet, sous la forme de services fournis par un prestataire* ».[15] Cette définition précise par ailleurs que « *l'informatique en nuage est une forme particulière de gérance de l'informatique, dans laquelle l'emplacement et le fonctionnement du nuage ne sont pas portés à la connaissance des clients* ».[16] D'autres définitions sont indiquées en Annexe 2 du présent rapport.

En d'autres termes, le Cloud est un mode d'organisation et de gestion informatique permettant l'accès et l'utilisation, à distance, de services informatiques (logiciels, applications, plateformes, infrastructures, stockage, *etc.*) standardisées, automatisées, virtualisées et industrialisées/mutualisées, qui sont fournies par un prestataire de services de Cloud (le « **Prestataire de Cloud** ») (en anglais, *cloud services provider*) à plusieurs clients, comme des services à la demande et généralement facturés à l'usage.[17]

Le Prestataire de Cloud fournit ainsi à son client, en principe, par le biais d'un abonnement, une panoplie de ressources/services informatiques comprenant, généralement :

• la mise à disposition d'une infrastructure informatique (un parc de machines, de serveurs servant notamment au stockage de données, *etc.*) ;

• la mise à disposition d'une plateforme de développement et d'exploitation d'outils (applications informatiques, *etc.*) appartenant au client mais dont les moyens de production et d'exploitation sont hébergés par le Prestataire de Cloud ;

---

[14] Pour des commodités de lecture, il sera fait usage du terme de « Cloud », dans ce rapport et non de l'expression de « cloud computing » ou encore d'« informatique en nuage ».

[15] Avis de la Commission générale de terminologie et de néologie publié au Journal Officiel de la République Française (JORF) du 6 juin 2010, Vocabulaire de l'informatique et de l'internet, NOR: CTNX1012892X.

[16] Même référence que ci-dessus. Définition reprise de celle établie par le US National Institute of standards and technology (NIST) (https://csrc.nist.gov/publications/detail/sp/800-145/final).

[17] Autrement résumé, le Cloud est une « forme évoluée d'externalisation, dans laquelle le client ou l'utilisateur dispose d'un service en ligne dont l'administration et la gestion opérationnelle sont effectuées par un sous-traitant. Le Cloud Computing se caractérise également par une facturation à la demande et une disponibilité quasi immédiate des ressources » (Revue Communication Commerce Électronique, La définition des contours juridiques du Cloud Computing, cabinet d'avocats Granrut, novembre 2012).

• selon une approche étendue, la mise à disposition par le Prestataire de Cloud d'un outil (logiciel, application, etc.) et de services associés prêts à l'emploi (maintenance corrective et évolutive de l'outil, hébergement de l'outil, *etc.*).

Le client accède à ces services,[18] à la demande, et à distance, via un réseau informatique étendu, tel qu'internet.

Normalisation en l'absence d'encadrement normatif – Le Cloud ne fait, actuellement, l'objet d'aucun encadrement législatif et/ou réglementaire spécifique, que cela soit au niveau international, régional et/ou national.[19]

Cependant, les comités de normalisation internationaux que sont l'Organisation Internationale de Normalisation (ISO) et la Commission Électrotechnique Internationale (CIE) ont élaboré trois normes spécifiques au Cloud dont, en particulier, la norme ISO/IEC 17788:2014 Technologies de l'information – Informatique en nuage –, qui propose une vue d'ensemble et définit le vocabulaire applicable aux services de Cloud. En particulier, cette norme conceptualise les différentes couches de services, à savoir : logiciel (ou application) en tant que service (SaaS) ; plateforme en tant que service (PaaS) ; et infrastructure en tant que service (IaaS). Elle spécifie également la terminologie pour les modèles de déploiement du Cloud, notamment en opérant une distinction entre Cloud public et Cloud privé.[20]

L'organisme national de normalisation, l'AFNOR, pour sa part, a diffusé en 2014 plusieurs normes sur le sujet et l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) a publié en 2016 un référentiel d'exigences applicables aux Prestataires de Cloud.[21]

Ces normes n'ont aucune force juridique contraignante, notamment à l'égard des Prestataires de Cloud, et leur respect relève donc d'une démarche volontaire des acteurs concernés. Toutefois, dans les faits, elles semblent s'imposer sur le terrain des concepts et de la description des couches de services[22] et des modèles de Cloud.[23]

---

[18] *On parle usuellement de « couches de services », chaque couche correspondant à un service de Cloud (IaaS, PaaS, SaaS). Ces différentes catégories de services sont détaillées ci-après.*

[19] *Voire toutefois en matière bancaire et financière les avis exprimés par les régulateurs et qui sont évoqués ci-après.*

[20] *Les deux autres normes sont : (i) la norme ISO/IEC 17789:2014 Technologies de l'information – Informatique en nuage – Architecture de référence. De nature plus technique, elle contient des schémas et des descriptions qui montrent comment s'articulent les différents aspects du Cloud ; et (ii) la norme ISO/IEC 27018:2014 Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans le Cloud public agissant comme processeur de PII.*

[21] *ANSSI, Prestataires de services d'informatique en nuage (SecNumCloud) – Référentiel d'exigences –Version 3.1 du 11 juin 2018 (https://www.ssi.gouv.fr/uploads/2014/12/secnumcloud_referentiel_v3.1_anssi.pdf).*

[22] *V. supra note n° 18.*

[23] *Voir par exemple : https://aws.amazon.com/fr/types-of-cloud-computing/ ; https://docs.microsoft.com/fr-fr/learn/modules/intro-to-azure-fundamentals/what-is-cloud-computing.*

Les principaux modèles de Cloud – L'adoption du Cloud comme nouvelle technologie peut se réaliser selon trois modèles de base : le Cloud privé (qui se décline lui-même en un Cloud privé interne ou externe), le Cloud public, et, enfin, le Cloud hybride.

Brièvement, pour ne retenir que les caractéristiques principales de ces trois modèles :

• le Cloud privé correspond à la mise en œuvre de services Cloud au moyen d'une infrastructure dédiée à une entreprise ; cette infrastructure est affectée à l'usage exclusif de cette entreprise et est localisée, soit au sein de cette dernière, avec ou sans le concours d'un prestataire externe (Cloud privé interne), soit chez le Prestataire de Cloud (Cloud privé externe).

• À l'opposé, le Cloud public correspond à la mise en œuvre de services Cloud par le biais d'une infrastructure partagée entre plusieurs entreprises, clientes du Prestataire de Cloud. Cette infrastructure est localisée chez le prestataire.

• Enfin, entre ces deux modèles, le Cloud hybride constitue la combinaison des deux précédents modes/types de Cloud. Ainsi, une infrastructure dédiée à une entreprise cliente du Prestataire de Cloud (Cloud privé) et une infrastructure partagée entre plusieurs entreprises, clientes du Prestataire de Cloud (Cloud public), coexistent.

Il est à noter qu'il existe d'autres déclinaisons du Cloud :

• le Cloud communautaire, qui est un Cloud privé externe dédié à plusieurs entreprises (clientes d'un Prestataire de Cloud) intervenant dans un même secteur d'activités ; et

• le Cloud souverain, qui correspond à un modèle de Cloud, « dont les données sont entièrement stockées et traitées sur le territoire national par une entité de droit français et en application des lois et normes françaises. »[24] Il peut s'agir d'un Cloud public mais sous réserve qu'il soit fourni par une société de droit français, soumise au droit national et respectant les conditions de localisation des données.[25]

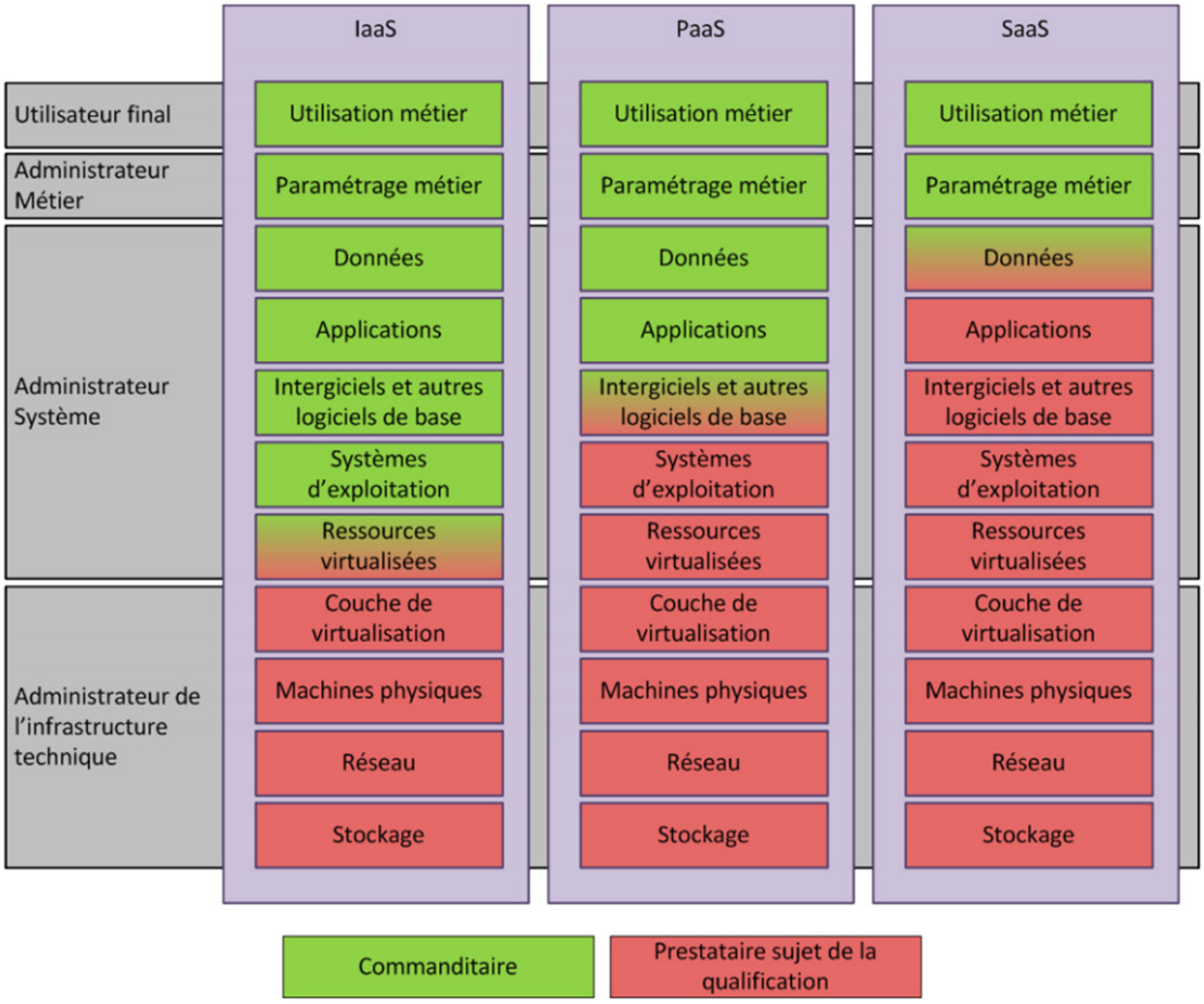
Les différentes « couches de services » de Cloud – Comme indiqué précédemment, la norme ISO/IEC 17788:2014 identifie trois couches de services de Cloud adaptés aux différents besoins des clients, à savoir les services IaaS, PaaS et SaaS.

---

[24] *Note d'information du 5 avril 2016 relative à l'informatique en nuage (Cloud Computing) par le directeur général des collectivités locales et le directeur chargé des Archives de France : https://francearchives.fr/file/f7ace4517613a246583fd2dd673a0e6d0f86c039/static_9151.pdf.*

[25] *On peut noter que le concept de Cloud souverain est assez élastique et ne se limite pas nécessairement à un territoire national. On parle en effet volontiers d'un Cloud souverain à l'échelle de l'Union européenne, par opposition aux services de Cloud fournis par les entreprises de pays tiers (cf., par exemple, J. Henno, Demain, un Cloud souverain européen ? Les Echos, 25 janvier 2021.*

Quels services/activités incluent-ils exactement ? Le schéma ci-dessous[26] est très couramment utilisé pour illustrer les couches de services que recouvrent le Cloud proposés par les Prestataires de Cloud.



[26] *Figurant dans le document de l'ANSSI : Prestataires de services d'informatique en nuage (SecNumCloud) – Référentiel d'exigences – Version 3.1 du 11 juin 2018 (https://www.ssi.gouv.fr/uploads/2014/12/secnumcloud_referentiel_v3.1_anssi.pdf).*

Dans son étude, reprise par la FBE, le Comité de Bâle applique cette classification au secteur financier :[27]

• Le service de fourniture d'infrastructures (*Infrastructure as a Service ou IaaS*)[28] est le service aux termes duquel le Prestataire de Cloud met à disposition de son client, une infrastructure informatique (serveur, stockage, sauvegarde, capacité de calcul, réseaux, *etc.*), qu'il peut utiliser, ou encore configurer à distance pour composer son environnement. Le client n'a ainsi pas besoin d'investir dans l'acquisition d'équipements, de ressources, qui sont virtualisées et externalisées auprès du Prestataire de Cloud (et/ou du(des) sous-traitant(s) de ce dernier) et que le client prend en location, généralement par le biais d'un abonnement. Le client reste toutefois maître (et responsable), tout particulièrement, de ses applications, données, et de leur stockage, de certains composants réseaux et du système d'exploitation, dont il doit notamment assurer la maintenance.[29]

• Le service de fourniture d'une plateforme informatique (*Platform as a Service ou PaaS*)[30] inclut les services de l'IaaS mais va encore plus loin : outre l'infrastructure (serveurs, stockage, réseaux, *etc.*), le Prestataire de Cloud fournit également, directement et/ou via son(ses) sous-traitant(s), les outils dits « *middleware* » (système d'exploitation, base de données, serveur web, etc.). Dans le cadre du PaaS, le Prestataire de Cloud met, généralement par le biais d'un abonnement, à la disposition du client, un environnement informatique (plateforme), au sein duquel le client peut développer, créer, configurer, tester et exécuter ses propres outils (applications, logiciels, *etc.*). Le système d'exploitation, l'infrastructure, etc. sont sous la responsabilité du Prestataire de Cloud tandis que le client conserve

---

[27] Comité de Bâle sur le contrôle bancaire, Saines pratiques – Implications des évolutions de la technologie financière pour les banques et les autorités de contrôle bancaire, Février 2018 et FBE, ou en anglais European Banking Federation (EBF), The use of Cloud Computing by Financial Institutions, 4 June 2020, Technical paper. Voir également, ACP-Banque de France, Les risques associés au Cloud computing, Analyses et synthèses, n° 16, juillet 2013 (https://acpr.banque-france.fr/les-risques-associes-au-cloud-computing-juillet-2013).

[28] Exemple : Microsoft Azure.

[29] L'ANSSI définit l'IaaS comme un « service [qui] concerne la mise à disposition de ressources informatiques abstraites (puissance CPU, mémoire, stockage etc.). Le modèle IaaS permet au commanditaire de disposer de ressources externalisées virtualisées. Ce dernier garde le contrôle sur le système d'exploitation (OS), le stockage, les applications déployées ainsi que certains composants réseau (pare feu, par exemple)» (ANSSI, Prestataires de services d'informatique en nuages (SecNumCloud) – Référentiel d'exigences, Version 3.1 du 11 juin 2018).

Pour la Banque de France, « (l)'IaaS (…) offre une infrastructure informatique comme de la puissance de calcul, des machines virtuelles incluant un système d'exploitation, du stockage, des services de sauvegarde » (ACP-Banque de France, Les risques associés au Cloud Computing, Analyses et synthèses, n° 16, juillet 2013 (https://acpr.banque-france.fr/les-risques-associes-au-cloud-computing-juillet-2013)).

Il est fait parfois également référence (comme dans l'étude de la FBE précitée) au CaaS ou Containers-as-a-Service. Il s'agit d'une variante de l'IaaS. Selon Orange Business Services, « Le CaaS utilise le principe du container informatique, qui est une unité rassemblant le code et les configurations d'une application. Ce système permet la portabilité des applications à travers les réseaux, le stockage et les serveurs. Les containers permettent de mutualiser des ressources informatiques au niveau des bibliothèques de code afin de déployer des applications plus rapidement. Appliquée au cloud, l'utilisation de containers optimise le dimensionnement et l'orchestration multi-sites des applications hébergées sur une infrastructure cloud. »

[30] Exemple : IBM Blockchain Platform (IBM).

la maîtrise complète des outils (applications, logiciels, *etc.*) qu'il installe, configure et exploite sur la plateforme.[31]

• Enfin, le service de fourniture d'applications ou logiciels (*Software as a Service* ou SaaS) constitue le service le plus connu du grand public.[32] Le Prestataire de Cloud met, généralement par le biais d'un abonnement, à la disposition du client : (i) des outils (logiciels, applications, *etc.*) qu'il héberge directement dans son système d'information sur une plateforme (comprenant l'ensemble des matériels, serveurs, réseaux, mis en place et exploités directement par le Prestataire de Cloud, pour en assurer l'hébergement), ou indirectement au travers de son(ses) sous-traitant(s) et qui sont accessibles et utilisables à distance (via Internet, *etc.*) par le client ; et (ii) des services associés prêts à l'emploi, tels que la maintenance (corrective et évolutive) et l'hébergement des outils, *etc.* et qui sont fournis par le Prestataire de Cloud et/ou son(ses) sous-traitant(s).[33]

Il est à noter qu'il existe d'autres services que recouvre le Cloud, tel que le service de fourniture d'un bureau virtuel ou bureau virtuel hébergé (*Desktop as a Service* ou DaaS)[34], par lequel le Prestataire de Cloud permet au client, généralement par le biais d'un abonnement, d'accéder à un bureau virtuel à distance (via Internet, *etc.*). « *(L)e DaaS consiste à déporter la gestion et la fourniture des environnements de travail (mais parfois aussi des applications) dans le (c)loud* ».[35]

---

[31] *L'ANSSI définit le « PaaS » comme un « service [qui] concerne la mise à disposition par le prestataire de plateformes d'hébergement d'applications. Le commanditaire n'a pas la maîtrise de l'infrastructure technique sous-jacente, gérée et contrôlée par le prestataire (réseau, serveurs, OS, stockage, etc.). Le commanditaire a cependant la maîtrise des applications déployées sur cette plateforme. Il peut aussi avoir la maîtrise de certains services composant cette plateforme ou de certains éléments de configuration suivant la répartition des rôles définie dans le service. Exemple : applications en conteneurs gérés par un outil d'orchestration »(ANSSI, Prestataires de services d'informatique en nuages (SecNumCloud) – Référentiel d'exigences, Version 3.1 du 11 juin 2018).*

La Banque de France indique que « (l)e PaaS (…) fournit une plateforme de développement et/ou d'exécution intégrée, reposant sur un catalogue de composants logiciels et techniques standardisés dont l'infrastructure sous-jacente est transparente pour l'utilisateur » (ACP-Banque de France, Les risques associés au Cloud Computing, Analyses et synthèses, n° 16, juillet 2013 (https://acpr.banque-france.fr/les-risques-associes-au-cloud-computing-juillet-2013)).

[32] *Exemple : Office 365 (Microsoft).*

[33] *L'ANSSI définit le « SaaS » comme un « service [qui] concerne la mise à disposition par le prestataire d'applications hébergées sur une plateforme partagée. Le commanditaire n'a pas la maîtrise de l'infrastructure technique sous-jacente. Le prestataire gère de façon transparente pour le commanditaire l'ensemble des aspects techniques requérant des compétences informatiques. Le commanditaire garde la possibilité d'effectuer quelques paramétrages métier dans l'application. Exemples : « CRM », outils collaboratifs, messagerie, Business Intelligence, « ERP », etc.» (ANSSI, Prestataires de services d'informatique en nuages (SecNumCloud) – Référentiel d'exigences, Version 3.1 du 11 juin 2018).*

Pour la Banque de France, «(l)e SaaS (…) est une solution applicative répondant à un domaine d'utilisation précis supportant une fonction métier (gestion de la relation clientèle, gestion financière, …) ou un service transverse (messageries, outils collaboratifs…)» (ACP-Banque de France, Les risques associés au Cloud Computing, Analyses et synthèses, n° 16, juillet 2013 (https://acpr.banque-france.fr/les-risques-associes-au-cloud-computing-juillet-2013)).

[34] *Dominique Filipopone, DaaS ou la virtualisation du poste de travail dans le Cloud, Journal du Net, 1er septembre 2001 (https://www.journaldunet.com/solutions/cloud-computing/1091879-daas-ou-la-virtualisation-du-poste-de-travail-dans-le-cloud/).*

[35] *Dominique Filipopone, DaaS ou la virtualisation…, op. cit.*

Cloud « bancaire »

Le Cloud s'est progressivement imposé depuis une dizaine d'années dans le secteur financier mondial, grâce aux avantages offerts par cette nouvelle forme de gestion informatique qui favorise l'accès à l'innovation, à la performance et à la sécurité technologiques (rapidité, flexibilité, volume, capacité énergétique, *etc.*[36]), tout en rationalisant les ressources, les expertises et les coûts induits pour les utilisateurs. L'appréciation de ces avantages relève de la stratégie propre à chaque catégorie d'acteurs, étant précisé que les modèles de déploiement du Cloud permettent une adaptabilité de cette technologie aux besoins des utilisateurs.[37]

Le Cloud s'est imposé comme une technologie incontournable pour permettre la numérisation du secteur financier, en particulier dans le domaine bancaire. Cette technologie s'est avérée être un accélérateur, voire un facteur d'émulation, pour les acteurs de petite/moyenne taille ainsi que pour les nouveaux acteurs du secteur bancaire, tels que les fintech et les néo-banques, qui y trouvent le moyen de déployer une panoplie de services bancaires et financiers numériques dans de très courts délais de mise sur le marché. Cette agilité est rendue possible pour ce type d'entreprises principalement grâce au recours à des Prestataires de Cloud (privés externes et/ou publics), alors que les grands groupes bancaires historiques ont abordé cette nouvelle technologie de manière prudente en la faisant cohabiter avec les infrastructures informatiques d'origine.[38]

Le mouvement progressif des grands groupes bancaires vers le Cloud, notamment hybride, s'est confirmé au fil des années mais concerne principalement les fonctions dites « support » (telles que la gestion des ressources humaines, la communication, *etc.*) et seulement marginalement les fonctions relevant de l'activité « cœur de métier » (comme les services de tenue de compte et l'émission et la gestion de moyens de paiement y associés, l'octroi de crédit, *etc.*).[39] Néanmoins, de nouvelles stratégies se dessinent, comme celles initiées en juillet 2020 par deux grands groupes bancaires européens, décidant de loger leurs activités bancaires dans un Cloud public.[40]

Face au constat d'un recours grandissant au Cloud par le secteur bancaire et aux enjeux liés à cet usage, en termes notamment de maîtrise et contrôle du stockage, d'accès et d'utilisation de données

---

[36] *Lamy Droit du Numérique, Lamy Pratique, Éditions Wolters Kluwer, Mai 2015 : « le Cloud Computing ou Informatique dans les nuages est né du constat que de nombreux serveurs dans le monde ne sont pas utilisés au plein de leur capacité et que les besoins d'une entreprise en puissance et capacité de stockage peuvent varier dans le temps. Le Cloud Computing consiste donc à mutualiser ces serveurs et considérer la puissance de calcul et de stockage des serveurs comme l'électricité ».*

[37] *La Tribune, Pourquoi les banques cèdent aux sirènes du « Cloud », 1er juillet 2019. Voir déjà, en 2011, l'Agefi, L'informatique dématérialisée à l'essai dans les banques françaises, 3 mars 2011.*

[38] *Le Cahier Techno, Cloud computing : de l'expectative à la mise en pratique, Revue banque n°748, mai 2012.*

[39] *Le Cahier Techno, L'heure du Cloud public a-t-elle sonné pour les banques françaises ? Revue Banque n° 835, septembre 2019.*

[40] *Les Echos, Après Deutsche Bank, HSBC s'allie avec un GAFA pour se déployer sur le Cloud, 18 juillet 2020 ; Les Echos, Cloud bancaire : les banques européennes avancent leurs pions, 22 juillet 2020.*

relevant du cœur de métier de la banque, avec en toile de fond, les risques liés à la cybercriminalité[41] et les questions de souveraineté technologique, le Haut Comité Juridique de Place (HCJP) a souhaité conduire la présente étude.

Elle s'est concentrée sur les seuls établissements de crédit au sens de l'article L. 511-1 du Code monétaire et financier (par commodité de langage, on utilisera le terme de « banque » indistinctement). Par conséquent, la présente étude ne s'intéresse pas aux autres formes d'établissements réglementés du secteur bancaire (à savoir, en particulier, les sociétés de financement, les établissements de paiement et les établissement de monnaie électronique), ni aux entreprises relevant d'autres réglementations sectorielles du secteur financier au sens large[42] (entreprises d'investissement, sociétés de gestion de portefeuille, entreprises d'assurance et de réassurance, *etc.*), même si les questions liées à l'utilisation du Cloud sont pertinentes à leur égard[43], notamment dans le contexte de groupes du secteur financier comprenant des entreprises soumises à ces réglementations.

Pour les besoins de l'analyse, nous utiliserons ainsi dans le présent rapport le terme de « Cloud bancaire » de façon générale pour désigner le recours au Cloud (sans distinguer parmi ses différentes formes)[44] par les banques.

Nul ne conteste la tendance irréversible de transformation numérique des banques au moyen des solutions informatiques de Cloud et de bénéfices qui en résultent, tant pour les banques en termes de gestion de leurs ressources techniques, que pour la clientèle. Toutefois, leur déploiement à grande échelle au cœur même des métiers bancaires et financiers,[45] qui implique la transmission à des tiers non soumis à supervision d'informations et données sensibles concernant les clients,[46]

---

[41] Selon IBM, l'industrie des services financiers est celle qui est la plus touchée par la cybercriminalité en 2019, représentant 17% des attaques, parmi les 10 secteurs industriels les plus touchés (consommation, transports, média, services professionnels, etc.) dans l'années IBM Security, « X-Force Threat Intelligence Index 2020 », p. 29 (https://www.ibm.com/downloads/cas/DEDOLR3W).

[42] Telles que la Directive 2014/65/UE du Parlement européen et du conseil du 15 mai 2014 concernant les marchés d'instruments financiers (MIFID), la Directive 2009/138/CE du Parlement européen et du Conseil du 25 novembre 2009 sur l'accès aux activités de l'assurance (Solvabilité II), la Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement (PSD) ou encore la Directive 2009/110/CE du Parlement européen et du Conseil du 16 septembre 2009 concernant l'accès à l'activité des établissements de monnaie électronique (EMD).

[43] À ce titre, voir les orientations de l'AEAPP datées du 6 février 2020 relatives à l'externalisation auprès de Prestataires de Cloud, ainsi que, les orientations de l'AEMF du 3 juin 2020 sur le même sujet.

[44] Étant toutefois précisé que l'accent sera mis plus particulièrement sur les formes publiques et hybrides du Cloud, car ce sont elles qui sont le plus susceptibles de générer des risques pour les banques.

[45] Telles que les activités de recueil des dépôt du public, l'octroi de crédit, le conseil et la gestion de patrimoine, etc.

[46] Telles que leur situation patrimoniale, leur endettement, leurs coordonnées bancaires, etc.

se heurte à plusieurs difficultés qui mettent en exergue la situation croissante de dépendance des banques à l'égard de Prestataires de Cloud, auxquels la réglementation de la profession bancaire ne s'applique pas **(Section 1)**.

Le sujet de l'externalisation des services liés aux activités bancaires vers le Cloud – pas uniquement bancaires soit-dit en passant – a suscité des réactions de superviseurs, comme l'ACPR dès le début des années 2010, jusqu'à susciter la création d'un régime spécifique **(Section 2)**. Plus récemment, la période d'intensification des partenariats entre banques et Prestataires de Cloud a mis en lumière les difficultés dans la mise en œuvre concrète du cadre réglementaire européen, lequel connaît à présent une évolution visant à mieux appréhender les enjeux de sécurité informatique, opérationnelle et juridique du Cloud bancaire **(Section 3)**.

I- Enjeux liés au Cloud bancaire

Les enjeux liés au Cloud sont nombreux.[47] Parmi eux, on peut en relever quelques-uns qui sont plus particulièrement pertinents dans la sphère bancaire.

1.1 - Marché oligopolistique : dépendance des banques dû à un faible nombre de Prestataires de Cloud

1.1.1 - État du marché mondial

Selon le cabinet Gartner, en matière de Cloud, les géants du numérique occupent une place privilégiée sur un marché en forte croissance, le marché mondial des services de Cloud public[48] ayant atteint 257,5 milliards de dollars en 2020 contre 17,4 milliards en 2009. Ce marché présente un potentiel de progression de plus 18% par an pour 2021 et 2022.[49] Le segment de marché correspondant au service SaaS reste le plus important en proportion du marché, par rapport aux segments correspondant aux autres services. Toutefois, le cabinet estime que le service PaaS connaîtra la plus grande progression au cours des prochaines années et, ensemble avec le service Iaas, dépassera le service SaaS dès 2021 (à 120,75 milliards de dollars contre 117,8 milliards pour le service SaaS).

---

[47] *Par exemple, dans le domaine agricole : v. J. Henno, op. cit.*

[48] *En termes de dépenses effectuées par les clients finaux dans les services de Cloud public.*

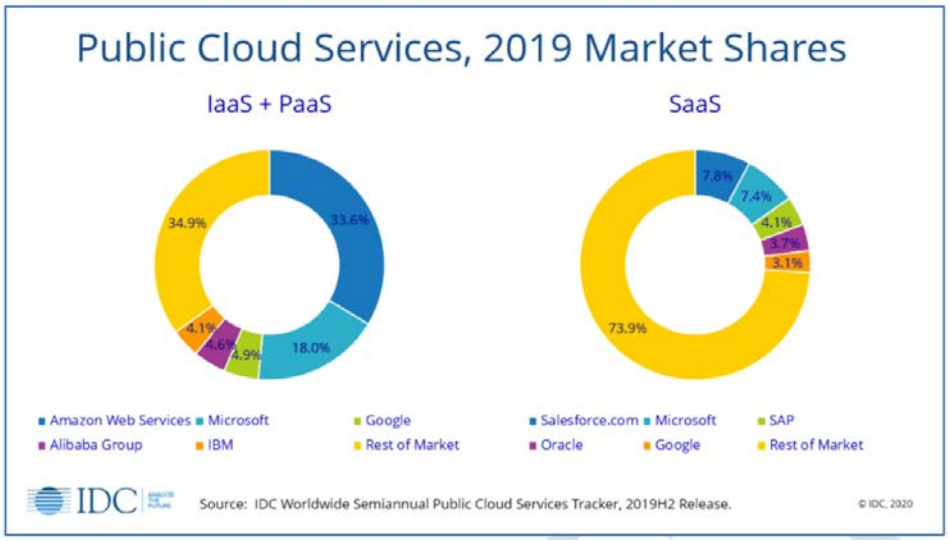
[49] *Gartner, Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 18% in 2021, 17 novembre 2020 (https://www.gartner.com/en/newsroom/press-releases/2020-11-17-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-grow-18-percent-in-2021).*

Marché mondial du Cloud public (en millions de dollars)

Couches de service	2019	2020	2021	2022
SaaS	102 064	101 480	117 773	138,261
IaaS	44 457	51 421	65 264	82 225
PaaS	37 512	43 823	55 486	68 964
Autres[50]	58 664	60 825	66 467	72 812
Total	**242 696**	**257 549**	**304 990**	**362 263**

Source : Gartner.

Le cabinet IDC indique de son côté que le marché mondial des services de Cloud public (services IaaS et PaaS) est dominé par Amazon Web Services (AWS), Microsoft Azure, Google et Alibaba, qui ensemble détiennent 61% de parts de marché. Le marché du service SaaS apparaît en revanche nettement moins concentré, puisque les cinq premiers acteurs, à savoir Salesforce, Microsoft, SAP, Oracle et Google ne détiennent que 26% du marché et le premier d'entre eux (Salesforce) dispose d'une part de marché inférieure à 8%.[51]

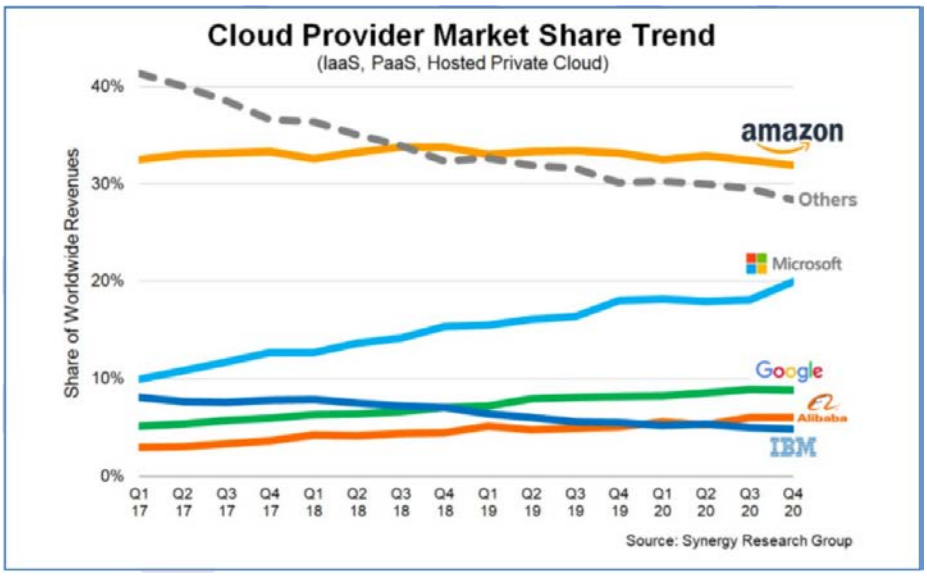


Source IDC

[50] *Ces services incluent: Cloud Business Process Services (BPaaS), Cloud Management and Security Services et Desktop as a Service (DaaS).*

[51] *IDC, Worldwide Public Cloud Services Market Totaled $233.4 Billion in 2019 with the Top 5 Providers Capturing More Than One Third of the Total, According to IDC, 18 août 2020 (https://www.idc.com/getdoc.jsp?containerId=prUS46780320). Voir également, Synergy Research Group, Cloud Market Growth Rate Nudges Up as Amazon and Microsoft Solidify Leadership, 29 octobre 2020 (https://www.srgresearch.com/articles/cloud-market-growth-rate-nudges-amazon-and-microsoft-solidify-leadership).*

Selon une étude plus récente de Synergy Research Group,[52] 2020 confirme la tendance à la concentration observée sur les marchés des services IaaS et PaaS avec une progression de Microsoft et au détriment du groupe constitué des acteurs ayant une plus faible part de marché (IBM, Salesforce, Tencent, Oracle, NTT, Baidu, SAP, Fujitsu and Rackspace).[53]



Au travers des chiffres, le constat suivant s'impose : émanant essentiellement de Prestataires de Cloud américains à l'origine (dans les segments des services IaaS et PaaS à tout le moins), l'offre de Cloud commence à être également fournie par des Prestataires asiatiques. Les prestataires européens sont nettement distancés. En 2020, SAP (entité allemande) a rejoint le classement à la 10e place avec 1% du marché mondial. Cette place avait été dévolue également au 4e trimestre 2018 à un autre Prestataire de Cloud européen, OVH (entité française), détenant à l'époque 1% du marché.[54]

Par conséquent, les banques de l'UE sont confrontées à un choix restreint, compte tenu du faible nombre de Prestataires de Cloud sur le marché mondial et, stratégique dans la mesure où ces principaux prestataires sont soumis à la législation de pays tiers à l'UE qui n'est pas toujours compatible avec le droit de l'UE ou celui de ses États membres (voir le paragraphe 1.2 - Enjeux liés à l'extraterritorialité des législations procédurales et répressives américaines et à la souveraineté de l'UE en matière de protection des données : l'exemple USA-UE - ci-après).

[52] *Synergy Research Group, Cloud Market Ends 2020 on a High while Microsoft Continues to Gain Ground on Amazon, 2 février 2021 (https://www.srgresearch.com/articles/cloud-market-ends-2020-high-while-microsoft-continues-gain-ground-amazon).*

[53] *Les données de marché ne couvrent malheureusement pas le segment du SaaS.*

[54] *Selon l'Usine nouvelle, OVH dans le Top 10 mondial du cloud, 14 février 2019.*

Cette situation fait écho au risque de concentration identifié par le CESB en 2006, lequel fait l'objet de recommandations détaillées de la part de l'ABE dans ses Orientations sur l'Externalisation.[55]

Le ROFIEG, dans un rapport datant de décembre 2019,[56] a résumé la relation entre les Prestataires de Cloud et leurs clients en soulignant les deux phénomènes suivants :

• d'une part, la structure oligopolistique du marché du Cloud, dominé « *par une poignée d'acteurs* » entraînant une « *profonde interconnexion entre une poignée de fournisseurs de services essentiels et l'ensemble du système financier* » pouvant créer « *des points de défaillance uniques* » ;[57] et

• d'autre part, cette structure oligopolistique du marché du Cloud se double d'une dépendance technologique vis-à-vis des Prestataires de Cloud pouvant inverser la relation de pouvoir traditionnelle entre le donneur d'ordre (le client) et le prestataire de services, lequel est un acteur évoluant hors du périmètre de la réglementation bancaire.

Le déséquilibre important en faveur des Prestataires de Cloud en raison de leur puissance économique et de leur expertise technologique créée une double asymétrie entre ces prestataires et leurs clients.

La puissance économique des Prestataires de Cloud est considérable. En termes capitalistiques, rappelons que les groupes auxquels appartiennent les deux premiers Prestataires de Cloud américains (Microsoft et Amazon) ont une capitalisation boursière supérieure à 1 000 milliards de dollars,[58] quand le premier groupe bancaire français est valorisé à 39 milliards d'euros.[59]

On estime que 82 milliards de dollars ont été investis en 2019 rien que dans les infrastructures de stockage de données, dont 44% par les quatre principaux Prestataires de Cloud, lesquels sont Amazon, Microsoft, Google et Alibaba.[60] Le cabinet Synergy Research Group rapporte que le nombre

---

[55] Voir notamment le paragraphe 66 des orientations de l'ABE (EBA/GL/2019/02) 25 février 2019. https://eba.europa.eu/sites/default/documents/files/documents/10180/2761380/6565c789-487b-4528-8a17-4b94147dc5b8/EBA%20revised%20Guidelines%20on%20outsourcing_FR.pdf. Ce thème est également présent dans les orientations de l'EIOPA, Orientations relatives à la sous-traitance à des prestataires de services en nuage du 6 février 2020 (EIOPA-BoS-20-002) applicables aux nouveaux contrats ou ceux modifiés à partir du 1er janvier 2021.

[56] Expert Group on Regulatory Obstacles to Financial Innovation (ROFIEG): 30 recommendations on regulation, innovation and finance (spéc. p. 11 Recommendation 5 – Outsourcing guidelines and certification/licensing). https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/191113-report-expert-group-regulatory-obstacles-financial-innovation_en.pdf.

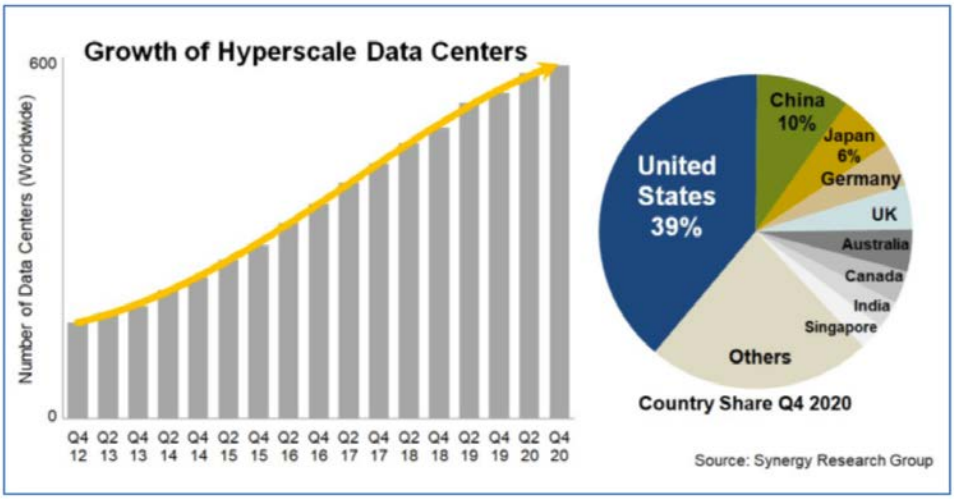
[57] Voir le paragraphe 61 du Joint Advice of the European Supervisory Authorities to the European Commission on the need for legislative improvements relating to the ICT risk management requirements in the EU financial sector (10 April 2019).

[58] Capital, Google, Amazon… Les Gafa sont au plus haut en Bourse, gare aux déceptions ! 20 avril 2020 (https://www.capital.fr/entreprises-marches/google-amazon-les-gafa-sont-au-plus-haut-en-bourse-gare-aux-deceptions-1367860).

[59] https://www.forbes.com/companies/bnp-paribas/?sh=2034c6b91a21 (chiffres au 12 mai 2020).

[60] L'Usine Nouvelle, 82 milliards de dollars investis en 2019 dans les datacenters du Cloud et colocation, 12 avril 2020.

d'infrastructures de stockage de données géantes (*hyperscale data centers*) a doublé depuis 2015 pour atteindre le nombre de 597 en 2020, dont presque 40% sont situés aux États-Unis (10% en Chine). Plus de 50% de ces infrastructures appartiennent à Amazon, Microsoft et Google.[61]



Source: Synergy Research Group

Ces chiffres permettent de comprendre que le secteur bancaire, comme d'autres secteurs d'activités, notamment industriels, ne peuvent investir à ce stade des sommes comparables, et doivent donc s'adresser aux Prestataires de Cloud devenus *de facto* incontournables.

Une telle concentration d'acteurs est caractéristique de ce nouveau marché : les Prestataires de Cloud forment ainsi un véritable oligopole.

Dans ce contexte, le rapport de force contractuel est parfois susceptible de déséquilibre entre les Prestataires de Cloud et les banques, et ces dernières peuvent éprouver des difficultés à négocier l'inclusion de certaines stipulations contractuelles répondant aux exigences réglementaires notamment en matière d'externalisation.

Au niveau des États eux-mêmes, la puissance économique que représentent les géants mondiaux du numérique constitue un sujet de préoccupation grandissant[62] suscitant des réactions politiques.

---

[61] *Synergy Research Group, Microsoft, Amazon and Google Account for Over Half of Today's 600 Hyperscale Data Centers, 26 janvier 2021 (https://www.srgresearch.com/articles/microsoft-amazon-and-google-account-for-over-half-of-todays-600-hyperscale-data-centers).*

[62] *Rapport pour le Ministre britannique de l'économie par un groupe d'experts présidé par l'ancien conseiller économique du président américain Barack Obama, le Professeur Jason Furman : Unlocking digital competition – Report of the Digital Competition Expert Panel, Mars 2019 ; Rapport d'un groupe d'experts présidé par la professeure Fiona Scott Morton pour le Stigler Center (Chicago Booth School of Business), Mai 2019 ; Rapport de l'Australian Consumer and Competition Commission, Digital Platforms Inquiry, juillet 2019.*

1.1.2 - Approche des États sur les risques de comportements anticoncurrentiels liés au marché oligopolistique

Aux États-Unis, la Commission judiciaire du Congrès américain a lancé en 2019 une enquête sur la concurrence dans les marchés du numérique,[63] clôturée par un rapport le 6 octobre 2020[64] qui met plus particulièrement en relief la domination des GAFA.[65] Précédé de seize mois d'enquêtes et de la consultation de 1,3 million de documents,[66] ce rapport s'interroge sur le rôle de ceux qui sont désignés comme « *Gatekeepers* » et souligne la mutation rapide d'entreprises[67] qui ont tendance à adopter des comportements de prédation, en recourant à des « *killer acquisitions of potential competitors* ».[68]

Cette Commission suggère donc des réformes visant à s'attaquer aux comportements anticoncurrentiels sur les marchés numériques, à renforcer l'application des lois sur les fusions et les monopoles et pour ce faire, à réformer le droit de la concurrence américain.[69]

Des recommandations sont également proposées pour un renforcement de la doctrine des « installations essentielles », qui exige des « plates-formes dominantes »[70] (telles que les GAFA) qu'elles fournissent un accès non discriminatoire à leurs services jugés essentiels, doctrine dont la portée a été remise en cause par la jurisprudence.[71] Le démantèlement de ces plates-formes par des

---

[63] *House Committee on the Judiciary, House Judiciary Committee Launches Bipartisan Investigation into Competition in Digital Markets, communiqué de presse, 3 juin 2019 (https://judiciary.house.gov/news/documentsingle.aspx?DocumentID=2051).*

[64] *Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary, Majority Staff Report and Recommendations, Investigation on Competition in Digital Markets, (https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf).*

[65] *Rapport, p. 6 : « In June 2019, the Committee on the Judiciary initiated a bipartisan investigation into the state of competition online, spearheaded by the Subcommittee on Antitrust, Commercial and Administrative Law. As part of a top-to-bottom review of the market, the Subcommittee examined the dominance of Amazon, Apple, Facebook, and Google, and their business practices to determine how their power affects our economy and our democracy. Additionally, the Subcommittee performed a review of existing antitrust laws, competition policies, and current enforcement levels to assess whether they are adequate to address market power and anticompetitive conduct in digital markets. »*

[66] *Rapport, loc. cit.*

[67] *« …that once were scrappy underdog startups that challenged the status quo have become the kinds of monopolies we last saw in the era of oil barons and railroad tycoon », voir en page 6 du rapport.*

[68] *Une annexe au rapport énumère plus de 560 acquisitions des GAFA remontant à 1988. Le Congrès critique à cet égard la Federal Trade Commission, qui a préféré « concentrer ses efforts sur des petits acteurs - incluant des enseignants de patin sur glace et des joueurs d'orgue », p. 404, note 2526.*

[69] *Voir rapport, p. 20.*

[70] *Le rapport use du vocable « dominant platforms ».*

[71] *Voir rapport, p. 396 à 398, spéc. p. 397 : « […] the Subcommittee recommends that Congress consider revitalizing the «essential facility» doctrine, the legal requirement that dominant firms provide access to their infrastructural services or facilities on a non-discriminatory basis. To clarify the law, Congress should consider overriding judicial decisions that have treated unfavorably essential facilities – and refusal to deal-based theories of harm. »*

séparations structurelles et des restrictions par secteurs d'activités,[72] l'interdiction faite aux plates-formes dominantes de s'autoréférencer,[73] ainsi que la modification de la réglementation relative aux acquisitions futures par les plates-formes dominantes, notamment au travers de l'obligation d'une notification HSR[74] complètent ces propositions.

L'avenir nous dira si une loi comparable au Glass-Steagall Act de 1933[75] qui, dans les années 1930, avait dissocié les activités de banque de détail et celles des banques d'investissement[76] sera adoptée, ou si on pourra observer des démantèlements tels que celui d'AT&T en 1984,[77] dans le cadre du nouveau mandat présidentiel.[78]

De même, en Chine, le gouvernement chinois (*State Administration for Market Regulation*) a, le 2 janvier 2020, soumis à consultation publique un projet de modification de son droit de la concurrence,[79] visant à y soumettre tous les acteurs chinois du numérique, et au premier chef, les BATX,[80] qui jusqu'à présent y échappaient.[81] Ce projet a été notamment alimenté par le succès phénoménal du réseau social TikTok, propriété du groupe Bydance.[82] Le projet prévoit ainsi des

---

[72] *Voir rapport, p. 377-381. Le Rapport cite en exemple certaines lois ayant ordonné la mise en œuvre de mesures de séparations strucurelles dans d'autres secteurs industriels, tels que le transport ferroviaire, la banque ou les médias : « Congress subsequently enacted a provision to prohibit railroads from transporting any goods that they had produced or in which they held an interest.[2411] Congress has legislated similar prohibitions in other markets. The Bank Holding Company Act of 1956 broadly prohibited bank holding companies from acquiring nonbanking companies[2412] Vertically integrated television networks, meanwhile, were subject to "fin-syn" rules, which prohibited networks from entering production and syndication markets.[2413] » (spéc. p. 380).*

[73] *Voir rapport, p. 381 à 383.*

[74] *La loi Hart-Scott-Rodino Antitrust Improvement Act (HSR) rend obligatoire depuis 1976 la notification au Department of Justice et à la Federal Trade Commission des projets de fusion de taille supérieure à un certain seuil (voir : https://www.ftc.gov/enforcement/statutes/hart-scott-rodino-antitrust-improvements-act-1976).*

[75] *https://history.house.gov/HouseRecord/Detail/15032450290.*

[76] *Ou, plus récemment, la loi Volcker visant à séparer les activités de compte propre de celles réalisées pour la clientèle (https://www.federalreserve.gov/supervisionreg/volcker-rule.htm).*

[77] *Le 1er janvier 1984, afin de stimuler la concurrence, le département américain de la Justice avait obtenu qu'AT&T se sépare de plusieurs de ses filiales. La procédure avait débuté en 1974, le département de la Justice ayant à l'époque invoqué la loi Sherman contre les monopoles. Pour un aperçu historique de cette décision et de ses conséquences en termes de concurrence, voir : https://www.justice.gov/atr/att-divestiture-was-it-necessary-was-it-success.*

[78] *Bien que bi-partisane, cette analyse approfondie a déjà suscité un mini-rapport de la part des républicains (voir : https://republicans-judiciary.house.gov/wp-content/uploads/2020/10/2020-10-06-Reining-in-Big-Techs-Censorship-of-Conservatives.pdf).*

[79] *http://www.samr.gov.cn/hd/zjdc/202001/t20200102_310120.html.*

[80] *Baidu, Alibaba, Tencent, Xiaomi, les quatre premières entreprises du web chinois.*

[81] *Simon Associés, Lettre du numérique, 13 mars 2020 (https://www.lettredunumerique.com/P-2222-489-A1-la-loi-antitrust-en-chine-le-projet-de-modification-en-vue-d-une-regulation-renforcee-des-batx.html).*

[82] *En près de trois ans, TikTok compte plus d'1,5 milliard d'utilisateurs mensuels (https://sensortower.com/blog/tiktok-revenue-downloads-2019).*

sanctions pécuniaires pouvant s'élever à un montant maximum équivalent à 7 millions de dollars,[83] chiffre qui reste toutefois nettement inférieur aux standards européens en la matière.[84]

Enfin, en Europe, de nombreux travaux ont été initiés à ce sujet. En France, l'Autorité de la concurrence, dans sa contribution au débat sur la politique de concurrence et les enjeux numériques du 19 février 2020,[85] suggère d'entamer une réflexion pour déterminer s'il faut assouplir le standard applicable à la notion d'infrastructure essentielle ou développer un nouveau standard afin de qualifier certains actifs « d'incontournables ».

Le 20 mai 2020, cette même autorité a lancé une enquête sectorielle « Fintechs » portant notamment sur des sujets tels que l'impact des évolutions technologiques sur les activités financières, en particulier dans le domaine des paiements.

Au niveau européen, le 15 décembre 2020, la Commission européenne a publié le *Digital Services Act* (« **DSA** »)[86] qui a pour objectif d'assurer un environnement concurrentiel équitable. Plus précisément, le DSA porte sur les services numériques et propose de mettre à jour la directive e-commerce de 2000,[87] époque à laquelle Facebook n'existait pas et Google avait à peine deux ans.

Le même jour, la Commission européenne a publié le *Digital Market Act* (« **DMA** »)[88] lequel a pour objet la mise en place d'une réglementation *ex ante* des plateformes structurantes ou « *gatekeepers* ». Il s'agira d'encadrer l'activité d'acteurs du numérique ayant acquis un fort pouvoir de marché, susceptible de conduire à terme à une position monopolistique difficile à remettre en cause.

On notera que la Commission européenne a identifié quatre services clés qui relèveront des règles de concurrence applicables aux plates-formes gatekeepers, dont les services de Cloud ; ces derniers ayant été ajoutés à la suite d'un amendement de compromis intervenu à la commission « *Internal Market and Consumer Protection* », le 30 septembre 2020[89].

---

[83] *Cf. Lettre du numérique citée supra en note n°81.*

[84] *En deux ans, la Commission européenne a infligé trois sanctions à Google pour un total de 8,2 milliards d'euros. V. Les Echos, L'Union européenne inflige à Google une nouvelle amende de 1,49 milliard d'euros, 20 mars 2019 (https://www.lesechos.fr/tech-medias/hightech/lue-inflige-a-google-une-nouvelle-amende-de-149-milliard-deuros-1002161).*

[85] *https://www.autoritedelaconcurrence.fr/sites/default/files/2020-02/2020.02.28_contribution_adlc_enjeux_num.pdf.*

[86] *Proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, 15 décembre 2020 (COM(2020) 825 final et 2020/0361 (COD)).*

[87] *Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur.*

[88] *Proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), 15 décembre 2020 (COM(2020) 842 final et 2020/0374 (COD)).*

[89] *Les trois autres services sont : les entreprises offrant des services d'intermédiation en ligne (notamment les places de marché, les magasins d'applications et les réseaux sociaux ; les moteurs de recherche en ligne ; et les systèmes d'exploitation.*

Enfin, rappelons que la Commission européenne a publié en octobre 2020 deux listes de pratiques illicites pour les *gatekeepers*.[90] La première liste (*blacklist*) porte sur des pratiques directement considérées comme déloyales et la seconde (*greylist*) énumère des pratiques déloyales pour lesquelles l'intervention du régulateur compétent est requise.

1.2 - Enjeux liés à l'extraterritorialité des législations procédurales et répressives américaines et à la souveraineté de l'UE en matière de protection des données : l'exemple USA-UE

L'origine non européenne des principaux Prestataires de Cloud, et leur soumission à des systèmes juridiques ne relevant pas de l'UE, interroge sur l'application de dispositions légales ou réglementaires étrangères entrant en conflit avec le droit de l'UE ou celui de ses États membres, telles que notamment, le RGPD, la loi de blocage de 1968,[91] le secret bancaire,[92] le secret des affaires,[93] etc.

Dans le contexte de la fourniture de services de Cloud par des Prestataires de Cloud à des banques devant répondre à des exigences réglementaires, une telle question ne peut en effet être éludée, notamment au regard des enjeux stratégiques que le Cloud suscite, non seulement en matière de contrôle de l'accès et de l'utilisation des données et de la préservation de leur confidentialité, sécurité et intégrité, mais également de manière plus générale, en termes de sécurité informatique. Compte tenu de la nationalité des trois Prestataires de Cloud les plus importants en termes de parts de marché, nous proposons de prendre en exemple le caractère extraterritorial de certaines lois américaines pour illustrer notre propos.[94]

1.2.1 - Collecte de données dans le cadre de procédures judiciaires américaines : CLOUD Act

L'extraterritorialité des lois américaines et la possibilité pour les autorités américaines d'accéder aux données ou à en demander la communication, n'est pas un sujet récent sur la scène européenne (voir paragraphe 1.2.2 - Collecte de données dans le cadre des textes américains dits de « surveillance » :

[90] *En se concentrant principalement sur les moteurs de recherche, les systèmes d'exploitation, les services de Cloud et les services d'intermédiation en ligne – DGs CNECT/GROW informal working document – List of (potentially) unfair practices - Blacklist/whitelist (unfair practices that are self-executing).*

[91] *Loi n°68-678 du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères.*

[92] *Articles L. 511-33 et L. 511-34 du Code monétaire et financier.*

[93] *Article L. 151-1 du Code de commerce.*

[94] *Étant entendu que le présent rapport n'a certes pas vocation à étudier la question de l'extraterritorialité des lois américaines en général.*

FISA, Patriot Act - ci-dessous). Toutefois, la promulgation aux États-Unis, le 23 mars 2018 du *Clarifying Lawful Overseas Use of Data Act* (ou « **CLOUD Act** »)[95] a mis en lumière les préoccupations des autorités nationales et européennes (voir paragraphe 1.1 - Marché oligopolistique : dépendance des banques dû à un faible nombre de Prestataires de Cloud - ci-dessus).

Le CLOUD Act permet aux autorités américaines, agissant par l'intermédiaire des autorités de poursuite civiles et pénales dans le cadre d'investigations criminelles concernant des « *serious crimes* », en vue d'obtenir, par voie notamment d'injonction, de la part de tout prestataire de services de communications électroniques et de tout prestataire de service informatique à distance soumis à la juridiction américaine qu'il communique les contenus d'une communication filaire ou électronique, tout enregistrement ou toute autre information, donnée portant sur un client ou abonné qu'il a en sa possession, sous sa garde ou sous son contrôle, quel que soit le lieu de stockage de ladite communication, enregistrement, information, donnée, *etc.*[96]

On relèvera que le CLOUD Act se différencie des autres textes dit extraterritoriaux (voir paragraphe 1.2.2 - Collecte de données dans le cadre des textes américains dits de « surveillance » : FISA, Patriot Act - ci-dessous), car, comme indiqué précédemment, il s'applique uniquement aux réquisitions judiciaires dans le cadre de procédures pénales pour lesquelles un juge américain est mandaté (équivalent des réquisitions judiciaires françaises)[97].

Le périmètre et les conditions d'application de ce texte laissent subsister des interrogations notamment quant à la notion exacte de *serious crime*,[98] aux garanties qui assortissent les décisions

---

[95] https://www.congress.gov/bill/115th-congress/house-bill/4943/text.

[96] *Paragraphe 2713 du Titre 18 du Code des États-Unis (U.S.C) : « A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States ». « Un prestataire de service de communications électroniques ou un prestataire de service informatique à distance se conformera aux obligations (…) de préserver, sauvegarder ou de divulguer les contenus d'une communication filaire ou électronique ainsi que tout enregistrement ou toute autre information portant sur un client ou abonné en possession, sous la garde ou sous le contrôle dudit prestataire, que ladite communication, ledit enregistrement ou ladite autre information, soit localisé(e) aux États-Unis ou en dehors des États-Unis ». Le CLOUD Act modifie le Stored Communication Act de 1986, qui protège les communications électroniques et définit les politiques de confidentialité et d'accès par des agences fédérales américaines, aux seules données détenues sur des serveurs hébergés aux États-Unis. Ce texte fait suite à la décision Microsoft de 2016 de la cour d'appel de New York qui a considéré qu'une réquisition judiciaire fondée sur le Stored Communication Act, contre un prestataire américain ayant refusé de communiquer des données relatives à un citoyen américain hébergées en Irlande et demandé d'emprunter la voie de la coopération judiciaire internationale (le Mutual Legal Assistance Treaty - «MLAT»), ne pouvait s'appliquer aux données stockées à l'étranger. La question devait être tranchée par la Cour Suprême, mais sans attendre cette issue, le Congrès a adopté le CLOUD Act le 23 mars 2018.*

[97] *On parle de subpoena qui est une injonction de comparaître devant un tribunal, soit pour y témoigner, soit afin de produire un document.*

[98] *Le CLOUD Act vise les « serious crime[s], including terrorism », ainsi que la notion de « threat of death or serious bodily harm to any person » - § 2523. Executive agreements on access to data by foreign governments - DEFINITIONS.- In this section, spéc. D et G. Pour une large définition, cf. l'article 37 du CFR (United States Code of Federal Regulations).*

de justice ordonnant la communication des données, l'absence de transparence du déroulé des opérations de transferts des données, informations ou enregistrements aux autorités américaines, ou encore la place laissée au chiffrement des données de nature à limiter ou empêcher la transmission par les prestataires soumis au CLOUD Act des données, informations ou enregistrements aux autorités américaines.[99]

Certains auteurs ont fait part de leur inquiétude soulevée par le caractère extraterritorial du CLOUD Act.[100]

Le CLOUD Act doit en tout état de cause être mis en perspective avec les textes nationaux et européens, notamment la loi de blocage de 1968 et le RGPD.[101]

Plusieurs initiatives législatives et réglementaires sont en cours pour répondre aux enjeux du CLOUD Act. En France, dans la continuité du rapport Gauvain, des réflexions ont débuté en vue d'un projet de révision de la loi de blocage de 1968 initié par les autorités françaises depuis 2019, sans toutefois se concrétiser, à ce jour, par un projet ou proposition de loi.[102] Au plan européen, l'option d'un accord bilatéral entre les États-Unis et l'UE,[103] notamment en vue d'assurer la conformité du CLOUD Act avec le RGPD,[104] a été envisagée.[105]

---

[99] R. Gauvain, C. d'Urso, S. Damais, Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises de lois et mesures à portée extraterritoriale, rapport à la demande du Premier ministre, Edouard Philippe, 26 juin 2019, Assemblée Nationale (https://www.vie-publique.fr/rapport/38473-proteger-nos-entreprises-des-lois-et-mesures-portee-extraterritoriale). Le rapport propose notamment de moderniser la loi de blocage de 1968 afin de réformer le droit français pour lutter contre l'extraterritorialité des poursuites étrangères et notamment américaines.

[100] Voir par exemple : F. Plénacoste et E. Daoud, CLOUD Act : des Inquiétudes légitimes, Dalloz IP/IT, n° 12, décembre 2018, p. 680; E. Jouffin et M. Abadie, Le cocktail détonnant du CLOUD Act, Extraterritorialité, sécurité nationale et libertés individuelles, Banque et Droit, novembre-décembre 2018, n° 182. Pour un propos plus nuancé, E. Mignon, Faut-il avoir peur du CLOUD Act ? Flash d'information, August & Debouzy, 25 juin 2018, voire rassurant : Microsoft, Faut-il avoir peur du CLOUD Act ?, 14 janvier 2020 (pour l'anecdote, Microsoft a été l'objet d'une procédure judiciaire aux États-Unis en raison de son refus de transmettre des données détenues en Irlande, approuvé par les juges d'appel, ce qui a suscité l'adoption du CLOUD Act).

[101] Ainsi l'article 48 du RGPD interdit la divulgation ou la transmission de données personnelles résultant d'une décision d'une juridiction ou d'une autorité administrative d'un pays tiers à l'exception que la demande soit fondée sur un accord international en vigueur entre le pays tiers et l'UE ou un État membre.

[102] Francis Lefebvre Formation, La protection des entreprises françaises contre les lois et mesures extraterritoriales : retour sur les propositions du Rapport Gauvain, 14 janvier 2020 (https://www.flf.fr/actualite/la-protection-des-entreprises-francaises-contre-les-lois-et-mesures-extraterritoriales).

[103] Le CLOUD Act offre un mécanisme, par lequel les États-Unis peuvent conclure des accords bilatéraux qualifiés d'executive agreements en principe avec d'autres pays [paragraphe 2523 du titre 18 du Code des États-Unis (U.S.C)].

[104] Un tel accord international est autorisé par le CLOUD Act ((1 8 U.S.C. § 2703(h)(2)) qui permet la conclusion d'un accord bilatéral avec un État en vue de faciliter les mesures d'obtention de preuves électroniques au niveau international afin de pallier les carences et insuffisances des MLAT actuels et l'article 48 du RGPD.

[105] Les États-Unis peuvent signer des accords bilatéraux avec d'autres pays (executive agreements), tels que l'accord conclu entre les États-Unis et le Royaume-Uni le 3 octobre 2019. Dans ce contexte, la question de l'application territoriale du CLOUD Act se pose dans des termes similaires si le prestataire, non américain, a son siège dans ce pays ou encore, quand bien même il n'aurait pas son siège dans un pays signataire d'un accord bilatéral, s'il sous-traite ses prestations auprès d'un prestataire qui a son siège dans un pays signataire.

Toutefois, ces discussions ont été freinées en raison de la difficulté de concilier des textes dont l'articulation revêt une certaine dose de défi, et d'initiatives menées parallèlement au niveau européen, la Commission européenne ayant présenté, le 17 avril 2018[106], une proposition de règlement « *E-evidence* »,[107] visant à rendre plus aisée et plus rapide pour les autorités policières et judiciaires des États membres l'obtention de preuves électroniques hébergées notamment par des Prestataires de Cloud, indépendamment de la localisation géographique de ces preuves. À ce jour, le règlement « *E–Evidence* » est toujours à l'état de proposition.[108]

Enfin, on notera au passage que le sujet du CLOUD Act apparaît en filigrane des partenariats avec des Prestataires de Cloud américains. En comparaison, certains acteurs européens du Cloud ne manquent pas de rappeler que ce texte ne les concerne pas en raison de leur localisation géographique et de l'absence d'appartenance à un groupe américain.[109]

1.2.2 - Collecte de données dans le cadre des textes américains dits de « surveillance » : FISA, Patriot Act

Comme évoqué précédemment (voir paragraphe 1.2.1 - Collecte de données dans le cadre de procédures judiciaires américaines : CLOUD Act - ci-dessus), le risque de captation des données en application de règlementations américaines extraterritoriales, n'est pas récent. En effet, la collecte de données aux fins d'activités de « surveillance » est notamment issue de textes plus anciens, tels que le *FISA Act* de 1978 (notamment section 702)[110] et le *Patriot Act* de 2001 (notamment section 215).[111]

Le *FISA Act* est sous les feux de l'actualité en étant clairement cité par la CJUE dans la décision Schrems II[112] rendue le 16 juillet 2020 ainsi que dans la décision en référé du Conseil d'État du

---

[106] *Voir communiqué de presse (IP/18/3343).*

[107] *Proposition de règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale (COM(2018) 225 final et 2018/0108 (COD)) (https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime/e-evidence_en).*

[108] *https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2018/0108 (COD)&l=en.*

[109] *Usine Digitale, GAIA-X OVH et T-systems s'allient pour former un cloud européen, 14 septembre 2020 (https://www.usine-digitale.fr/article/dans-le-cadre-de-gaia-x-ovhcloud-et-t-systems-s-allient-pour-fournir-un-cloud-public-europeen.N1004269) ; voir également, OVH.Cloud, CLOUD Act, Quel impact pour les utilisateurs de cloud, blog, 21 septembre 2018 (https://blog.ovh.com/fr/blog/quel-est-limpact-du-cloud-act-pour-les-utilisateurs-de-cloud/).*

[110] *La loi sur la surveillance du renseignement étranger (Foreign Intelligence Surveillance Act-FISA), votée en 1978, amendée plusieurs fois, décrit les procédures de surveillance physique et électronique, ainsi que la collecte d'information à l'étranger de manière directe ou indirecte.*

[111] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism. Ce texte a été réformé par le Freedom Act, et l'Executive order 12-333 de 1981, puis modifié en 2004 et 2008. Il renforce les pouvoirs de surveillance des services secrets et réduit les possibilités de contrôle que le Congrès et le pouvoir judiciaire peuvent exercer.*

[112] *Arrêt C-311/18 du 16 juillet 2020 - Data Protection Commissioner/Maximillian Schrems et Facebook Ireland.*

13 octobre 2020 concernant la plateforme de données de santé, Health Data Hub.[113]

La CJUE, dans sa décision (§ 180), souligne que « *l'article 702 du FISA ne fait ressortir d'aucune manière l'existence de limitations à l'habilitation qu'il comporte pour la mise en œuvre des programmes de surveillance aux fins du renseignement extérieur, pas plus que l'existence de garanties pour des personnes non-américaines potentiellement visées par ces programmes* ».

Dans une affaire concernant la Plateforme des données de santé (PDS), également appelée *Health Data Hub*, destinée à faciliter le partage des données de santé, afin de favoriser la recherche, le Conseil d'État relève pour sa part que, dans le traitement des données confiées à Microsoft, cette dernière est tenue par les termes d'un arrêté du 9 octobre 2020 postérieur à l'introduction de la requête, lequel prévoit qu' : « *Aucun transfert de données à caractère personnel ne peut être réalisé en dehors de l'Union européenne* ».[114]

La Haute juridiction précise que le traitement de ces données par Microsoft sur le territoire de l'UE ne constitue pas en lui-même une illégalité grave et manifeste, mais qu'il ne peut être totalement exclu que les autorités américaines, dans le cadre de programmes de surveillance et de renseignement, exigent de Microsoft et de sa filiale irlandaise l'accès à certaines données de santé.[115] Face à l'existence d'un tel risque, il est fait injonction à *Health Data Hub* de modifier son contrat avec Microsoft pour renforcer la protection des droits des personnes concernées sur leurs données.[116]

Les enjeux d'extraterritorialité sont donc bien présents et la possibilité d'accès dans l'UE à des données de citoyens européens par des autorités américaines ne peut pas être exclue.

1.2.3 - Invalidation du *Privacy Shield* par la CJUE

L'annulation du *Privacy Shield*, par la CJUE dans son arrêt Schrems II du 16 juillet 2020[117] souligne l'insuffisance de garanties fournies par les institutions américaines sur la protection des données personnelles et des intérêts des citoyens européens.

---

[113] *Conseil d'État, ordonnance du 13 octobre 2020, n° 444937, statuant en référé (https://www.conseil-etat.fr/actualites/actualites/health-data-hub-et-protection-de-donnees-personnelles-des-precautions-doivent-etre-prises-dans-l-attente-d-une-solution-perenne).*

[114] *Point 13 de la décision.*

[115] *Voir paragraphe 17 de l'ordonnance du Conseil d'État, mentionnant le fait que, d'un point de vue technique, Microsoft soit amené à faire droit à une demande des autorités américaines en application de l'article 702 du FISA, ce qui méconnaîtrait alors les articles 28 et 48 du RGPD.*

[116] *Article 1er de l'ordonnance du Conseil d'État.*

[117] *Arrêt C-311/18 - Data Protection Commissioner/Maximillian Schrems et Facebook Ireland.*

Des négociations entre les États-Unis et l'UE sur un nouvel accord international ont été initiées en août 2020.[118]

La genèse du *Privacy Shield* est éclairante pour illustrer les difficultés relatives à la sauvegarde de la protection des intérêts européens.

En juillet 2000, la Commission européenne avait considéré que l'accord États-Unis/UE dit *Safe Harbor* permettait le transfert licite de données personnelles entre ces deux pays, dès lors que l'entreprise américaine qui acquiert ces données adhérait à cet accord. Ce dernier, mis à mal en 2013 par les révélations d'Edward Snowden sur les programmes de surveillance de masse de la NSA,[219] a été invalidé par la CJUE le 6 octobre 2015,[120] au motif de l'insuffisance de la protection offerte par ce texte contre l'accès par les autorités américaines, aux données transférées vers ce pays.

Quelques mois de négociations plus tard, un nouvel accord était trouvé entre les deux blocs et signé le 12 juillet 2016,[121] le *Privacy Shield*. Cet accord devait renforcer les dispositions protectrices du *Safe Harbor*, mais souffrait in fine de critiques identiques.

Dans son arrêt du 16 juillet 2020, la CJUE a, pour invalider le *Privacy Shield*, invoqué notamment l'absence de garanties suffisantes contre les demandes d'accès des autorités ou institutions américaines, ainsi que l'impossibilité pour les citoyens européens de faire valoir leurs droits devant les tribunaux américains, entrainant l'interdiction de transmettre des données personnelles de l'UE vers les États-Unis sur le fondement de cet accord.

Cette même décision confirme la validité d'un autre outil qui permet de transférer de façon encadrée les données personnelles hors de l'Espace Économique Européen vers les États-Unis ou vers d'autres pays : les clauses contractuelles types adoptées par la Commission européenne.[122] Cette validation est toutefois soumise à la condition que la législation du pays qui reçoit les données assure une protection substantiellement équivalente à celle de l'UE.

La Commission européenne ainsi que le Comité Européen de la Protection des Données,[123] ont procédé à l'analyse de cette décision et ont publié respectivement un projet de nouvelles clauses

[118] *Communiqué de presse commun du Commissaire européen à la Justice Didier Reynders et du Secrétaire d'État américain au commerce Wilbur Ross du 10 août 2020.*

[119] *The National Security Agency (NSA) is a U.S. national-level intelligence agency of the Department of Defense, under the authority of the Director of National Intelligence.*

[120] *Arrêt C-362/14.*

[121] *Décision n° 2016/1250 relative à la non adéquation de la protection des données assurée par le Safe Harbor.*

[122] *Décision de la Commission du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil (JO 2010, L 39, p. 5), telle que modifiée par la décision d'exécution (UE) 2016/2297 de la Commission du 16 décembre 2016 (JO 2016, L 344, p. 100).*

[123] *Réunit toute les autorités de protection des données européennes, dont la CNIL en France. Il veille à ce que le RGPD soit appliqué de manière cohérente dans les pays de l'UE, ainsi qu'en Norvège, au Liechtenstein et en Islande.*

contractuelles types adaptées à cette décision[124] ainsi que des recommandations relatives à des mesures complémentaires pour accompagner la mise en place de ces clauses.[125] Ces publications sont soumises à consultation publique.

Néanmoins, l'adoption de la version définitive des nouvelles clauses contractuelles types se fait attendre et ce retard maintient dans l'insécurité juridique les responsables de traitement de données personnelles et les sous-traitants réalisant des transferts de données hors de l'Union européenne.

Sous l'égide de *BusinessEurope*, une déclaration commune de plusieurs associations professionnelles européennes a été adressée au Comité Européen à la Protection des Données, afin de l'alerter sur l'impossibilité pratique de mettre en œuvre les dernières recommandations concernant les mesures complémentaires.[126]

On notera enfin que les tensions autour de l'accès aux données personnelles par la communauté du renseignement américain se cristallisent notamment autour de la notion de sécurité nationale. L'*executive order* du Président Biden du 12 mai 2021[127] sur l'amélioration de la cybersécurité du pays (« Cyber EO ») offre un exemple de cette question.

Le Cyber EO a pour objet de renforcer la cyber-résilience des agences gouvernementales américaines en leur fixant divers objectifs précis concernant, notamment, leurs fournisseurs de services de Cloud. La section 2 « *suppression des obstacles au partage des informations sur les menaces* », entend accentuer ce partage, jugé restreint du fait des termes contractuels (*contract language*).[128] Des textes sont attendus, d'une part afin de s'assurer que les règles relatives aux marchés publics seront amendés afin que les fournisseurs s'engagent à prendre des mesures pour collecter, préserver et partager les informations avec les agences fédérales américaines et d'autre part, afin de préciser quels entreprises seront concernées par ces exigences. Toutefois, ce texte va au-delà du périmètre des prestataires technologiques des agences gouvernementales.

D'une part, le communiqué de presse de la Maison Blanche[129] appelle globalement le secteur privé à « suivre l'exemple du gouvernement fédéral et à prendre des mesures ambitieuses pour augmenter

---

[124] *Commission implementing decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.*

[125] *European Data Protection Board, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data et Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.*

[126] *https://www.businesseurope.eu/sites/buseur/files/media/public_letters/imco/2020-09-30_mbe-a.jelinek_-_european_data_protection_board.pdf.*

[127] *Executive Order on Improving the Nation's Cybersecurity (https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/).*

[128] *Ce texte peut s'appuyer sur une loi de 2015 (S.754 - Cybersecurity Information Sharing Act of 2015) visant à « Améliorer la cybersécurité aux États-Unis par un meilleur partage de l'information sur les menaces de cybersécurité, et à d'autres fins ».*

[129] *https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/.*

et aligner les investissements en matière de cybersécurité dans le but de minimiser les incidents futurs ». Par ailleurs, la section 4 du Cyber EO évoque une labélisation « *energy star* », afin que le public soit informé du fait qu'un logiciel a été développé en conformité avec les exigences de sécurité *ad hoc*, démontrant ainsi que les marchés publics ne sont pas les seuls concernés par les initiatives portées par le décret présidentiel du 12 mai.

En outre, le fait que soient évoqués[130] des principes techniques tels que le recours à des architectures « *zéro confiance* »[131], des pratiques d'authentification multi-facteurs et de chiffrement des données, démontre la volonté de fixer des standards. Enfin, on ne peut exclure que, par « capillarité », les clauses qui seront imposées aux grands fournisseurs du gouvernement américain (dont les GAFAM) puissent ensuite être opposées par ces dernier à leurs clients, relançant ainsi les discussions au sujet de la perméabilité des entreprise européennes aux réglementations de portée extraterritoriale. Cette préoccupation transparaît dans l'annonce faite le 17 mai 2021 relative à la stratégie de la France en matière de Cloud. L'un des trois axes de cette stratégie étant un « Cloud de confiance » fondé sur le label ANSSI SecNum Cloud, les données devant être localisées et exploitées dans des infrastructures en Europe.[132]

1.3 - Enjeux de sécurité

Les enjeux de sécurité des infrastructures de Cloud résonnent actuellement de manière plus concrètes compte tenu des nombreux évènements faisant l'actualité, préoccupant désormais tant le co-contractant du prestataire de Cloud que le client ou utilisateur final du service, qui en subissent également toutes les conséquences.

La technologie du Cloud, bien que virtuelle, présente des facteurs de risque bien réels et multiples qui exigent que la sécurité doit être dans le Cloud, pour éviter les risques accidentels et à l'extérieur du Cloud pour parer les menaces malveillantes des activités de piratages informatiques.

Les menaces internes et externes au Cloud peuvent causer des dommages considérables sur les systèmes et créer des pertes de confidentialité, de disponibilité ou d'intégrité des services/données. Le périmètre de sécurité à mettre en œuvre est donc vaste et porte tant sur les infrastructures matérielles/immatérielles que les ressources humaines des prestataires de services de Cloud et

[130] *Section 3. Modernisation de la cybersécurité du gouvernement fédéral.*

[131] *Zero trust : aucune confiance n'est accordée par défaut à un terminal qui se connecte au réseau interne ou à l'extérieur. Les droits ne sont accordés qu'en fonction d'une évaluation du risque dynamique, et l'utilisateur ne possède que des droits minimaux nécessaires et sur un périmètre limité.*

[132] *Voir note de bas de page n° 142 en page 37.*

de leurs clients. La longue liste des critères de sécurité comprend notamment : la qualification des personnels, la protection des centres de données physiques, la robustesse et fiabilité des infrastructures, la surveillance, etc.

Les répercussions des failles de sécurité de toutes nature des infrastructures de Cloud sont conséquentes pour les clients directes et indirectes des prestataires de Cloud.

L'actualité est riche en incidents marquant qui semblent s'enchainer de manière exponentielle depuis un recours au Cloud plus systématique de tous secteurs de l'économie. En 2019, la fuite de données personnelles massives de 100 millions de clients américains (soit un peu moins d'un tiers de la population des États-Unis) et 6 millions de clients canadiens de la Banque *Capital One* et détenues par son fournisseur de Cloud a contribué à une prise de conscience collective de l'importance du sujet de la sécurité informatique.[133] L'affaire interpellant particulièrement, dans la mesure où l'auteur n'avait pas, selon les enquêteurs, le profil d'un cybercriminel de haut vol mais plutôt d'un amateur qui aurait tiré profit d'une mauvaise configuration du *firewall* du serveur de la banque.[134] La banque américaine s'est vue infliger une amende de 80 millions de dollars pour avoir négligé sa cybersécurité.[135]

L'incendie des locaux abritant une partie des serveurs d'OVH Cloud en mars 2021[136], pouvant être qualifié de catastrophe industrielle, entrainant la destruction des serveurs, l'incapacité de récupérer des données, l'indisponibilité sur du long terme, l'inaccessibilité à certains sites internet participe également largement à cette inquiétude généralisée.

Enfin, plus récemment en mai 2021, AXA a été victime d'une attaque ciblée par « *ransomware* » qui a touché ses opérations informatiques en Asie du Sud-Est.[137] Les pirates menacent contre rançon de faire fuiter les 3 téraoctets (To) de données personnelles des clients.

Néanmoins, les banques sont certainement parmi les secteurs les plus sensibilisés et matures quant au niveau de protection exigé. La mobilisation est forte sur tous les sujets sécurité pour apporter des garanties nécessaires à la confiance et la viabilité de cette technologie.

---

[133] Reuters, Capital One customer data breach rattles investors, 30 juillet 2019 ; J. Raynal, Piratage bancaire : comment 100 millions de personnes ont été touchées par un vol de données, La Tribune, 30 juillet 2019 ; H. Murphy et S. Bond, Capital One data breach sparks cloud security fears, Financial Times, 31 juillet 2019.

[134] R. McMillan, How the Accused Capital One Hacker Stole Reams of Data From the Cloud, Wall Street Journal, 4 août 2019.

[135] K. Wack, Capital One to pay $80M in connection with massive data breach, American Banker, 6 août 2020.

[136] Le site de l'entreprise OVH à Strasbourg touché par un « important incendie », Le Monde, 10 mars 2021 ; R. Loukil, Les leçons tirées par OVH de l'incendie de son datacenter à Strasbourg, l'Usine Nouvelle, 23 mars 2021.

[137] B. de Meyer, L'attaque contre Axa souligne les risques cyber planant sur le secteur financier, L'Agefi, 18 mai 2021 ; R. Gueugneau, Une filiale d'AXA victime d'une cyberattaque en Asie, Les Échos, 16 mai 2021.

Les gouvernements nationaux et autorités européennes sont fortement impliqués dans la construction européenne d'un Cloud de confiance répondant aux exigences de sécurités technologiques.

En réponse à ces enjeux, plusieurs actions sont menées concomitamment sous différentes formes, nous en rappellerons les principales :

Sur le terrain législatif :

• la révision de la Directive NIS[138] est engagée par les travaux européens pour renforcer les mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information au sein de l'UE.[139] Cette révision est accompagnée d'un nouveau projet de directive dédié à la résilience informatique dans le secteur financier ;[140]

• l'adoption du *Cybersecurity Act*[141] en 2019 encourage le recours à la certification et la reconnaissance des certificats délivrés par un État membre dans toute l'UE, contribuant de fait à renforcer la sécurité du marché unique numérique européen. Véritable avancée pour l'autonomie stratégique européenne, ce règlement présente un double volet : l'adoption du mandat permanent de l'ENISA, l'Agence européenne pour la cybersécurité, et la définition d'un cadre européen de certification de cybersécurité ; et

• enfin le Règlement DORA, auquel la Section 3 (Vers un nouveau paradigme réglementaire en matière d'externalisation informatique dans le secteur financier : le Règlement DORA) est consacrée, qui prévoit notamment les obligations de sécurité et de résilience que les entités financières devront respecter afin d'assurer la maîtrise des risques liés à leurs dispositifs d'infrastructure informatique, dont le Cloud.

Sur le terrain de la certification :

Sur la base du *Cybersecurity Act*, l'ENISA s'est vu confier la mission de préparer un schéma européen de certification de cybersécurité pour les services Cloud par la Commission européenne. Ce schéma de certification permettra aux Prestataires de Cloud d'assurer la conformité de leurs services par rapport à des exigences spécifiques et uniques à travers l'Union européenne, visant à garantir un haut niveau de sécurité et la confiance dans ces services.

De nombreux schémas de certification existent à travers les différents États membres, comme, entre autres, C5 de BSI en Allemagne, SecNumCloud de l'ANSSI en France et ENS de l'OC-CCN

[138] *Cf. note de bas de page n° 7 en page 3.*

[139] *Cf. note de bas de page n° 8 en page 3.*

[140] *Cf. note de bas de page n° 12 en page 3.*

[141] *Règlement (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) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) No 526/2013 (règlement sur la cybersécurité).*

en Espagne.[142] Bien que ces schémas de certification aient le même objectif, ils ont une approche et des exigences différentes. Par conséquent, une fragmentation importante du marché intérieur relatif aux technologies de l'information et de la communication peut être constatée. Les prestataires de services qui ont l'intention de fournir des services Cloud dans d'autres États membres sont donc exposés à des conditions et contraintes différentes.

Pour résoudre ces problèmes, un schéma européen de certification de cybersécurité pour les services de Cloud commun va être conçu pour uniformiser le marché. L'objectif est d'offrir un cadre juridique unique, de renforcer la confiance, ainsi que la transparence dans le marché intérieur. Ce nouveau schéma de certification se basera sur les cadres existants, tels que les schémas de certification « Cloud » des différents États membres, des normes et des règles techniques.

Le Projet Gaia-X

En octobre 2019, un projet d'infrastructure de données européennes a été présenté à Dortmund lors du Sommet sur le numérique, initiant ainsi le projet de coopération franco-allemand GAIA-X officialisé le 4 juin 2020.[143] Les représentants de plusieurs entreprises européennes et internationales, ainsi que des organisations scientifiques collaborent en vue de construire une infrastructure de données fiable et sécurisée européenne. Plusieurs entreprises européennes se sont rassemblées en vue de contribuer au projet GAIA-X en matière de partage des données (*data sharing*). Dans ce cadre, les participants visent à élaborer un rapport sur les écosystèmes et les exigences des utilisateurs, non seulement dans le secteur financier, mais aussi dans d'autres domaines tels que l'industrie 4.0 (à savoir par exemple la fabrication intelligente, la logistique collaborative dans un secteur connecté ou encore la maintenance collaborative), le secteur de la santé, le secteur public, le *smart living*, l'énergie, la mobilité ou encore l'agriculture.

---

[142] On relèvera à cet égard que la France vient d'annoncer sa stratégie en matière de Cloud (communiqué de presse : https://minefi.hosting.augure.com/Augure_Minefi/r/ContenuEnLigne/Download?id=B32CFA9B-74D2-411D-A501-82041939FC67&filename=1002%20-%20Le%20Gouvernement%20annonce%20sa%20strat%C3%A9gie%20nationale%20pour%20le%20Cloud.pdf, et dossier de presse : https://minefi.hosting.augure.com/Augure_Minefi/r/ContenuEnLigne/Download?id=5D2238B1-0260-4705-8793-AAF280A29F58&filename=Strat%C3%A9gie%20nationale%20pour%20le%20Cloud.pdf). Cette stratégie s'articule autour de trois axes : (i) le Label « Cloud de confiance » fondé sur le label ANSSI SecNum Cloud, les données devant être localisées et « logées » dans des infrastructures en Europe ; (ii) le « Cloud au centre » afin d'accélérer l'évolution numérique de l'État par la mise en œuvre des engagements du Gouvernement en matière de transformation numérique des administrations. Les services numériques des administrations seront hébergés sur l'un des deux Cloud interministériels internes de l'État ou sur les offres de Cloud proposées par les industriels satisfaisant des critères stricts de sécurité ; et (iii) « stratégie industrielle ambitieuse » qui identifiera et soutiendra des projets industriels de développement de technologies Cloud en France.

[143] Gaïa X, FAQs on the GAIA-X project (https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/FAQ/faq-projekt-gaia-x.html) ; Vie Publique, Souveraineté numérique : Gaïa-X, le futur Cloud européen bientôt lancé ? (https://www.vie-publique.fr/en-bref/277330-souverainete-numerique-gaia-x-le-futur-cloud-europeen-bientot-lance) ; voir : Fagot, Cloud européen : l'alliance Gaia-X prend son envol, Le Monde, 20 novembre 2020.

Cette plateforme permettra de référencer des services de *Cloud computing* respectant un cahier des charges en termes de sécurité, d'interopérabilité, de transparence et de confiance, en s'appuyant sur les standards et normes techniques, sectoriels et réglementaires. Les membres de l'organisation s'engagent à garantir la transparence et la sécurité en vue de favoriser le développement d'un écosystème numérique interopérable fédéré européen.

1.4 - Enjeux de conformité pour les banques ayant recours à des Prestataires de Cloud

Comme dans toute industrie, une forte concentration des acteurs a pour conséquence inévitable d'introduire un certain déséquilibre dans le rapport de force contractuel. Le Cloud bancaire n'échappe pas à la règle et les banques éprouvent en effet des difficultés à négocier leurs contrats avec les Prestataires de Cloud, comme la presse s'en est faite l'écho,[144] et comme les autorités le reconnaissent elles-mêmes.[145]

L'enjeu n'est pas que commercial. En effet, comme discuté plus loin dans le présent rapport, les banques ont l'obligation d'inclure certaines clauses dans les contrats qu'elles concluent généralement avec des prestataires de service auxquels elles confient la réalisation de *fonctions critiques ou importantes.*[147] Ces clauses sont destinées à permettre à la banque, et par ricochet, l'autorité qui la supervise, de contrôler les conditions dans lesquelles les prestations externalisées sont réalisées. Or, le recours par les banques à des services de Cloud relève de cette obligation.[148]

On peut relever parmi les clauses dont l'inclusion dans les contrats d'externalisation de service de Cloud des banques s'impose,[149] celles qui soulèvent certaines difficultés de négociation :

• l'autorisation expresse d'une sous-externalisation d'une fonction critique ou importante, ou de parties significatives de celle-ci, ainsi que les conditions particulières liées ;

---

[144] *Les Échos, Pourquoi le Cloud est un casse-tête pour les banques, 4 août 2019 ; Les Échos, Cloud : la réglementation appliquée aux banques se précise peu à peu, 22 octobre 2018, citant les négociations entre grandes banques françaises et AWS et Microsoft Azure.*

[145] *Voir ACP-Banque de France, Les risques associés au Cloud computing, Analyses et synthèses n° 16, juillet 2013, p. 10 (https://acpr.banque-france.fr/les-risques-associes-au-cloud-computing-juillet-2013). Plus récemment, voir Commission, Commission staff working document, Impact assessment accompagnying the document Proposal for a Regulation of the European Parliament and of the Council on digital resilience for the financial sector, 24 septembre 2020 (SWD(2020) 198 final.*

[146] *Voir paragraphe 2 (L'appréhension du Cloud par la réglementation bancaire).*

[147] *ABE, Orientations relatives à l'externalisation, 25 février 2019 (EBA/GL/2019/02) (voir, spéc. §29 à 31 sur la notion de fonctions critiques ou importantes), lesquelles s'articulent, en France, avec les dispositions de l'arrêté du 3 novembre 2014 (en particulier les articles 238 et suivants). Pour plus de détails sur la réglementation applicable en France, voir paragraphe 2.2.1 (La situation en France) ci-dessous.*

[148] *Voir paragraphes 2.1 (Cadre réglementaire de l'UE : une évolution progressive et limitée) et 2.2 (Au niveau des États membres : un cadre réglementaire hétérogène) ci-après.*

[149] *Cf. paragraphe 13 (Phase contractuelle) des Orientations sur l'Externalisation.*

• le(s) lieu(x) (c'est-à-dire les régions ou pays) où la fonction critique ou importante sera assurée et/ou où les données pertinentes seront conservées et traitées, y compris le lieu de stockage éventuel, et les conditions à remplir, y compris l'obligation d'informer la banque si le prestataire de services envisage de modifier le(s) lieu(x) ;

• les dispositions concernant l'accessibilité, la disponibilité, l'intégrité, la confidentialité et la sécurité des données pertinentes ;

• le droit de la banque de contrôler en permanence les performances du prestataire de services ;

• les niveaux de service convenus, qui devraient inclure des objectifs de performance quantitatifs et qualitatifs précis pour la fonction externalisée afin de permettre un suivi en temps utile, de sorte que des mesures correctives appropriées puissent être prises dans les meilleurs délais si les niveaux de service convenus ne sont pas respectés ;

• les obligations de *reporting* du prestataire de services envers la banque, y compris la communication par le prestataire de services, de tout fait nouveau susceptible d'avoir une incidence significative sur sa capacité à exercer efficacement la fonction critique ou importante selon les niveaux de service convenus et conformément aux lois et aux exigences réglementaires applicables et, le cas échéant, l'obligation de présenter des rapports de la fonction de contrôle interne du prestataire de services ;

• l'obligation de mettre en œuvre et de tester les plans d'urgence de continuité de l'activité ;

• des dispositions garantissant l'accès aux données appartenant à la banque en cas d'insolvabilité, de résolution ou d'interruption des activités commerciales du prestataire de services ;

• l'obligation de faciliter le transfert de la fonction externalisée vers un autre prestataire de services ou la ré-internalisation de la fonction au sein de la banque concernée ;

• l'obligation pour le prestataire de services de coopérer avec les autorités compétentes et les autorités de résolution de la banque, y compris avec les autres personnes désignées par celles-ci ;

• l'élaboration, avec la banque concernée, de stratégies de sortie ;

• pour les établissements, une référence claire aux pouvoirs de l'autorité nationale de résolution, en particulier aux articles 68 et 71 de la directive 2014/59/UE (directive BRRD), et notamment une description des « obligations essentielles » du contrat au sens de l'article 68 de ladite directive ;

• le droit inconditionnel de la banque et des autorités compétentes d'inspecter et d'auditer le prestataire de services en ce qui concerne, en particulier, la fonction critique ou importante externalisée.

La consultation réalisée par la Commission européenne en amont du projet de règlement européen sur la résilience opérationnelle numérique dans le secteur financier (le « **Règlement DORA** »)[150] a souligné les difficultés éprouvées par les acteurs du secteur financier (dont les banques) à négocier ces clauses dans leurs contrats, notamment avec les Prestataires de Cloud : « *Most respondents have experienced difficulties during contractual negotiations with ICT TPPs* [*Information and Communication Technology* (ICT) *Third Party Providers* (TPP)]. *They pointed out to several aspects as being difficult to negotiate, such as for instance: (i) ICT and security related legal obligations imposed by the national or EU supervisory authority (e.g. 2019 EBA Outsourcing Guidelines), (ii) regular and mandatory audit clauses /right to audit (especially with the larger global CSPs [Cloud Services Providers]), (iii) geographical storage of data (e.g. GDPR requirements), (iv) sub-contractor approvals, (v) customer and its external auditors subcontracting information and control rights, (vi) information rights, (vii) exit strategies for SaaS products, (viii) post-termination assistance, (ix) resolution requirements under BRRD directive, (x) business continuity clause, (xi) penalties for non-compliance with SLAs and (xii) transparency on processing orders to subcontractors and outsourcing chains that lead abroad, etc.* »[151]

L'absence ou le défaut de conformité de ces clauses dans les contrats d'externalisation de prestations de services ou autres tâches opérationnelles essentielles ou importantes expose les banques à un risque de sanction administrative,[152] voire de mise en jeu de leur responsabilité, notamment à l'égard de leurs clients. Cette situation est asymétrique puisque les Prestataires de Cloud, comme généralement, la plupart des sous-traitants de banques, ne sont pas assujettis aux règles imposées au secteur bancaire. Au surplus, les failles évoquées dans l'encadrement contractuel de l'externalisation remettent en cause le contrôle et le suivi indirect des activités externalisées des banques exercés par les autorités de supervision.

En conclusion, tous ces enjeux, et en particulier le dernier, illustrent les limites atteintes par la réglementation bancaire actuellement en vigueur qui, bien qu'ayant cherché à s'adapter au phénomène nouveau du Cloud, s'est révélée incomplète.

---

[150] *Pour une présentation et une discussions détaillées de ce projet de règlement, voir la section 3 ci-après.*

[151] *Commission, Staff working document, op. cit., p. 76. V. également, p. 19 : « financial institutions often have difficulties in negotiating written agreements tailored to their prudential legal and regulatory requirements or cannot fully enforce rights of access as stipulated in contracts with ICT TPPs. Their initial contract with the TPP often does not provide for sufficient safeguards on how the sub-outsourcing process should be monitored (i.e. no notification of the sub-outsourced services, lack of relevant information on the type of function further sub-outsourced or on the actual location or jurisdiction where the sub-outsourcing is performed). This may be the result of a high degree of asymmetry in negotiating positions between financial institutions and hyper-scale technology providers, which leads to contractual limitations or gaps (e.g. on rights to access, audit and obtain information from TPPs. »*

[152] *ACPR, Décision n° 2019-04, Only Payment Services, grief n° 7 (en l'occurrence toutefois, c'est l'absence de formalisation par écrit du contrat d'externalisation qui a été sanctionnée).*

II- L'appréhension du Cloud par la règlementation bancaire : entre morcellement et hétérogénéité

Face à l'engouement des acteurs pour le Cloud bancaire et aux enjeux que son utilisation présente, la réglementation bancaire s'est progressivement construite pour appréhender ce phénomène. Élaborée dans un premier temps à deux niveaux (au niveau européen (**2.1**) et au niveau des législations nationales (**2.2**)), elle présente certaines faiblesses. La nécessité de changement de paradigme s'est imposée, délaissant le terrain étroit des règles de l'externalisation, pour atteindre un véritable encadrement du risque sur les tiers Prestataires de Cloud (**2.3**).

2.1 - Cadre réglementaire de l'UE : une évolution progressive et limitée

Au niveau européen tout d'abord, le superviseur bancaire a marqué son attention au développement de l'externalisation, qui a donné lieu en Europe à des lignes directrices du CEBS en 2006.[153] Le principe général de ces lignes directrices a été que les établissements devaient garder la maîtrise de leurs prestations externalisées, notamment par l'instrument des contrats avec leurs prestataires de services. Ces dispositions ont été générales et ne se sont pas focalisées sur l'informatique. Il convient de rappeler qu'à l'époque, le CESB n'était qu'un comité consultatif de la Commission européenne (qualifié de « comité de niveau 3 », issu de la réforme inspirée du rapport Lamfalussy[154]), dépourvu de tout pouvoir normatif ou de supervision.[155] Ce n'est qu'à partir du 2010, à la suite des recommandations du rapport de Larosière,[156] que le CESB, en devenant l'ABE[157], a acquis le statut d'autorité européenne de supervision dotée de certains pouvoirs normatifs, dont celui d'émettre des orientations ou des recommandations.[158]

Au regard de l'importance croissante du recours au Cloud bancaire par les banques et des risques qui leurs sont associés, l'ABE a lancé une consultation concernant un projet de recommandations

---

[153] *CESB, Guidelines on outsourcing, 14 December 2006 (https://eba.europa.eu/sites/default/documents/files/documents/10180/104404/6300a204-2d64-494f-b81e-fd3e235a74bb/GL02OutsourcingGuidelines.pdf.pdf?retry=1).*

[154] *Final report of the committee of wise men on the regulation of european securities markets, sous la direction de A. Lamfalussy, 15 février 2001 (https://www.esma.europa.eu/sites/default/files/library/2015/11/lamfalussy_report.pdf).*

[155] *V. Commission européenne, https://ec.europa.eu/info/business-economy-euro/banking-and-finance/regulatory-process-financial-services/regulatory-process-financial-services_en#the-lamfalussy-architecture).*

[156] *Report of the high-level group on financial supervision in the EU, chaired by Jacques de Larosière, 25 février 2009 (https://ec.europa.eu/economy_finance/publications/pages/publication14527_en.pdf).*

[157] *De même pour le Comité européen des régulateurs de marchés de valeurs mobilières (CERVM, devenu l'AEMF) et le Comité des contrôleurs d'assurance et de pensions professionnelles (CCAPP, devenu l'AEAPP).*

[158] *Règlement (UE) No. 1093/2010 du Parlement européen et du conseil du 24 novembre 2010, instituant une Autorité européenne de surveillance (Autorité bancaire européenne). Voir article 16 qui lui donne le pouvoir d'émettre des orientations et des recommandations à destination des autorités nationale de supervision bancaire et des établissements financiers.*

relatives à l'externalisation vers des Prestataires de Cloud, le 17 mai 2017.[159] Les recommandations finales ont été publiées dans leur version définitive le 28 mars 2018.[160]

Ces recommandations ont précisé les orientations du CESB de 2006. Elles concernaient en particulier l'évaluation du caractère critique des activités externalisées, la notification au superviseur national compétent des activités externalisées pertinentes et la mise à disposition d'un registre des dispositifs d'externalisation, la localisation et la conformité du traitement des données, la sécurité des systèmes d'information, la prise en compte des risques et l'encadrement contractuel de l'externalisation en chaîne, la mise en œuvre contractuelle d'un droit d'audit effectif au bénéfice de l'établissement supervisé et des autorités compétentes sur les Prestataires de Cloud, et enfin, l'application de plans de continuité de l'activité et de plans de réversibilité.

Le traitement spécifique réservé au Cloud fut toutefois de courte durée. En effet, l'ABE décida finalement d'intégrer le Cloud au régime général de l'externalisation à l'occasion de l'élaboration des orientations relatives à l'externalisation (les « **Orientations sur l'Externalisation** ») qui devaient abroger et remplacer les orientations du CESB de 2006.[161] Les Orientations sur l'Externalisation sont entrées en vigueur le 30 septembre 2019.[162] Elles prévoient un cadre organisationnel et contractuel harmonisé pour l'ensemble des activités externalisées par les banques et les autres entreprises du secteur bancaire.[163] Les Orientations sur l'Externalisation ont repris en substance les

[159] *ABE, Consultation paper on Draft recommendations on outsourcing to cloud service providers under Article 16 of Regulation (EU) No 1093/2010 (EBA/CP/2017/06), 17 mai 2017 (https://eba.europa.eu/sites/default/documents/files/documents/10180/1848359/c1005743-567e-40fc-a995-d05fb93df5d1/Draft%20Recommendation%20on%20outsourcing%20to%20Cloud%20Service%20%20%28EBA-CP-2017-06%29.pdf).*

[160] *ABE, Recommandations sur l'externalisation vers des fournisseurs de services en nuage, ABE/REC/2017/03 (https://eba.europa.eu/sites/default/documents/files/documents/10180/2170125/de3571be-cdba-4c42-997e-98ec85eac7c2/Recommendations%20on%20Cloud%20Outsourcing%20(EBA-Rec-2017-03)_FR.pdf). Il est intéressant de relever que ces recommandations ont adopté comme définition du « Cloud computing » la définition harmonisée qui a été élaborée par US National Institute of standards and technology (NIST) et qui définit également les modèles de déploiement du Cloud, i.e. public, privé, hybride, communautaire) et les modèles de services. Voir pour référence US NIST, The NIST Definition of Cloud Computing, Special Publication 800-145.*

[161] *ABE, Orientations relatives à l'externalisation (EBA/GL/2019/02), 25 février 2019 (https://eba.europa.eu/sites/default/documents/files/documents/10180/2761380/6565c789-487b-4528-8a17-4b94147dc5b8/EBA%20revised%20Guidelines%20on%20outsourcing_FR.pdf). Ces orientations abrogent et remplacent également les orientations du CESB relatives à l'externalisation de 2006.*

[162] *Sous réserve de certaines recommandations, qui font l'objet d'un régime transitoire distinct et seront pleinement effectives au-delà du 31 décembre 2021. Elles sont applicables dès le 30 septembre 2019 pour tous les accords d'externalisation conclus, révisés ou modifiés à cette date et à partir du 31 décembre 2021 pour le stock des contrats en cours.*

[163] *À savoir, les entreprises d'investissement relevant de la directive CRD IV, les établissements de paiement et les établissements de monnaie électronique. Il convient de noter que les entreprises d'investissement (ainsi que les établissements de crédit fournissant des services d'investissement ou commercialisant des dépôts structurés au sens MIF2) sont soumises aux articles 30 à 32 du règlement délégué (UE) 2017/565. Les deux autres autorités européennes de supervision sectorielles que sont l'AEAPP et l'AEMF, ont récemment publié des orientations spécifiques, inspirées des recommandations de l'ABE de 2018 relatives à l'externalisation vers des Prestataires de Cloud : L'AEAPP a ainsi publié des orientations relatives à la sous-traitance à des Prestataires de Cloud le 6 février 2020 (EIOPA-BoS-20-002) et l'AEMF a publié le rapport final des orientations relatives à l'externalisation vers des Prestataires de Cloud le 18 décembre 2020 (ESMA50-1157/2403).*

recommandations de l'ABE publiées en 2018 mentionnées plus haut.[164]

Cependant, les règles posées par les Orientations sur l'Externalisation ne sont pas écrites « en dur » puisqu'elles ne figurent pas dans un texte de l'UE à valeur obligatoire dans l'ordre juridique des États membres (directive ou règlement). En effet, s'ils doivent tout mettre en œuvre pour respecter ces orientations, les autorités compétentes des États membres et les établissements financiers peuvent toutefois décider de ne pas s'y conformer, en justifiant de leurs raisons de ne pas le faire (procédure dite de « *comply or explain* »).[165]

Cela dit, il convient de noter que, contrairement à la matière bancaire, certaines directives européennes sectorielles comprennent des dispositions sur l'externalisation. C'est ainsi le cas dans le domaine de l'assurance[166] et des marchés financiers.[167] Pour autant, la même critique peut être formulée à l'égard des orientations sur le Cloud émanant des autorités relevant de ces deux secteurs (L'AEAPP et l'AEMF) : elles n'ont pas plus de force contraignante que les Orientations sur l'Externalisation. Au surplus, une approche sectorielle reflétée par les orientations des trois autorités européennes est de nature à créer des risques de chevauchement et de divergences préjudiciables aux banques dont les activités relèvent plusieurs règlementations sectorielles (par exemple, la bancassurance ou les banques prestataires de services d'investissement).[168]

Il suffit d'observer brièvement la situation au niveau des États membres, pour constater à quel point la réglementation manque d'homogénéité.

2.2 - Au niveau des États membres : un cadre réglementaire hétérogène

2.2.1 - La situation en France

Si l'on regarde en France tout d'abord, on observera que, bien avant les orientations du CESB de 2006, le règlement CRBF n° 97-02 du 21 février 1997 (le « **Règlement 97-02** »)[169] prévoyait à cette époque un régime juridiquement contraignant de l'externalisation des activités bancaires, en référence à des *prestations de services essentielles externalisées* (« **PSEE** »).

---

[164] *Néanmoins, plusieurs terminologies liées au Cloud demeurent définies dans les Orientations sur l'Externalisation et deux paragraphes font référence à l'externalisation vers un Prestataire de Cloud, ou « externalisation en nuage » (i.e. paragraphes 54 (h), 82, 83 et 97).*

[165] *Article 16, §(3) et (4) du règlement (UE) No. 1093/2010. Voir, pour une description appliquée au secteur bancaire en France, ACPR, https://acpr.banque-france.fr/europe-et-international/banques/reglementation-europeenne/orientations-de-lautorite-bancaire-europeenne).*

[166] *Directive 2009/138/CE du Parlement européen et du Conseil du 25 novembre 2009 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice (solvabilité II), spéc. article 49 et règlement délégué (UE) 2015/35 de la Commission, article 274).*

[167] *MIF 2, article 16(5) et le règlement délégué (UE) 2017/565 de la Commission, les articles 30 à 32.*

[168] *Voir à propos du projet d'orientations sur le Cloud de l'AEMF, la réponse à la consultation de l'EBF (https://www.ebf.eu/innovation-cybersecurity/outsourcing-to-cloud-service-providers-ebf-responds-to-esma-consultation/).*

[169] *Règlement CRBF n° 97-02 du 21 février 1997 relatif au contrôle interne des établissements de crédit et des entreprises d'investissement.*

Selon ce règlement, les banques étaient ainsi tenues, notamment, de prévoir contractuellement les conditions du contrôle de l'exécution des prestations externalisées en imposant l'insertion de certaines clauses dans les contrats avec leurs sous-traitants, en particulier la clause dite « d'audit » par laquelle les prestataires consentent un droit d'accès aux informations relatives aux conditions d'exécution des prestations externalisées aux banques concernées et aux autorités de supervision compétentes, ainsi que la possibilité de conduire des inspections dans les locaux des prestataires.

L'ACPR s'est officiellement préoccupée du sujet du Cloud à l'occasion d'une enquête conduite auprès des acteurs « banques et assurances » dès 2013, et dont les conclusions ont souligné l'accroissement de l'intérêt de ces acteurs, notamment bancaires, pour l'externalisation en mode Cloud hybride ou public.[170] Au terme de cette consultation de place, le régulateur a observé que certaines fonctions dites support (notamment certaines ressources informatiques), devraient, eu égard à leur contribution dans la réalisation de certains services fournis à la clientèle et leur rôle dans la continuité de l'activité, être considérées comme constituant une externalisation de prestations de services ou d'autres tâches opérationnelles essentielles ou importantes. Le règlement CRBF n° 97-02 mentionné précédemment est devenu aujourd'hui l'arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'ACPR (l'« **Arrêté sur le Contrôle Interne** »).[171]

Le recours au Cloud par les banques devrait donc relever, pour certains services Cloud, du régime des prestations de services ou autres tâches opérationnelles essentielles ou importantes prévu aux articles 231 et suivants de l'Arrêté sur le Contrôle Interne.[172] D'un point de vue de hiérarchie de normes, les Orientations sur l'Externalisation doivent donc être articulées avec l'Arrêté sur le Contrôle Interne, qui reste, en France, le cadre normatif applicable dans cette matière. À cet égard, l'ACPR précise que « *les dispositions des orientations relatives à l'externalisation*

[170] *ACP-Banque de France, Les risques associés au Cloud computing, Analyses et synthèses, n°16, juillet 2013 (https://acpr.banque-france.fr/sites/default/files/medias/documents/201307-risques-associes-au-cloud-computing.pdf).*

[171] *Ibid, page 13. Selon les termes employés par le régulateur, « Au-delà des questions d'organisation et de compétences que soulève le recours au cloud computing, les risques spécifiques qui s'ajoutent aux risques classiques engendrés par toute externalisation informatique doivent être parfaitement maîtrisés dans les domaines de la banque et de l'assurance. (…) En matière d'externalisation de prestations essentielles ou d'autres tâches importantes, il n'est pas évident que des fonctions considérées comme « support » ne soient pas en pratique à considérer comme essentielles ou importantes, eu égard à la place qu'elles prennent dans la réalisation de certains services et pour la continuité de l'activité (ressources informatiques notamment). »*

[172] *Anciennement les articles 37-1 et suivants du Règlement 97-02. L'Arrêté sur le Contrôle Interne s'applique également, notamment, aux sociétés de financement, aux entreprises d'investissement, aux établissements de paiement et de monnaie électronique. Au surplus, les établissements de crédit fournissant des services d'investissement ou commercialisant notamment des dépôts structurés au sens de la directive MIF2 doivent respecter les dispositions des articles 30 à 32 du règlement délégué (UE) 2017/565 précité.*

doivent être lues à la lumière de celles de l'arrêté du 3 novembre 2014 ».[173] Cet arrêté a été mis en cohérence, notamment avec les Orientations sur l'Externalisation en février 2021.[174] Les établissements assujettis au contrôle de l'ACPR (en premier lieu les banques) qui recourent au Cloud bancaire devraient donc appliquer, en plus des Orientations sur l'Externalisation, les articles 231 et suivants de l'Arrêté sur le Contrôle Interne pour les prestations de services ou autres tâches opérationnelles essentielles ou importantes.[175]

Ce régime prévoit le principe d'une responsabilité pleine et entière pour les banques ayant recours à l'externalisation, ainsi que l'obligation de maîtriser les risques y afférents, étant rappelé que, comme sous l'empire de l'ancien Règlement 97-02, les banques sont ainsi tenues de prévoir contractuellement, notamment avec les Prestataires de Cloud les conditions du contrôle de l'exécution des prestations externalisées en imposant l'insertion de certaines clauses dans les contrats.

Il convient de noter qu'à côté des autorités de supervisions, d'autres régulateurs se sont également manifestés. La CNIL avait publié en 2012 des recommandations pour les entreprises qui envisagent de recourir au Cloud afin de limiter son impact sur la sécurité des données à caractère personnel dont ces entreprises ont la responsabilité.[176]

---

[173] *ACPR, Notice de conformité aux Orientations de l'Autorité bancaire européenne relatives à l'externalisation (EBA/GL/2019/02), 16 juillet 2019. Cette interprétation lève indirectement une question terminologique posée par les deux textes. En effet, selon l'avis de certains praticiens, cette formule devrait signifier que les notions de « prestations de service ou autres tâches opérationnelles essentielles ou importantes » de l'Arrêté sur le Contrôle Interne et de « fonctions critiques et importantes » des Orientations sur l'Externalisation sont des notions équivalentes qui doivent être soumises aux mêmes règles (voir M. de Marolles, Quid des nouvelles Orientations pour les établissements de crédit français, depuis ce 30 septembre 2019, une révolution ou une simple évolution ? Banque & Droit, n°189, janvier-février 2020, l'avis de ces praticiens ayant été donné eu égard aux différences de rédaction entre l'arrêté (article 10 r)) et les orientations (§N°29-c)).*

[174] *Arrêté du 25 février 2021 modifiant l'arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'Autorité de contrôle prudentiel et de résolution (JORF, n°0056 du 6 mars 2021, n° 16). Le texte ajoute, notamment, une série de définitions à l'article 10 de l'Arrêté sur le Contrôle Interne (« incident opérationnel ou de sécurité », « actif informatique », « système d'information », « service informatique », « risque informatique » et « sécurité du système d'information »), renforce les exigences en matière de contrôle interne en mettant l'accès sur la sécurité informatique (article 11(e) modifié) et créée, après l'article 270, un nouveau titre (« Titre VI bis - Gestion du risque informatique »), imposant, notamment, aux établissements assujettis à établir une stratégie informatique (article 270-1), d'organiser la gestion de leur risque informatique (article 270-2) et d'établir une politique écrite de sécurité informatique et de sensibilisation à la sécurité des dirigeants effectifs, du personnel et des prestataires (article 270-3).*

[175] *Et, le cas échéant, les articles 30 à 32 du règlement délégué (UE) 2017/565 de la Commission pour les banques qui exercent des activités d'investissement. De plus, lorsque le Prestataire de Cloud fournit des prestations qui participent à l'exécution des obligations relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme et au gel des avoirs incombant aux banques donneuses d'ordres, celles-ci doivent respecter des obligations spécifiques prévues aux articles 9 et 10 de l'arrêté du 6 janvier 2021 relatif au dispositif et au contrôle interne en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme et de gel des avoirs et d'interdiction de mise à disposition ou d'utilisation des fonds ou ressources économiques (un délai de mise en conformité est prévu pour les contrats d'externalisation conclus avant le 1er mars 2021 et jusqu'au 16 janvier 2022).*

[176] *CNIL, Recommandations pour les entreprises qui envisagent de souscrire a des services de Cloud, 25 juin 2012 (https://www.cnil.fr/sites/default/files/typo/document/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a_des_services_de_Cloud.pdf).*

On relèvera également qu'en France, l'ANSSI s'était également saisie du sujet du Cloud[177] sous l'angle des risques liés à la perte de maitrise du système d'information, à la confidentialité et à l'intégrité des données (en particulier dans les « nuages publics » où les données de plusieurs organismes sont mutualisées et stockées,[178] et à une dépendance technologique accrue vis-à-vis des Prestataires de Cloud.

2.2.2 - Contexte réglementaire des autres États membres

En dehors de la France, certains États membres de l'UE avaient, avant la publication des Orientations sur l'Externalisation, adopté des textes de portée juridique variable, toutefois généralement non contraignants, soit spécifique au Cloud (le Luxembourg ou le Royaume-Uni), soit s'inscrivant dans des thématiques plus générales (tel qu'en Belgique, où l'autorité de supervision a publié en 2009 une circulaire en matière de services financiers via internet, ou encore, en Italie où la Banque d'Italie a publié en 2013 une circulaire relative à l'externalisation bancaire).[179]

Après la publication des Orientations sur l'Externalisation, la plupart des autorités de supervision des États membres de l'UE ont déclaré à l'ABE s'y conformer (notamment la France, l'Irlande et l'Autriche), ou leur intention de se conformer (comme l'Allemagne, le Royaume-Uni, l'Italie, la Belgique ou encore les Pays-Bas).[180] Les autorités espagnole et polonaise ont quant à elles informé l'ABE qu'elles ne se conformeraient que partiellement à ces orientations.[181] En effet, la Banque d'Espagne a invoqué le fait que les orientations 62 et 63 relatives aux conditions de surveillance de l'externalisation sont en contradiction avec la réglementation espagnole. Ainsi, celle-ci ne les appliquera pas en cas d'externalisation d'activités bancaires de réception de dépôt ou autres fonds remboursables du public, ainsi que dans l'hypothèse de l'externalisation de services de paiement. Le superviseur polonais a indiqué, pour sa part, qu'il ne se conformerait pas aux aspects des Orientations sur l'Externalisation relatifs aux services de Cloud précisément, étant souligné que celui-ci a par ailleurs publié une position en 2018, puis des recommandations en janvier 2020, traitant spécifiquement des conditions dans lesquelles les entités financières soumises à sa supervision peuvent avoir recours au Cloud

[177] *Dans ses recommandations de 2010 concernant la maitrise des risques liés à l'externalisation des systèmes d'information (ou « infogérance ») adressées aux organismes du secteur public et du secteur privé. Voir le communiqué de presse de l'ANSSI, Externalisation, Cloud Computing : maîtriser les risques pour les systèmes d'information, 3 décembre 2010 (https://www.ssi.gouv.fr/uploads/IMG/pdf/2010-12-03_Communique_de_presse_guide_externalisation_maitriser_les_risques.pdf) et son guide intitulé Maîtriser les risques de l'infogérance – Externalisation des systèmes d'information, Décembre 2010 (https://www.ssi.gouv.fr/uploads/IMG/pdf/2010-12-03_Guide_externalisation.pdf).*

[178] *L'ANSSI relève dans son guide qu'il existe plusieurs architectures en nuage et distingue ainsi les « nuages publics », qui sont destinés à l'usage du grand public, des « nuages privés », destiné à l'usage exclusif d'une organisation ou d'une entreprise.*

[179] *Voir, pour le détail, l'annexe n° 3 du présent rapport.*

[180] *ABE, Compliance table (EBA/GL/2019/02), 8 octobre 2020 (https://www.eba.europa.eu/sites/default/documents/files/document_library//875334/EBA%20GL%202019%2002%20%20-%20%20CT%20GLs%20on%20outsourcing%20arrangements.pdf).*

[181] *Ibid.*

(public et hybride).[182] Une présentation de la réglementation applicable en Allemagne, Belgique, Espagne, Italie, Luxembourg, aux Pays-Bas, Pologne et au Royaume-Uni en cas de recours au Cloud par les banques figure en annexe 3 au présent rapport.

Malgré le fait qu'une majorité d'autorités nationales ait indiqué se conformer (ou avoir l'intention de se conformer) aux Orientations sur l'Externalisation, comme la Commission européenne le relève toutefois dans son étude d'impact relative au Règlement DORA,[183] le cadre réglementaire des différents États européens régissant le recours au Cloud par des établissements bancaires reste encore très hétérogène, certains étant perçus comme plus contraignants que d'autres, notamment en matière de Cloud : « *It was also highlighted that certain jurisdictions in Europe have more stringent requirements for outsourcing and require certain data localization or pre-approvals from regulators, which may be in conflict with other laws, e.g. the GDPR and the current EU-wide initiatives for the free flow of data. The lack of standardization in controls, processes, and reporting across industry results in unnecessary complexity and frustration for both financial institutions and third parties* ».

2.3 - Nécessité d'une approche régulatoire plus holistique : vers un encadrement du risque sur les tiers (*third party risk*) ?

L'approche consistant à appréhender le Cloud bancaire au travers des règles encadrant l'externalisation des fonctions critiques ou importantes, si elle n'est pas propre au modèle européen,[184] a atteint ses limites particulièrement dans l'environnement juridique européen. Sur la forme, la portée juridique des Orientations sur l'Externalisation est incertaine et limitée en ce qu'elles s'insèrent dans un cadre réglementaire national hétérogène et morcelé. En substance, ces dernières reprennent principalement les orientations de 2006 du CESB sans bouleverser l'économie générale du texte) et présentent peu de dispositions spécifiques au Cloud (elles-mêmes assez peu contraignantes)[185]. Sur

[182] *Voir, pour le détail, l'annexe n° 3 du présent rapport.*

[183] *Commission, Staff working document, op. cit., p. 76.*

[184] *Aux États-Unis, pays d'origine des leaders du Cloud, les établissements financiers ayant recours au Cloud doivent en particulier se référer à la note publiée par le Federal Financial Institutions Examination Council (« **FFIEC** ») le 10 juillet 2012, qui souligne en réalité les risques clés liés à l'externalisation à des Prestataires de Cloud identifiés dans des recommandations et orientations déjà préexistantes. Ainsi, le FFIEC renvoie les institutions financières aux fondamentaux relatifs aux risques et à la gestion des risques définis dans le guide du FFIEC intitulé Information Technology Examination Handbook. Le FFIEC précise également qu'afin de pallier ces risques, les institutions doivent notamment procéder à une évaluation des risques, un audit du sous-traitant, une mise en place ou une revue de politiques de sécurité informatique, une identification des risques réputationnels, juridiques et règlementaires et prévoir une politique de continuité des opérations en cas de perturbation.*

De manière similaire, les exigences applicables en cas de recours au Cloud par une institution financière chinoise sont disséminées au sein de différentes réglementations relatives par exemple à la cybersécurité, aux mesures de protection des clients de services financiers ou encore à la lutte anti-blanchiment.

Pour plus de détails, voir l'annexe n° 3 au présent rapport.

[185] *§54(h) (mentions dans le registre des accords d'externalisation), §82 et 83 (exigences en termes de sécurité des systèmes) et §97 (vérification des compétences des auditeurs internes ou externes).*

le fond, elles n'intègrent pas le rôle grandissant des prestataires de technologies de l'information et de la communication (« **TIC** ») en général (et des Prestataires de Cloud en particulier) et, par voie de conséquence, de l'inversion du rapport de force entre la banque et ses sous-traitants, comme illustré plus haut.[186]

Enfin, du fait de leur nature juridique de cette catégorie de texte de niveau 3, de nature interprétative, les Orientations sur l'Externalisation sont impropres à répondre aux enjeux liés à l'extra-territorialité de la législation des pays dont sont originaires les principaux Prestataires de Cloud : une intervention législative au niveau de l'UE est en effet nécessaire.

Un changement de paradigme doit s'opérer : la dimension du risque n'est plus simplement celle qui est liée au mode de gestion de l'activité bancaire reposant sur l'externalisation elle-même, mais celle qui résulte de la dépendance de la banque à des services critiques fournis par des tiers Prestataires de cloud, notamment l'exposition au risque de défaillance de ces derniers.

Le risque inhérent à cette dépendance s'accroit lorsque les Prestataires de Cloud ont la particularité soit d'être en dehors de la juridiction de l'Union, soit soumis à la juridiction de l'Union mais, de par leur rattachement juridique territorial, également soumis à d'autres systèmes juridiques se situant en dehors de la juridiction de l'Union.

Cette nouvelle approche de l'encadrement des risques sur les tiers prestataires de services critiques (incluant les Prestataires de Cloud critiques) relevant de la sphère financière a déjà été amorcée par l'UE, faisant le choix de soumettre à la supervision d'autorités relevant du secteur financier notamment des tiers prestataires de services comme : les agences de notation, supervisées par l'AEMF,[187] ainsi que les administrateurs d'indices de référence, supervisés par l'autorité nationale compétente.[188]

Dans le cadre de la consultation sur le Règlement DORA, la Commission européenne a ainsi relevé qu'une très large majorité de répondants souhaitait en effet que les Prestataires TIC critiques[189] (incluant les Prestataires de Cloud critiques) fassent l'objet d'un régime de surveillance directe.[190] Cela rejoint l'approche poursuivie par la FBF et la FBE dans leurs travaux consacrés au Cloud bancaire.[191]

---

[186] *Cf. supra paragraphe 1.4 - Enjeux de conformité pour les banques ayant recours à des Prestataires de Cloud.*

[187] *Règlement (CE) No. 1060/2009 du Parlement européen et du Conseil du 16 septembre 2009 sur les agences de notation de crédit.*

[188] *Règlement (UE) No. 2016/1011 du Parlement européen et du Conseil du 8 juin 2016 concernant les indices utilisés comme indices de référence dans le cadre d'instruments et de contrats financiers ou pour mesurer la performance de fonds d'investissement. Pour une présentation plus détaillée et critique, voir par exemple : E. Jouffin, La convergence des préoccupations dans la divergence des moyens, Banque & Droit n° 196 mars-avril 2021, p. 4.*

[189] *Il est intéressant de noter que l'ABE utilise l'expression « critical third party provider » dans les orientations précitées.*

[190] *Commission, Staff working document, p. 76 : « An overwhelming majority of respondents supported the introduction of an oversight framework for ICT TPPs. The majority of respondents agreed that it should focus on critical ICT TPPs and "criticality" be based on a set of both qualitative and quantitative thresholds (e.g. concentration, number of customers, size, interconnectedness, substitutability, complexity, etc.). »*

[191] *Les travaux de la FBE sur le sujet du Cloud bancaire peuvent être consultés sur la page Cloud Banking de son site internet.*

C'est tout l'enjeu du Règlement DORA présenté par la Commission européenne en septembre 2020, qui agrège d'une part, le cadre réglementaire existant, en particulier les Orientation sur l'Externalisation décrites plus haut[192] et, d'autre part, le changement de dimension qui vise à soumettre les Prestataires TIC critiques à la surveillance d'un superviseur financier.

III- Vers un nouveau paradigme règlementaire en matière d'externalisation informatique dans le secteur financier : le règlement Dora

3.1 - Les principaux apports du Règlement DORA

La présente section n'a pas vocation à présenter le Règlement DORA[193] de manière exhaustive. Elle vise uniquement à mettre en lumière les apports du Règlement DORA qui sont pertinents dans le cadre du présent rapport.

3.1.1 - Les objectifs du Règlement DORA

Le Règlement DORA prévoit des exigences harmonisées afin d'accroitre et de sauvegarder la résilience opérationnelle[194] des établissements et professionnels réglementés de la banque, des marchés financiers et de l'assurance. Il a pour objet de répondre aux problématiques déjà identifiées dans les sections 1 - Enjeux liés au Cloud bancaire - et 2 - L'appréhension du Cloud par la réglementation bancaire : entre morcellement et hétérogénéité - ci-dessus, notamment l'impact potentiellement systémique sur le secteur financier de l'exposition et de la dépendance croissante des professionnels réglementés à l'égard des Prestataires de Cloud, l'absence d'un cadre harmonisé pour la maîtrise des risques associés aux TIC et l'insuffisance du cadre réglementaire actuel concernant l'externalisation au regard du déséquilibre le plus souvent constaté dans la relation entre Prestataires de Cloud et institutions financières.

[192] *Les Orientations de l'ABE sur la gestion de risques liés aux TIC et la Directive NIS.*

[193] *Les dispositions du Règlement DORA présentées dans cette section sont issues de la première version du projet de règlement publiée le 24 septembre 2020, COM (2020) 595 final, 2020/0266 (COD).*

[194] *La résilience opérationnelle est définie comme la capacité pour une institution financière à construire, sauvegarder et surveiller son intégrité opérationnelle d'un point de vue technologique en s'assurant, directement ou indirectement, au moyen du recours à des services de prestataires technologiques, qu'il dispose de l'ensemble des fonctionnalités liées aux TIC nécessaires pour garantir la sécurité de ses réseaux et systèmes d'information qui lui permet de fournir ses services et de garantir la qualité de ces services.*

[195] *Article 2. Les entités réglementées concernées incluent les établissements du « secteur bancaire » (établissements de crédit, de paiement, de monnaie électronique, entreprises d'investissement), de l'assurance (entreprises d'assurance, fonds de retraite professionnelle supplémentaire, intermédiaires) de la gestion d'actifs ; les infrastructures de marché (plates-formes de négociation, contreparties centrales, dépositaires centraux, prestataires de services de communication de données, référentiels centraux) ; les intermédiaires en financement participatif ; les prestataires de services sur actifs numériques et émetteurs de jetons ; les agences de notation de crédit ; les contrôleurs légaux des comptes et les cabinets d'audit et les administrateurs d'indices de référence d'importance critique.*

Il est prévu que le Règlement DORA prenne la forme d'un règlement européen d'application directe dans les États membres. Ce règlement inclura des règles trans-sectorielles applicables au-delà du secteur bancaire[195] et s'articulera autour de deux piliers : d'une part, les obligations applicables aux entités financières traitant avec les Prestataires TIC et, d'autre part, la surveillance des Prestataires TIC établis au sein de l'Union européenne qui sont considérés comme « critiques » par les autorités européennes.

3.1.2 - Une harmonisation du cadre de la gestion des risques liés aux TIC au sein des entités financières

Dans le cadre du premier pilier, le Règlement DORA prévoit les obligations que les entités réglementées concernées devront respecter afin d'assurer la maîtrise des risques liés à leurs dispositifs de TIC. Ces obligations portent notamment sur la gouvernance de ces dispositifs, la gestion des risques, le *reporting* des incidents de sécurité, les tests de résilience opérationnelle et le recours à des prestataires de services de TIC (« **Prestataires TIC** »), lesquels incluent les Prestataires de Cloud[196]. Il est prévu que ces obligations puissent être mises en œuvre sur la base d'un principe de proportionnalité. Le(s) critère(s) de proportionnalité à prendre en compte, le cas échéant, devraient être précisés au cours du processus d'élaboration du règlement DORA.

S'agissant du recours à des prestataires de services de TIC, les obligations prévues par le Règlement DORA ne se limiteront pas aux seules situations d'externalisation, mais auront vocation à englober toutes les relations contractuelles entre une entité réglementée concernée et les Prestataires TIC. À cet égard, les obligations prévues par le Règlement DORA sont très proches des principales exigences prévues par les Orientations sur l'Externalisation applicables aux entités réglementées concernées qui ont recours à l'externalisation[197], notamment la contractualisation d'obligations à la charge des Prestataires TIC et de droits au bénéfice des professionnels réglementés. Sur ce point, le Règlement DORA prévoit le recours à des clauses contractuelles types pour les services de Cloud qui devraient être élaborées par la Commission européenne et adoptées par la voie d'actes délégués[198]. On relèvera également que, à l'instar des Orientations sur l'Externalisation, le Règlement DORA fait peser cette obligation de contractualisation uniquement sur les entités réglementées concernées, à l'exclusion des Prestataires TIC.

---

[196] *Les prestataires de services de TIC sont définis comme les entreprises fournissant des services numériques, parmi lesquelles les fournisseurs de services de Cloud computing, de solutions logicielles, de services d'analyse de données, les centres de stockages de données (datacenters), à l'exclusion des fournisseurs de matériel informatique (hardware components) et des fournisseurs de réseaux et de services de communications électroniques.*

[197] *Une analyse d'écart présentant les similitudes et les divergences entre le Règlement DORA et les Orientations sur l'Externalisation est proposée en annexe n° 4 de ce rapport.*

[198] *Considérant (55), article 27(3).*

3.1.3 - L'introduction d'un mécanisme de surveillance directe des Prestataires TIC « critiques »

Dans le cadre du second pilier, il est prévu que les Prestataires TIC établis dans l'Union européenne et considérés comme « critiques » par les AES fassent l'objet d'une surveillance directe par l'une des AES.[199] Les Prestataires TIC critiques établis en dehors de l'Union européenne (pour lesquels une surveillance directe ne serait pas possible ou pleinement efficace) ne pourront pas fournir des services aux entités réglementées concernées du fait de l'interdiction expresse faite à ces dernières par le Règlement DORA d'avoir recours à ces prestataires.[200]

Le caractère critique d'un Prestataire TIC sera déterminé par un comité mixte composé de membres des trois AES, sur la base de critères définis dans le Règlement DORA, tels que notamment le degré de substituabilité d'un service, l'impact potentiel d'un dysfonctionnement du Prestataire TIC sur les activités réglementées, l'importance systémique des institutions financières ayant recours à ce prestataire et le nombre d'États-membres dans lesquels ce prestataire est établi.[201]

Chaque Prestataire TIC désigné comme « critique » par le comité mixte sera ainsi surveillé par un « Superviseur Principal » (*Lead Overseer)*, désigné par le même comité, qui sera l'AES du secteur d'activité ayant majoritairement recours à ce Prestataire TIC. Le Superviseur Principal aura pour fonction de s'assurer que ce Prestataire TIC critique met en œuvre des dispositifs de gouvernance suffisamment complets, robustes et efficients. À cette fin, le Superviseur Principal disposera de prérogatives étendues à l'égard du Prestataire TIC telles que des pouvoirs d'enquête, de contrôle sur pièces, d'inspection sur place ainsi que la possibilité de formuler des recommandations et les mesures correctives, ou encore le pouvoir de prononcer des astreintes en cas de non-conformité à ses recommandations.

Cette nouvelle surveillance directe des Prestataires TIC critiques par un Superviseur Principal s'articulera avec la supervision des entités réglementées par les autorités nationales et européennes compétentes[202]. Ces autorités disposeront de tous les pouvoirs de surveillance nécessaires pour s'assurer du respect par les entités réglementées concernées des exigences du Règlement DORA leur incombant. Elles pourront également ordonner la suspension temporaire de l'utilisation des

---

[199] *La structure et les instances de la surveillance directe sont détaillées à l'article 29.*

[200] *Article 28(9). Selon le considérant (58), cette interdiction n'équivaut pas à l'obligation de localisation des données au sein de l'Union européenne car le Règlement DORA ne comporte à ce stade aucune exigence concernant le stockage ou le traitement des données.*

[201] *Article 28(2). Cette liste n'est pas limitative.*

[202] *Désignées conformément à l'article 41. Afin de permettre cette articulation, le Règlement DORA inclut également des obligations de coopération et d'échange d'informations entre les différents superviseurs.*

services fournis par un Prestataire TIC critique jusqu'à ce que celui-ci remédie aux déficiences et aux risques identifiés par un Superviseur Principal, voire à prononcer la résiliation immédiate des contrats conclus avec ce prestataire[203].

Le Règlement DORA est en revanche moins précis concernant les sanctions administratives ou disciplinaires qui pourront être prononcées à l'encontre des Prestataires TIC critiques en cas de méconnaissance de leurs obligations ou des recommandations formulées par le Superviseur Principal. En particulier, le contenu exact de ces sanctions ainsi que l'autorité compétente pour les prononcer (le Superviseur Principal ou les autorités nationales des États membres) ne semble pas avoir été arrêtés à ce stade.

Le groupe de travail a identifié un certain nombre de pistes d'amélioration du texte et formule les recommandations discutées ci-après.

3.2 - Pistes d'amélioration du Règlement DORA et propositions du HCJP

3.2.1 - Surveillance des prestataires TIC critiques

3.2.1.1 - Exposé du problème

Le Règlement DORA établit un cadre de surveillance des Prestataires TIC désignés comme critiques par les AES (section II, articles 28 et suivants).

Ce régime de surveillance appelle trois remarques.

(i) Obligation d'établissement dans l'Union

Le Règlement DORA confère en effet aux AES certains pouvoirs de surveillance à l'égard des Prestataires TIC critiques leur permettant : (i) de contrôler la mise en place de règles, de procédures, de mécanismes et des dispositifs pour gérer les risques informatiques[204] ; (ii) d'adopter des plans de supervision individuels [205] ; (iii) de conduire des enquêtes et des inspections générales[206] ; (iv) de formuler des recommandations ; (v) ainsi que d'imposer des astreintes pour obliger les Prestataires TIC critiques à se conformer à certaines obligations (notamment en termes de fourniture d'information et

[203] *Article 37.*

[204] *Article 30(1).*

[205] *Article 30(3).*

[206] *Article 31(1).*

de coopération de bonne foi avec les AES).[207] Cependant, en l'état actuel du texte, si les Prestataires TIC critiques ne disposent pas d'une implantation permanente dans l'Union et que les entités financières ne concluent pas des accords contractuels pour la fourniture des services informatiques par le biais de cette implantation, l'exercice de ces pouvoirs de surveillance pourra s'avérer, en pratique, très limité car il sera tributaire des accords de coopération conclus avec les autorités des pays d'origine de ces prestataires (en termes d'échange d'informations et de coordination des activités de surveillance).[208]

Or, le Règlement DORA n'impose aucune obligation, directement à la charge des Prestataires TIC ressortissant de pays situés hors de l'Union de s'établir sur le territoire de l'Union, préalablement à la fourniture de leurs services aux entités financières. Ce n'est qu'indirectement que cette obligation est prévue, à l'article 28(9) du Règlement DORA, en posant un principe d'interdiction, à l'adresse des entités financières, « *de faire appel à un prestataire de services informatique établi dans un pays tiers* » qui répondrait à la qualification de critique au sens de l'article 28(2) du Règlement DORA.[209]

De tels prestataires sont ceux qui « *n'ont pas établi d'activité ou de présence dans l'Union* » selon la définition de « tiers prestataire de services informatiques établi dans un pays tiers » figurant à l'article 3(19) du Règlement DORA (les « **Prestataires TIC Pays Tiers** »).[210]

Ces notions sont particulièrement floues et ne sont pas formulées de façon juridique. Que signifie la notion d'activité ? Le fait que le Prestataire TIC ait simplement conclu des contrats de prestation de services informatiques avec une ou plusieurs entités financières situées dans l'Union, suffirait-il à caractériser la poursuite d'une activité dans l'Union ? Quant à la notion d'établissement dans l'Union, cela signifie-il que le Prestataire TIC doit avoir ouvert au minimum un bureau de représentation ? Voire même n'ait simplement recours qu'à des intermédiaires ou de simples agents commerciaux ?[211] Ou cela vise t'il plutôt une implantation plus permanente, telle qu'une succursale ou même une filiale ? L'imprécision des termes est entretenue par une certaine incohérence interne du texte du Règlement DORA. Ainsi, le paragraphe (58) du préambule parle de Prestataire TIC « constitué »

---

[207] *Article 31(4).*

[208] *Par exemple, pour la mise en œuvre de toute inspection sur place (article 34 du Règlement DORA).*

[209] *« Les entités financières ne font pas appel à un tiers prestataire de services informatiques établi dans un pays tiers qui serait désigné comme critique en vertu du paragraphe 1, point a), s'il était établi dans l'Union. »*

[210] *Article 3(19). Voir les termes utilisés dans la version anglaise, qui ne sont pas plus précis : « ICT third-party service provider established in a third country' means an ICT third-party service provider that is a legal person established in a third-country, has not set up business/presence in the Union, and has entered into a contractual arrangement with a financial entity for the provision of ICT services ».*

[211] *Un intermédiaire agissant sous le contrôle de son mandant peut ainsi caractériser l'existence d'un établissement dans le pays dans lequel cet intermédiaire agit pour le compte du mandant (cf. dans le cadre de la mise en œuvre du passeport européen en matière bancaire, Commission européenne, Commission interpretative communication, freedom to provide services and the interest of the general good in the second banking directive, 20 juin 1997, SEC(97) 1193 final, p. 10 et s.).*

dans l'Union,[212] ce que l'on peut comprendre comme *ayant créé dans l'Union une filiale dotée de la personne morale*, et non pas simplement un établissement (bureau de représentation ou succursale) dépourvu d'une telle personnalité, ce que la version anglaise de texte pourrait laisser entendre.[213]

(ii) Contractualisation avec les filiales européennes des Prestataires TIC critiques et soumission du contrat de prestation au droit de l'Union

Alors que le Règlement DORA prévoit l'obligation d'incorporer les clauses visées à l'article 27(2) du Règlement DORA (voir ci-après les propositions formulées au paragraphe 3.2.4 - Obligations à la charge des Prestataires TIC en matière contractuelle - concernant cet aspect), il n'impose pas que le contrat de prestation de service soit conclu par l'intermédiaire de l'implantation européenne du Prestataire TIC critique. En d'autres termes, nonobstant l'obligation imposée aux entités financières de faire appel à des prestataires de services informatique critiques qui ont établi une activité ou une présence dans l'Union,[214] le règlement ne précise rien quant à l'identité du cocontractant de l'entité financière. En d'autres termes, quand bien même le Prestataire TIC critique disposerait d'une filiale européenne, le contrat de prestation de services informatiques pourrait être conclu avec toute autre entité juridique appartenant au groupe de ce prestaire (et en particulier, son entreprise mère) située dans un pays tiers et non pas uniquement la filiale en question. Partant, ce contrat pourrait d'ailleurs tout aussi bien être soumis à la loi d'un pays tiers et non pas à celle d'un État membre de l'Union. Ici encore, le Règlement DORA n'impose aucune obligation à cet égard.

La question se pose dès lors de savoir si l'obligation d'implanter une filiale dans l'Union ne devrait pas s'accompagner, corrélativement, non seulement de l'obligation faite aux entités financières, ainsi qu'aux prestataires, de conclure leur contrats de prestation de services informatiques avec cette filiale, afin de donner plein effet à la surveillance des Prestataires TIC critiques, mais également, celle de soumettre ces contrats au droit de l'Union et/ou de l'un des États membres. En effet, étant soumis à la loi d'un pays tiers, le contrat de prestation pourrait éluder les règles posées par le Règlement DORA (notamment en ce qui concerne les clauses contractuelles que le contrat doit comporter), sauf à considérer, soit que le règlement DORA constitue une loi de police au sens de l'article 9(1) du règlement (UE) No. 593/2008 (le « **Règlement Rome I** »)[215] (en d'autres termes, que ce règlement

---

[212] *« L'exigence que les tiers prestataires de services informatiques qui ont été désignés comme critiques soient **constitués dans l'Union** n'équivaut pas à une localisation des données puisque le présent règlement ne comporte aucune autre exigence concernant le stockage ou le traitement des données à effectuer dans l'Union ».*

[213] *« The **requirement of legal incorporation in the Union** of ICT third-party service providers which have been designated as critical does not amount to data localisation since this Regulation does not entail any further requirement on data storage or processing to be undertaken in Union ».*

[214] *Article 28(9) du Règlement DORA, cité plus haut.*

[215] *Règlement (UE) No. 593/2008 du Parlement européen et du Conseil du 17 juin 2008 sur la loi applicable aux obligations contractuelles (Rome I). Article 9(1) : « Une loi de police est une disposition impérative dont le respect est jugé crucial par un pays pour la sauvegarde de ses intérêts publics, tels que son organisation politique, sociale ou économique, au point d'en exiger l'application à toute situation entrant dans son champ d'application, quelle que soit par ailleurs la loi applicable au contrat d'après le présent règlement. » Voir sur cette notion, également la discussion au paragraphe 3.2.4(ii) (Modifications proposées) ci-dessous.*

relève de l'ordre public international) que le juge saisi aurait obligation d'appliquer (article 9(2) du même règlement) au regard de son droit national (c'est-à-dire, selon la loi du *for*)[216], soit que les règles de rattachement prévues par l'article 3(3) du Règlement Rome I trouvent matière à s'appliquer,[217] ce qui pourrait éventuellement être le cas si le contrat ne présente pas de lien d'extranéité[218].

Pour autant, indépendamment du choix de la loi applicable au contrat, il convient cependant de rappeler que les parties peuvent également choisir de soumettre leur contentieux contractuel à la compétence des tribunaux d'un État non-membre de l'Union[219] – quand bien même, d'ailleurs, la loi applicable au contrat serait celle d'un État membre. Dans ce cas, il est vraisemblable que le juge étranger compétent écartera le droit de l'Union s'il le considère incompatible avec sa loi nationale. Au surplus, le juge saisi n'a pas l'obligation d'appliquer une loi de police étrangère pour écarter l'application de la stipulation contractuelle qui serait en conflit avec elle.[220]

(iii) Sanction des obligations des Prestataires TIC critiques

Enfin, si le Règlement DORA prévoit un régime de supervision des Prestataires TIC critiques, il reste peu disert en termes d'obligations mises à leur charge et de sanctions. En effet, le projet de règlement impose de manière directe à ces prestataires uniquement de communiquer des informations, de permettre à l'AES agissant en qualité de superviseur principal la réalisation d'enquêtes et inspections, de répondre aux recommandations émises par les superviseurs principaux à la suite de leurs évaluations et, enfin, de coopérer de bonne foi avec les superviseurs principaux,[221] le cas échéant

[216] *En d'autres termes, le droit national du juge saisi tel qu'incorporant le Règlement DORA qui, en tant que règlement européen, a un effet direct dans l'ordre juridique des États membres.*

[217] *Lequel prévoit que « Lorsque tous les autres éléments de la situation sont localisés, au moment de ce choix, dans un pays autre que celui dont la loi est choisie, le choix des parties ne porte pas atteinte à l'application des dispositions auxquelles la loi de cet autre pays ne permet pas de déroger par accord ».*

[218] *Cela étant dit, une telle hypothèse pourrait être discutée si les prestations de Cloud sont, dans les faits, réalisées hors du territoire de l'Union, au moyen de ressources ou d'infrastructures localisées dans un ou plusieurs pays tiers, puisque le Règlement DORA ne comporte aucune exigence concernant le stockage ou le traitement des données dans l'Union (cf. considérant (58) de ce règlement). Au surplus, l'article 3(3) du Règlement Rome I n'aurait pas non plus particulièrement vocation à s'appliquer si les deux parties contractent depuis leurs sièges respectifs situés dans des États membres différents et que les prestations informatiques concernent les données relatives aux clients collectées par l'entité financière au travers de ses différentes succursales ou filiales européennes.*

[219] *Il n'existe en effet aucune obligation, en droit international privé, de faire coïncider le pays désigné en vertu de la clause de choix de la loi applicable avec celui qui dont les tribunaux sont rendus compétents au titre de la prorogation conventionnelle de compétence. C'est d'ailleurs, dans la perspective d'une absence d'identité de pays désignés au titre de ces deux clauses que les chambres internationales du tribunal de commerce et de la Cour d'appel de Paris trouvent leur intérêt notamment dans le contexte du Brexit, les contrats pouvant rester soumis au droit anglais, tandis que le tribunal de commerce de Paris recevrait compétence (voir : HCJP, Préconisations sur la mise en place à paris de chambres spécialisées, pour le traitement du contentieux international des affaires, 3 mai 2017).*

[220] *En droit de l'Union, c'est ce que prévoit l'article 9(2) du règlement Rome I : la loi de police étrangère ne s'impose pas au juge saisi, qui dispose d'une certaine latitude pour lui donner ou non effet. D'ailleurs, cette disposition doit se lire dans l'autre sens : le Règlement Rome I permet au juge saisi de prendre en compte la loi de police étrangère.*

[221] *Articles 30(1) et (3), 32, 33 et 34.*

sous astreinte.[222] Pour autant, aux termes de l'article 37, lorsque les recommandations émises par les superviseurs principaux ne sont pas suivies d'effet par les Prestataires TIC critiques, c'est aux entités financières que revient la responsabilité de suspendre l'utilisation des services fournis par les prestataires, voire de résilier les contrats de prestation de service, sur l'injonction de leurs propres superviseurs.[223] Les recommandations émises par le superviseur principal ne semblent pas avoir de force obligatoire ou contraignante à l'égard du Prestataire TIC concerné et, partant, aucun pouvoir de sanction, directement à l'égard de ce prestataire, ne semble être accordé au superviseur principal (hormis celui d'infliger des astreintes, mentionné ci-dessus).[224] Les pouvoirs de sanction dont sont dotées les autorités nationales compétentes, visés à l'article 44, ne semblent l'être qu'à l'égard des entités financières.

Les recommandations émises par l'AES superviseur principal devraient donc avoir force contraignante à l'égard du Prestataire TIC concerné, et leur non-respect faire l'objet de sanctions effectives, proportionnées et dissuasives.

Ici encore, un parallèle avec le Règlement CRA (voir définition ci-dessous) peut être établi, puisque ce dernier accorde un pouvoir de sanction spécifique à l'AEMF (amendes) en cas de manquements par les agences de notation enregistrées des obligations qui sont mises à leur charge par le Règlement CRA (article 36 bis et annexe 3 du Règlement CRA). Le montant des amendes peut, dans les faits, être significatif.[225] De même, à titre de comparaison, le RGPD prévoit un régime de sanctions administratives autonome sévère en cas de manquement à certaines obligations prévues par le règlement (articles 83(4), (5) et (6)), les amendes pouvant s'élever jusqu'au montant le plus élevé entre 20 millions d'euros et 4% du chiffre d'affaires mondial. On notera également que le nouveau projet de règlement européen sur l'intelligence artificielle ou « *Artificial Intelligence Act* » (le « **Règlement IA** »)[226] poursuit la même logique.[227]

Enfin, en ce qui concerne la résiliation des contrats de prestation de services informatiques par les entités financières à la demande de leur superviseur prévue à l'article 37(3) du Règlement DORA, le règlement est muet quant aux conditions dans lesquelles cette résiliation peut intervenir,[228] en particulier au regard du sort d'éventuelles pénalités sanctionnant une résiliation anticipée qui pourraient être prévues dans le contrat. Par conséquent, afin d'assurer le plein effet de ce droit de

[222] *Article 30(4).*

[223] *Article 37(3).*

[224] *Voir en ce sens, le constat fait par le Comité économique et social européen (CESE), dans son avis du 2 mars 2021, n° 6634/21 (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6634_2021_INIT&from=EN).*

[225] *ESMA fines Fitch €5,132,500 for breaches of conflict of interest requirements, communiqué de presse, 28 mars 2019.*

[226] *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts, 21 avril 2021, COM(2021) 206 final, 2021/0106 (COD).*

[227] *Article 71.*

[228] *L'article 27(2) se limite à imposer que les contrats comportent des stipulations régissant « les droits de résiliation et le délai de préavis minimal correspondant pour la durée du contrat, conformément aux attentes des autorités compétentes » (§(i)).*

résiliation, le Règlement DORA devrait préciser que la résiliation n'ouvre pas droit à indemnité au profit du Prestataire TIC.

3.2.1.2 - Modifications proposées

(i) Création d'une filiale européenne

Afin d'assurer une meilleure efficacité de la surveillance des Prestataires TIC critiques, il est nécessaire d'imposer la création d'une implantation dans l'Union. Deux possibilités existent[229] : soit une succursale, soit une filiale, c'est-à-dire, une société dotée de la personnalité morale. En termes de supervision, la succursale présente de nombreux inconvénients liés à son absence de personnalité morale, à commencer par sa soumission à la loi du siège de la personne morale à laquelle elle se rattache, c'est-à-dire, par hypothèse, la loi d'un pays tiers, ainsi que l'absence d'une structure de gouvernance qui lui soit propre.

À titre de comparaison, un parallèle peut être établi avec le règlement (CE) No. 1060/2009 sur les agences de notation (le « **Règlement CRA** »). C'est en effet le choix qui a été fait par ce règlement aux termes duquel seules les notations émises par des personnes morales établies dans l'Union et enregistrées par l'AEMF peuvent être utilisées à des fins réglementaires par des entités réglementées (telles que les établissements de crédit, les entreprises d'investissement, *etc.*) (articles 4 et 14 du Règlement CRA).

Par conséquent, une telle implantation devrait être sous la forme d'une société dotée de la personnalité morale, disposant ainsi de la pleine capacité juridique à l'engager à l'égard des tiers et de répondre d'éventuels manquements à l'égard du superviseur européen.

(ii) Contractualisation avec la filiale européenne et soumission du contrat de prestation au droit de l'Union

Du point de vue du superviseur, afin de donner plein effet à la surveillance des Prestataires TIC critiques, la fourniture par ces derniers de leurs services aux entités financières devrait être encadrée par des contrats de prestation de services informatiques conclus avec cette filiale établie dans l'Union. Cette filiale assumerait l'entière responsabilité de la fourniture de ces services, tant à l'égard de ses clients, que de son superviseur et, le cas échéant, des tiers.

[229] *Par exemple, la Directive NIS évoque ainsi la notion d'installation stable. Voir Considérant (21) : « Aux fins d'identification des opérateurs de services essentiels, l'établissement dans un État membre suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable. La forme juridique retenue pour un tel établissement, qu'il s'agisse d'une succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante à cet égard ». Voir également considérant (64).*

Dans la même veine, et en cohérence avec le RGPD, le contrat de prestation de services informatiques conclu entre l'entité financière et la filiale du Prestataire TIC critique dans l'Union devrait être soumis au droit d'un État membre de l'Union et la clause attributive de compétence juridictionnelle prévu dans ce contrat devrait désigner les tribunaux compétents d'un État membre de l'Union.

(iii) Sanctions

Un régime de sanctions spécifiques devrait être instauré, donnant compétence aux AES pour les infliger (de manière similaire à ce que prévoit le Règlement CRA, en termes de compétence des autorités européennes). Ces sanctions devraient être effectives, proportionnées et dissuasives (à l'instar de ce que le RGPD (ou le Règlement IA) prévoit).

Par ailleurs, l'article 37(3) du Règlement DORA devrait préciser que lorsque les entités financières résilient les accords contractuels conclus avec les Prestataires TIC critiques sur injonction des autorités compétentes, une telle résiliation n'ouvre aucun droit à indemnité d'aucune sorte au profit des cocontractants de l'entité financière.

3.2.2 - Aménagement de l'interdiction pour les entités financières de faire appel à des prestataires TIC critiques établis hors de l'Union européenne

Le principe d'interdiction strict, tel qu'envisagé par le Règlement DORA, pourrait par ailleurs entrainer des conséquences pénalisantes des points de vue juridique et opérationnel pour le secteur bancaire, en raison de l'insécurité juridique soulevée par les questions suivantes :

(i) l'interdiction de recourir à des Prestataires TIC Pays Tiers critiques dans un contexte intragroupe[230] ;

(ii) les incertitudes quant à la question de savoir sur qui pèse la charge d'apprécier le caractère critique des Prestataires TIC de pays tiers (les « **Prestataires TIC Pays Tiers** ») avant de contracter avec eux le cas échéant ; et

(ii) les conséquences découlant de la désignation comme critique d'un Prestataire TIC Pays Tiers au cours de la vie du contrat de prestation de services informatiques conclu après l'entrée en application de DORA, alors que le prestataire en cause n'était pas désigné comme critique au moment de la conclusion du contrat.

[230] *La question de l'exclusion des Prestataires TIC Intragroupes critiques situés dans des pays tiers est discutée au paragraphe 3.2.3 (Exclusion des Prestataires TIC intragroupes du champ) ci-dessous.*

Si, dans son principe, le régime d'interdiction n'est pas débattu, un aménagement nous parait nécessaire en vue d'en minimiser les impacts négatifs en termes de sécurité juridique – et opérationnelle – indiqués ci-dessus.

3.2.2.1 - Responsabilité de la détermination du caractère « critique » des Prestataires de TIC Pays Tiers

(i) Exposé du problème

La combinaison des articles 28(1), 28(6) et 28(9) du Règlement DORA créée une incertitude quant à savoir sur qui pèsera l'obligation de déterminer si un Prestataires TIC Pays Tiers est critique ou non. Alors que l'article 28(1) prévoit clairement que, s'agissant d'un Prestataire TIC fournissant ses services dans l'Union, cette responsabilité incombe aux AES, l'article 28(9) apparaît, quant à lui, nettement plus ambigu, car il semble faire supporter aux entités financières la charge d'apprécier le caractère critique du prestataire si ce dernier était établi dans l'Union, en prélude à toute fourniture de services au sein de l'Union.

En l'absence de clarté, cette situation fragilise la sécurité juridique des opérations et le respect de la conformité à ce principe d'interdiction :

• à défaut de précision, les entités financières pourraient considérer que le règlement met à leur charge l'examen du caractère critique des Prestataires TIC établis hors de l'Union. Or cette évaluation ne peut être appréciée par les entités financières, dans la mesure où, notamment, les critères fixés aux §(e) et (f) de l'article 28(2) renvoient à des informations que seules les AES ont à leur disposition, à savoir : le nombre d'États membres au sein desquels les Prestataires TIC établis Pays Tiers procurent leurs services et le nombre d'États membres dans lesquels les entités financières, qui utilisent un même Prestataire TIC, opèrent[231] ;

• à défaut de clarté, comment interpréter la liste des prestataires critiques établis et communiqué annuellement par les AES, dans le cas d'absence de mention de Prestataires TIC Pays Tiers ? Cela signifierait-il qu'aucun Prestataire TIC Pays Tiers n'est considéré comme critique, ou qu'il appartient aux entités financières qui traitent avec ces prestataires de s'assurer qu'elles sont autorisées à le faire ?

Afin d'éviter toute incertitude, nous proposons les amendements suivants :

[231] *D'autant plus si le critère d'établissement repose sur la poursuite d'activités dans l'Union, ce qu'une entité financière ne peut vérifier si elle n'a pas déjà contracté avec le prestataire.*

(ii) Modifications proposées

Il est proposé de modifier les articles 28(1),[232] 28(6)[233] et 28(9)[234] du Règlement DORA pour y inclure une référence expresse aux Prestataires TIC Pays Tiers.

3.2.2.2 - Situation des contrats conclus avec des Prestataires TIC Pays Tiers postérieurement à l'entrée en vigueur de l'interdiction

(i) Exposé du problème

Postérieurement à l'entrée en application de DORA, le principe d'interdiction ne fera pas obstacle à ce qu'une entité financière puisse conclure un contrat de prestation de services informatiques avec un Prestataire TIC Pays Tiers non critique. La nécessité de disposer d'une procédure claire de classification et d'information officielle par les AES concernant le caractère critique d'un Prestataire TIC Pays Tiers s'impose donc tout particulièrement.

Le Prestataire TIC Pays Tiers pouvant être caractérisé comme critique, à tout moment au cours de la vie du contrat de prestation de services informatiques qu'il aura conclu avec une entité financière,[235] l'entité financière concernée sera contrainte de résilier ce contrat pour respecter l'interdiction visée à l'article 28(9) du Règlement DORA.

Pour préserver la sécurité juridique et opérationnelle des entités financières dans le cadre de leurs relations contractuelles avec les Prestataires TIC Pays Tiers considérés comme non critiques lors de l'entrée en relation, il est indispensable de prévoir un délai raisonnable entre l'information officielle par les AES de la criticité d'un Prestataire TIC Pays Tiers et le déclenchement de l'obligation, pour l'entité financière, de résilier le contrat en raison de l'application du principe d'interdiction de l'article

---

[232] *Une proposition de rédaction pourrait être la suivante : « 1. The ESAs, through the Joint Committee and upon recommendation from the Oversight Forum established pursuant to Article 29(1) shall:*

(a) designate the ICT third-party service providers that are critical for financial entities ***and the ICT third-party service providers established in a third country that would be designated as critical if they were established in the Union****, taking into account the criteria specified in paragraph 2;*

(b) [the remaining provision unchanged]. »

[233] *Une proposition de rédaction pourrait être la suivante : « 6. The ESAs, through the Joint Committee, shall establish, publish and yearly update the list of critical* ***ICT third-party service providers at Union level, and ICT third-party service providers established in a third country designated as critical.*** *»*

[234] *Une proposition de rédaction pourrait être la suivante : « 9. Financial entities shall not make use of an ICT third-party service provider established in a third country ~~that would be~~ designated as critical pursuant to point (a) of paragraph 1 ~~if it were established in the Union.~~ »*

[235] *Ces contrats étant généralement conclus à durée indéterminée ont vocation à perdurer dans le temps.*

28(9). En tout état de cause, la prise d'effet de la résiliation du contrat de prestation de services informatiques ne peut être immédiate et donc une période de transition suffisamment longue doit être prévue afin de permettre à l'entité financière de mettre en œuvre les procédures de réversibilité ou ré-internalisation idoines.

(ii) Modifications proposées

Il est donc proposé de modifier l'article 25(8) du Règlement DORA qui prévoit les cas dans lesquels le contrat de prestation de services informatiques doit être résilié, en y ajoutant un nouveau cas aux termes duquel la résiliation prend effet dans le délai d'une année après la notification de cette résiliation par l'entité financière au Prestataire TIC Pays Tiers à la suite de son classement comme prestataire critique par les AES.[236]

3.2.3 - Exclusion des Prestataires TIC intragroupes du champ de la surveillance des AES et de l'interdiction de recourir à des Prestataires TIC Pays Tiers

(i) Exposé du problème

Selon la rédaction actuelle du Règlement DORA, les Prestataires TIC intragroupes (les « **Prestataires TIC Intragroupes** ») remplissant les critères de l'article 28(1) pourraient être qualifiés de critiques et, partant, relever de la surveillance des AES (article 30). Au surplus, la rédaction actuelle des définitions de Prestataires TIC critiques (article 3(18)) et des Prestataires TIC Pays Tiers (article (3(19)), combinée au principe d'interdiction discuté plus haut, conduit à la conclusion que les Prestataires TIC Pays Tiers susceptibles d'être qualifiés de critiques, et qui appartiennent à des groupes financiers européens, peuvent également tomber dans le champ d'application de l'interdiction visée à l'article 28(9).

La soumission des Prestataires TIC Intragroupes critiques à cette surveillance et, lorsqu'ils sont établis dans un pays tiers, à cette interdiction, ne semble pas réaliser les objectifs de DORA. Par ailleurs, l'interdiction entrainerait des conséquences dommageables pour les groupes financiers européens qui ont créé des infrastructures hors de l'Union afin de répondre à des besoins technologiques spécifiques qui ne sont pas nécessairement offerts dans l'Union (par exemple l'accès à certaines innovations) et sécuritaires (ces infrastructures sont hébergées dans des entités contrôlées par ces groupes financiers). En effet, les Prestataires TIC Intragroupes critiques devraient se trouver hors du champ des dispositions ci-dessus pour les raisons suivantes :

[236] *« (e) when the ICT third-party service provider is an ICT third-party service provider established in a third country and It has been designated as critical pursuant to point (a) of paragraph 1 of Article 28 and is included in the list referred to in paragraph 6 of the same Article. In such case, the termination takes effect within a year from notice thereof served by the financial entity to the ICT third-party service provider.»*

• les Prestataires TIC Intragroupes ont pour entreprises mères des entités financières européennes ou des entreprises mères d'entités financières européennes, et dont le groupe fait l'objet d'une supervision par les autorités nationales et européennes sur base consolidée, ce qui permet ainsi le suivi et le contrôle, par les entités financières concernées (et indirectement, par leurs superviseurs), de l'application de la réglementation européenne sur l'ensemble du groupe. Au surplus, dans cette veine, les entités financières n'éprouvent ainsi *a priori* pas les difficultés à faire insérer les clauses relevant des Orientations sur l'Externalisation dans les contrats avec des prestataires appartenant à leurs groupes, qui ont pu être relevées à propos, notamment, des prestataires de services de Cloud. Dès lors, une surveillance spécifique supplémentaire paraît inutile ; et

• ces prestataires ont pour entreprises mères des entreprises ayant leur siège dans l'Union, le lien d'établissement territorial avec l'Union rejoint ainsi les exigences de rattachement géographique au territoire de l'Union visé par l'article 3(19) du Règlement DORA.

Cependant, du point du vue du superviseur, il conviendra de s'assurer que le recours à une filiale intragroupe ne serve pas à permettre à un Prestataire TIC critique d'échapper à la surveillance des AES au moyen notamment d'une structure de coopération (de type filiale commune par exemple) qui ne serait pas exclusivement contrôlée par une entité financière ou son entreprise mère et qui, par ailleurs, ne fournirait pas ses services exclusivement aux entreprises appartenant au même groupe.

(ii) Modifications proposées

La modification consisterait donc à exclure tout prestataire de services informatiques qui est une filiale contrôlé de manière exclusive par un groupe financier et fournit exclusivement ses services au sein de ce groupe du champ du régime de surveillance des AES prévue à l'article 30 et de l'interdiction prévue à l'article 28(9).

3.2.4 - Obligations à la charge des Prestataires TIC en matière contractuelle

(i) Exposé du problème

Comme évoqué précédemment, l'obligation d'insérer dans les contrats d'externalisation les clauses requises par les orientations applicables de l'ABE repose exclusivement sur les établissements de crédit. De même est-ce le cas dans le Règlement DORA.[237] Afin de réduire les difficultés éprouvées

[237] *Article 25(1) : « Les **entités financières** qui ont conclu des accords contractuels pour l'utilisation de services informatiques dans le cadre de leurs activités commerciales **restent à tout moment pleinement responsables du respect et de l'exécution** de toutes les obligations découlant du **présent règlement** et de la législation applicable aux services financiers. » À lire de manière combinée avec l'article 27(2) qui impose une liste de clauses contractuelles qui doivent figurer dans les contrats de prestation conclus par les entités financières.*

par les banques dans leurs négociations avec les Prestataires de Cloud comme relaté dans le présent rapport et d'améliorer l'efficacité de DORA sur ce terrain, il est recommandé de mettre également à la charge des Prestataires TIC le respect de cette obligation.

Au surplus, l'utilisation de clauses contractuelles types devrait être plus fortement incitée,[238] voire imposée, en s'inspirant de ce que prévoit le RGPD.[239] Le texte de l'article 27(3) du Règlement DORA est à cet égard doté d'une portée très limitée (les parties « *envisagent l'utilisation de clauses contractuelles types* »), puisqu'il laisse entendre que les parties sont libres de ne pas utiliser ces clauses types, du moment qu'elles en ont préalablement discuté entre elles. L'utilisation des clauses types risque donc de ne rester qu'un vœu pieux. Toutefois, la clause-type présente l'inconvénient d'un manque de flexibilité, la rédaction d'une telle clause n'étant pas nécessairement adaptée à toutes les situations particulières ou aux spécificités d'une relation contractuelle donnée. Il semble plutôt pertinent de prévoir une obligation de type « *comply or explain* » à la charge des deux parties, aux termes de laquelle l'usage de la clause-type s'imposerait *a priori*, sauf pour les deux parties de s'accorder mutuellement pour l'écarter, en justifiant, à leurs autorités respectives le cas échéant, de leur caractère inadéquat dans le contrat en cause. Cette contrainte aurait le mérite d'engager juridiquement tous les Prestataires TIC et non pas de ne peser qu'à la charge de l'entité financière. Ces clauses-types pourraient être adoptées par la Commission européenne ou adoptées par les AES et approuvées par la Commission, par voie d'actes d'exécution, selon une démarche similaire à celle qui est prévue par le RGPD en matière de transfert des données personnelles.[240]

La base juridique du Règlement DORA (article 114 du Traité sur le fonctionnement de l'Union européenne, TFUE), ainsi que l'inclusion des prestataires TIC dans le champ *ratione personae* du Règlement DORA[241] devrait permettre la soumission de ces prestataires à des obligations contraignantes, ce que le texte prévoit déjà à l'égard des Prestataires TIC critiques (articles 1(c) et 30 et suivants).

Il est regrettable que la Présidence portugaise du Conseil envisage purement et simplement la suppression de l'article 27(3) précité. Une telle suppression va à l'encontre de la direction prise par le RGPD qui devrait plutôt servir d'exemple pour les besoins du Règlement DORA.

---

[238] Cf. considérant (55) du préambule du Règlement DORA qui fait référence à l'initiative menée par la Commission européenne visant à développer une série de clauses types applicables en matière de prestations de Cloud.

[239] Le RGPD prévoit en effet que le responsable du traitement ou le sous-traitant ne peut transférer des données à caractère personnel vers un pays tiers ou à une organisation internationale que s'il a prévu des garanties appropriées. Ces garanties appropriées peuvent consister en l'usage de clauses types adoptées ou approuvées par la Commission européenne (cf. article 46(5), §(c) et (d)). Si l'usage de telles clauses n'est certes pas imposé (ni même ne constitue pas la seule voie offrant les garanties appropriées (p. ex. un code de conduite approuvé, une certification, etc.), le texte est néanmoins assez incitatif. Voir pour plus de détails: https://www.cnil.fr/fr/les-clauses-contractuelles-types-de-la-commision-europeenne.

[240] Articles 28(7) et (8), 63et 93(2) du RGPD.

[241] Article 2(u) du Règlement DORA.

(ii) Modifications proposées

Il est donc d'abord proposé de :

modifier l'article 27(2) du Règlement DORA. Pour cela, deux approches sont possibles.

• Première approche : imposer une obligation positive à la charge, en particulier, des Prestataires TIC (et non pas uniquement ceux qui sont jugés critiques) de **s'assurer**[242] que l'accord inclut les clauses visées par cet article.[243] Dans ce cas, on peut noter que les parties ne devraient pas pouvoir échapper à cette règle en soumettant leurs contrats de prestation au droit d'un pays tiers.

• Seconde approche : renforcer le caractère d'ordre public du texte de l'article 27(2), sans imposer d'obligation à la charge des parties. Sans faire référence à la qualification de loi police au sens de l'article 9(1) du Règlement Rome I,[244] l'article 27(2) pourrait simplement préciser qu'il s'applique « **quelque soit la loi applicable au contrat** ».[245]

Ensuite :

Il pourrait être fait une mention expresse à la conformité des accords contractuels de prestation de service aux exigences prévues à l'article 27 :

• dans l'article 30(2), au titre de l'évaluation réalisée par les superviseurs principaux ; et

• dans l'article 31(1)(d), parmi les domaines dans lesquels les superviseurs principaux peuvent faire des recommandations.

Se pose cependant la question de la sanction des obligations décrites ci-dessus. Comme indiqué plus haut, le Règlement DORA ne prévoit pas la possibilité pour les AES de sanctionner spécifiquement les Prestataires TIC (par exemple, en infligeant des amendes), notamment lorsque, à la suite de l'évaluation visée à l'article 30, ces derniers ne mettent pas en œuvre les recommandations qui leur ont été notifiées conformément à l'article 37(1), en dehors d'astreintes qui peuvent être éventuellement

---

[242] *En s'inspirant de la rédaction de l'Arrêté sur le Contrôle Interne Article 239 : « Les entreprises assujetties **s'assurent**, dans leurs relations avec leurs prestataires externes, que ces derniers : […] ».*

[243] *« 2. **Financial entities and ICT third-party service providers each ensure that the** ~~The~~ contractual arrangements on the use of ICT services shall include at least the following: [remaining provision unchanged] ».*

[244] *Qui relève de l'application de la loi nationale des États membres, et donc qui ne paraît pas pertinente s'agissant d'une disposition d'un règlement européen.*

[245] *Cela étant dit, il convient de rappeler que si le juge compétent est celui d'un pays tiers, alors, alors il ne sera probablement pas tenu d'appliquer le Règlement DORA au contrat de prestation de service (voir paragraphe 3.2.2.2 (Situation des contrats conclus avec des Prestataires TIC Pays Tiers postérieurement à l'entrée en vigueur de l'interdiction) ci-dessus). Par conséquent, pour donner plein effet à ce règlement, il est nécessaire, en tout état de cause, d'imposer aux parties de soumettre les litiges relatifs à leurs accords contractuels à la compétence du juge d'un État membre.*

décidées par le superviseur principal dans des cas limités[246] (et, au cas d'espèce, si le prestataire ne répond pas à la demande du superviseur principal de lui soumettre un rapport dans lequel sont précisées les mesures qui ont été prises par le prestataire pour répondre à ces recommandations).[247]

Pourtant, il serait alors logique d'envisager, soit à titre d'accompagnement, soit à titre alternatif à la suspension de l'utilisation des services fournis à l'entité financière, que le pouvoir d'astreinte des AES soit exercé à l'égard des Prestataires TIC critiques dans ces circonstances, en fonction de la gravité du manquement, qualifiée aux termes de l'article 30(4) – par exemple, si la non-conformité est délibérée (cf. article 37(4)(d)) –. L'obligation de résiliation du contrat interviendrait alors vraiment en derniers recours.

Cette astreinte pourrait faire également l'objet de la publication prévue à l'article 31(8).

Enfin, il est également proposé de :

modifier l'article 27(3) du Règlement DORA d'affermir l'obligation de « considérer » l'inclusion de clauses types, en prévoyant que, si de telles clauses types existent, les parties auront l'obligation d'y recourir, sauf si elles peuvent justifier d'un commun accord de leur caractère inadéquat dans le contrat en cause.[248]

[246] *Article 31(4) du Règlement DORA.*

[247] *Article 31(1)(c) du Règlement DORA. On rappellera que si les risques identifiés dans les recommandations n'ont pas été écartés, les autorités compétentes peuvent exiger des entités financières qu'elles suspendent temporairement l'utilisation ou le déploiement des services fournis par les prestataires,voire résilient, le contrat (article 37(3)).*

[248] *«3. ~~When negotiating~~ **In their** contractual arrangements, financial entities and ICT third-party service providers shall ~~consider the~~ use ~~of~~ **contractual clauses substantially compliant** with standard contractual clauses developed for specific services, **unless all the parties mutually agree that they can justify their inadequacy having regard to the particular circumstances of the contractual arrangement concerned.**»*

ANNEXE 1

Composition du groupe de travail

ANNEXE 1
LISTE DES MEMBRES DU GROUPE DE TRAVAIL
« Le Cloud bancaire : état des lieux et propositions »

PRÉSIDENT :

- **Frédérick Lacroix,** Avocat associé, Clifford Chance Europe LLP, membre du HCJP

RAPPORTEUR :

- **Irina Rambeloson,** Avocate, Clifford Chance Europe LLP

MEMBRES :

- **Marc Andries,** Chef de mission, Responsable de l'équipe de contrôle informatique sur place, Autorité de contrôle prudentiel et de résolution
- **Sandrine Bogey-Leleu,** Juriste Conseil Référent, Direction juridique groupe, BPCE
- **Noémie Dentu,** Direction Juridique de l'Autorité de contrôle prudentiel et de résolution
- **Laura Dufay-Krulik,** Directrice adjointe des services juridiques, Banque de France
- **Pauline Facon,** Adjointe au chef du Pôle affaire internationales, coordination européenne et enjeux technologiques, Direction générale du Trésor
- **Gérard Gardella,** ancien Magistrat, ancien Directeur Juridique du groupe Société Générale, Secrétaire Général du HCJP
- **Emmanuel Jouffin,** Responsable du département veille réglementaire groupe, La Banque Postale
- **Sylvain Lambert,** Juriste expert, Direction juridique Groupe, Société Générale
- **Marie-Astrid Larcher,** Adjoint au Directeur financier, Banque de France
- **Aude Mortureux de Faudoas,** Juriste Contrats et Propriété intellectuelle, Direction des Affaires Juridiques, Crédit Agricole S.A.
- **Alice Navarro,** DG Trésor, Magistrate, Conseillère juridique, Direction Générale du Trésor
- **Jean-Baptiste Poulle,** Avocat associé, Spitz Poulle Kannan
- **Nathalie Sambourg,** Direction Juridique de l'Autorité de contrôle prudentiel et de résolution
- **Sibylle de Vareilles,** Avocate, Spitz Poulle Kannan
- **Stéphane Yvon,** Juridique et conformité, Affaires Bancaires et Financières, Europe et International, Fédération bancaire française

ANNEXE 2

Glossaire et définitions

ANNEXE 2
GLOSSAIRE ET DÉFINITIONS

ABE : Autorité Bancaire Européenne.

ACPR : Autorité de Contrôle Prudentiel et de Résolution.

AEAPP : Autorité Européenne des Assurances et des Pensions Professionnelles.

AEMF : Autorité Européenne des Marchés Financiers.

AES : Autorités Européennes de Supervision.

AFNOR : Agence Française de Normalisation.

AMF: Autorité des Marchés Financiers.

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information.

Arrêté sur le Contrôle Interne : voir la définition donnée à cette expression en page 44.

BATX : Baidu, Alibaba, Tencent et Xiaomi.

BCE : Banque Centrale Européenne.

CEI : Commission Électrotechnique Internationale.

CESB : Comité Européen des Superviseurs Bancaires.

CJUE : Cour de Justice de l'Union Européenne.

Cloud : Tel qu'indiqué en introduction de ce rapport, la notion de Cloud fait l'objet de la définition officielle suivante : « *Mode de traitement des données d'un client, dont l'exploitation s'effectue par l'internet, sous la forme de services fournis par un prestataire* »[249]. Cette définition précise par ailleurs que « *l'informatique en nuage est une forme particulière de gérance de l'informatique, dans laquelle l'emplacement et le fonctionnement du nuage ne sont pas portés à la connaissance des client* »[250].

Par ailleurs, on peut également relever plusieurs autres définitions données par divers organismes officiels.

Pour la CNIL, « *(L)e Cloud Computing (…) fait référence à l'utilisation de la mémoire et des capacités de calcul des ordinateurs et des serveurs répartis dans le monde entier et liés par un réseau. Les*

[249] *Avis de la Commission générale de terminologie et de néologie publié au Journal Officiel de la République Française (JORF) du 6 juin 2010, Vocabulaire de l'informatique et de l'internet, NOR: CTNX1012892X*

[250] *Même référence que ci-dessus. Définition reprise de celle établie par le US National Institute of standards and technology (NIST) (https://csrc.nist.gov/publications/detail/sp/800-145/final).*

applications et les données ne se trouvent plus sur un ordinateur déterminé mais dans un nuage (cloud) composé de nombreux serveurs distants interconnectés »[251].

La Banque de France a également proposé une définition multicritères fondée notamment sur celle du *National Institute of Standards and Technology* (NIST). Le Secrétariat général de l'Autorité de Contrôle prudentiel propose donc de caractériser ces prestations de la façon suivante : « *le Cloud Computing consiste à déporter sur des serveurs distants des données et des traitements informatiques traditionnellement localisés sur des serveurs locaux, voire sur le poste de l'utilisateur. Il permet l'accès via un réseau, généralement entendu comme Internet, à la demande et en libre-service, à des ressources informatiques virtualisées et mutualisées habituellement facturées à l'usage (…)* »[252].

Enfin, pour l'ANSSI « *(l')'informatique en nuage peut être définie comme un modèle de gestion informatique permettant l'accès via un réseau à des ressources informatiques partagées et configurables. Ces ressources sont attribuées à la demande et parfois en libre-service* »[253].

Cloud bancaire : voir la définition donnée à cette expression en page 19.

CNIL : Commission Nationale Informatique et Libertés.

CRD IV : directive 2013/36/EU du Parlement européen et du Conseil du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement.

Directive NIS : voir la définition donnée à cette expression en page 3.

DMA : voir la définition donnée à cet acronyme en page 26.

DSA : voir la définition donnée à cet acronyme en page 26.

DSP : directive 2007/64/CE du Parlement européen et du Conseil du 13 novembre 2007 concernant les services de paiement dans le marché intérieur, modifiant les directives 97/7/CE, 2002/65/CE, 2005/60/VE ainsi que 2006/48/CE et abrogeant la directive 97/5/CE.

DSP2 : directive 2015/2366/EU du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur (DSP2).

ENISA : *European Union Agency for Cybersecurity* (Agence de l'Union Européenne pour la cybersécurité).

---

[251] *https://www.cnil.fr/fr/definition/cloud-computing*

[252] *Analyses et Synthèses – Les risques associés au Cloud Computing, Analyses et synthèses, n° 16, juillet 2013 (https://acpr.banque-france.fr/les-risques-associes-au-cloud-computing-juillet-2013).*

[253] *ANSSI, Prestataires de services d'informatique en nuages (SecNumCloud) – référentiel d'exigences – niveau Essentiel, Version 3.1 du 11 juin 2018 (https://www.ssi.gouv.fr/uploads/2014/12/secnumcloud_referentiel_v3.1_anssi.pdf).*

FBE : Fédération Bancaire Européenne.

FFIEC : voir la définition donnée à cet acronyme en page 47.

GAFAM : Google, Apple, Facebook, Amazon et Microsoft.

IaaS : voir la définition donnée à cette expression en page 15.

ISO : Organisation International de Normalisation.

MIF2 : directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE.

NIST : *National Institute of Standards and Technology.*

PaaS : voir la définition donnée à cette expression en page 15.

Prestataire de Cloud : voir la définition donnée à cette expression en page 11.

Prestataires TIC : voir la définition donnée à cette expression en page 50.

Prestataires TIC Pays Tiers : voir la définition donnée à cette expression en page 53.

Prestataires TIC Intragroupes : voir la définition donnée à cette expression en page 61.

PSEE : voir la définition donnée à cet acronyme en page 43.

Règlement DORA : voir la définition donnée à cette expression en page 40.

Règlement 97-02 : voir la définition donnée à cette expression en page 43.

Règlement CRA : voir la définition donnée à cette expression en page 56.

Règlement IA : voir la définition donnée à cette expression en page 56.

RGPD : Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

ROFIEG : *Expert Group on Regulatory Obstacles to Financial Innovation.*

SaaS : voir la définition donnée à cette expression en page 16.

TIC : voir la définition donnée à cet acronyme en page 48.

UE : Union européenne.

ANNEXE 3

État de la réglementation du Cloud dans certains États membres de l'Union européenne autres que la France, aux États-Unis et en Chine

ANNEXE 3
ÉTAT DE LA RÈGLEMENTATION DU CLOUD DANS CERTAINS ÉTATS MEMBRES DE L'UNION EUROPÉENNE AUTRES QUE LA FRANCE, AUX ÉTATS-UNIS ET EN CHINE[254]

« **Orientations ABE 2019** » désigne les orientations de l'ABE relatives à l'externalisation, en date du 25 février 2019 (EBA/GL/2019/02).

« **Orientations ABE 2017** » désigne les orientations de l'ABE en date du 20 décembre 2017, qui ont été remplacées par les Orientations ABE 2019.

I. États membres de l'Union européenne

Juridiction	Position de l'autorité de supervision	Conformité aux Orientations ABE
Allemagne	Les établissements financiers assujettis au contrôle de la *Bundesanstalt für Finanzdienstleistungsaufsicht* ("**Bafin**") doivent se référer aux orientations publiées par la Bafin en novembre 2018[255]. Les orientations de la Bafin recensent les exigences allemandes et européennes en matière d'externalisation. Selon les orientations de la Bafin, les **clauses suivantes doivent être intégrées dans le contrat passé entre l'établissement assujetti et le prestataire**[256] : • portée des services (en définissant notamment l'élément externalisé, les services support, les responsabilités du prestataire, le lieu d'exécution de l'externalisation, les dates de début et fin du contrat d'externalisation, les ratios clés de performance et les indicateurs permettant d'identifier un niveau de service inacceptable) ; • la communication d'informations et les droits d'audit de l'établissement assujetti (afin de	Ces recommandations sont à jour des Orientations ABE 2017, mais pas des Orientations ABE 2019. Selon le tableau de conformité de l'ABE[257], la Bafin a déclaré avoir l'intention de s'y conformer d'ici le 31 décembre 2020.

[254] *Étude réalisée au cours du troisième trimestre 2020, non mise à jour depuis.*

[255] *https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2018/meldung_181108_orientierungshilfe_cloud_anbieter.html*

[256] *Pages 7 et seq. des orientations de la Bafin.*

[257] *https://eba.europa.eu/sites/default/documents/files/document_library//875334/EBA%20GL%202019%2002%20%20-%20%20CT%20GLs%20on%20outsourcing%20arrangements.pdf*

Juridiction	Position de l'autorité de supervision	Conformité aux Orientations ABE
	s'assurer que l'assujetti dispose de l'ensemble des informations nécessaires pour superviser de manière appropriée les risques liés à l'externalisation) ; • la communication d'informations et les droits d'audit du régulateur : ✓ obligation pour le prestataire de coopérer sans restrictions avec le régulateur ; ✓ octroyer les autorisations nécessaires pour que le régulateur ait accès à l'ensemble des informations, des données et aux locaux du prestataire (ceci doit préciser les processus et les contrôles ainsi que la possibilité pour le régulateur d'effectuer un audit sur site du prestataire) ; ✓ décrire les possibilités pour le régulateur de contrôler et auditer la chaîne de sous-traitance en son intégralité ; • le droit pour l'assujetti de donner des ordres au prestataire ; • la protection des données (afin de s'assurer que le prestataire respecte les règles de protection des données ; l'assujetti doit également connaître le lieu de stockage des données) ; • les conditions de rupture du contrat (il faut notamment prévoir le cas de rupture sans faute dans l'hypothèse où le régulateur a demandé la rupture du contrat, ainsi que s'assurer qu'en cas de rupture du contrat les éléments externalisés continuent de l'être par le prestataire, jusqu'à ce que les éléments puissent être transférés à un autre prestataire ou à l'établissement assujetti) ; • la sous-traitance en cascade (il faut inclure des clauses sur la possibilité ainsi que sur les modalités de la sous-traitance en cascade en s'assurant que les obligations imposées par le régulateur soient respectées) ; • le devoir d'information dû par le prestataire à l'établissement assujetti (il devra notamment informer l'assujetti de toutes les circonstances	

Juridiction	Position de l'autorité de supervision	Conformité aux Orientations ABE
	pouvant impacter de manière négative la sous-traitance) ; • le droit applicable (si ce n'est pas le droit allemand, il faut que ce soit le droit d'un pays appartenant à l'UE ou l'EEE). Les orientations de la Bafin ne précisent pas les **sanctions applicables** en cas de non-conformité. Par ailleurs, il ne **semble pas qu'une autorisation préalable soit requise spécifiquement** du régulateur – la Bafin exige toutefois que l'assujetti procède à une évaluation des risques avant de conclure le contrat de sous-traitance (des précisions sur les modalités de cette évaluation sont données dans les orientations).	
Belgique	Les établissements financiers et les entreprises d'assurance doivent d'abord se conformer à la Circulaire CBFA 2009 17 du 7 avril 2009 traitant des exigences prudentielles en matière de services financiers via internet, publiée par la Commission bancaire, financière et des assurances[258]. Cette circulaire impose notamment à l'établissement assujetti d'obtenir les garanties nécessaires que le prestataire dispose de la compétence et de la qualité nécessaires pour effectuer de manière fiable et professionnelle les tâches sous-traitées, et pour en assurer la continuité. Par ailleurs, la circulaire impose à l'établissement assujetti d'inclure dans le contrat conclu avec le prestataire le droit pour lui de faire réaliser à sa propre initiative un audit de sécurité. Enfin, l'établissement assujetti doit veiller à ce que le prestataire fasse effectuer les examens indépendants de sécurité nécessaires. La Banque Nationale de Belgique ("**BNB**") a ensuite publié le 19 juin 2018 une circulaire à l'intention des établissements de crédit et sociétés de bourse mettant en œuvre les Orientations ABE 2017 et doit être lue conjointement avec la circulaire PPB 2004/5 sur les saines pratiques de gestion en matière de sous-traitance par des établissements de crédit et des entreprises d'investissement et la communication NBB_2012_11 relative aux attentes prudentielles en	Ces recommandations sont à jour des Orientations ABE 2017, mais pas des Orientations ABE 2019.

[258] *La section 6 p.6 traite de la sous-traitance de ces services à des prestataires externes.*

Juridiction	Position de l'autorité de supervision	Conformité aux Orientations ABE
	matière de Cloud (en date du 9 octobre 2012). Elle est entrée en vigueur le 1er juillet 2018. L'objectif de la circulaire de juin 2018 n'est pas de mettre en œuvre un nouveau régime mais de confirmer que les Orientations ABE 2017 sont intégrées dans l'activité de contrôle de la BNB. La circulaire PPB 2004 05 pose plusieurs principes de saine gestion dans la sous-traitance d'activités par les établissements assujettis : • une politique de sous-traitance devra être définie, devant être approuvée par le conseil d'administration et définissant les critères d'application pour décider de recourir à la sous-traitance ; • la responsabilité des organes d'administration des établissements assujettis sera maintenue, ces organes devant apporter le soin nécessaire à la maîtrise de tous les risques qui sont liés à la sous-traitance. Par ailleurs, la direction effective de l'établissement assujetti devra prendre des mesures lui permettant en permanence d'exercer le contrôle des activités du sous-traitant ; • la décision de sous-traiter, basée sur une analyse approfondie et documentée, pourra faire l'objet d'un contrôle interne et d'un contrôle externe ; • le choix du fournisseur de services et maintien de la continuité devra être opéré avec vigilance et prudence, en tenant compte de la santé financière, de la réputation et des capacités techniques et de gestion du prestataire ; • **s'agissant de la convention de sous-traitance** : ✓ elle doit prévoir des clauses d'adaptation et de résiliation suffisamment souples, devant notamment donner à l'établissement assujetti la possibilité d'élaborer une solution de rechange ; ✓ elle doit être conclue par écrit ; ✓ une attention particulière doit être accordée aux aspects de continuité, au caractère révocable de la sous-traitance et à l'intégrité du contrôle interne et externe ;	

Juridiction	Position de l'autorité de supervision	Conformité aux Orientations ABE
	✓ elle doit poser les règles de conduite qui, en application de la politique de compliance de l'établissement assujetti, seront d'application dans l'exercice de l'activité ; ✓ elle doit souligner de façon claire les responsabilités des deux parties ; • l'établissement assujetti doit s'assurer que les dispositions en matière de continuité et de protection auprès du prestataire sont adaptées à la nature et à l'importance des activités sous-traitées, conformément à sa propre politique en la matière et aux usages en vigueur au sein du secteur financier ; • l'établissement assujetti doit poser les conditions selon lesquelles le prestataire peut sous-traiter à nouveau à des tiers tout ou partie de l'activité sous-traitée, et les modalités s'appliquant à cette nouvelle sous-traitance ; • les auditeurs internes de l'établissement assujetti doivent, lorsqu'ils l'estiment nécessaire, avoir accès à tout moment et sans encombre aux activités sous-traitées et avoir la possibilité d'exercer leurs contrôles ; par ailleurs, la fonction de compliance doit également être assurée de manière intégrale dans le chef de l'établissement sous-traitant à l'égard de chaque activité sous-traitée ; • le régulateur doit avoir accès à tout moment aux activités sous-traitées et avoir la possibilité d'exercer sur ces activités son contrôle, y compris en effectuant des contrôles sur place ; • la sous-traitance ne peut porter préjudice au respect par l'établissement assujetti des règles auxquelles il est soumis en Belgique. Les orientations de la BNB ne donnent pas d'information quant aux sanctions applicables.	
Espagne	La Banque d'Espagne a déclaré se conformer aux Orientations ABE 2019[259], à l'exception des paragraphes 62 et 63. En effet, la Banque d'Espagne a	Oui, hormis les paragraphes 62 et 63.

[259] https://www.bde.es/f/webbde/INF/MenuHorizontal/Normativa/guias/EBA-GL-2019_02_EN.pdf

Juridiction	Position de l'autorité de supervision	Conformité aux Orientations ABE
	déclaré qu'en cas d'externalisation de services de paiement, alors une notification préalable serait nécessaire.	
Italie	Les règles en matière d'externalisation sont applicables en cas de sous-traitance à un prestataire de services de Cloud. Notamment, la Banque d'Italie a publié le 17 décembre 2013 une Circulaire no. 285[260] traitant du recours à l'externalisation par les établissements de crédit. En vertu de cette circulaire, plusieurs précautions doivent être prises en cas d'externalisation : (i) l'établissement assujetti doit prendre des mesures raisonnables afin de limiter les risques encourus par l'externalisation ; (ii) l'externalisation ne doit pas résulter en une délégation de responsabilité ; (iii) l'établissement assujetti doit mettre en place des systèmes de sauvegarde adéquats, des systèmes de séparation des données afin de garantir la protection et l'intégrité des informations et des données des clients, un droit d'audit et des plans de continuité.	Non – selon le tableau de conformité de l'ABE, la Banque d'Italie a déclaré avoir l'intention de s'y conformer d'ici le 30 septembre 2020.
Luxembourg	La commission de surveillance du secteur financier ("**CSSF**") a publié le 17 mai 2017 la circulaire CSSF 17/654 (modifiée en 2019 par la circulaire CSSF 19/714) traitant de la sous-traitance informatique reposant sur une infrastructure de Cloud. S'agissant de **la notification préalable du régulateur**, celle-ci est nécessaire, peu importe que la sous-traitance concerne une activité essentielle ou non. S'agissant **des clauses à intégrer dans le contrat d'externalisation**, la circulaire prévoit que le contrat doit comprendre : • une clause de droit applicable, soumettant le contrat au droit d'un des pays de l'UE ; • une clause prévoyant la résilience dans l'UE des services de Cloud offerts à l'assujetti (l'un des centres au moins de traitement des données doit être localisé dans l'UE et doit si nécessaire pouvoir reprendre les traitements, données et	Non – selon le tableau de conformité de l'ABE, la CSSF a déclaré avoir l'intention de s'y conformer d'ici le 30 septembre 2019.

Juridiction	Position de l'autorité de supervision	Conformité aux Orientations ABE
	systèmes distribués pour opérer de manière autonome les services) ; • une clause prévoyant les rôles et responsabilités, répartis entre toutes les parties dans la chaîne de sous-traitance (l'assujetti, l'opérateur des ressources, le tiers), l'ensemble devant rester cohérent ; • une clause définissant les niveaux de services attendus, exprimés qualitativement et quantitativement ; • une clause selon laquelle en cas de rupture de contrat, le tiers s'engage contractuellement à supprimer définitivement les données et systèmes de l'assujetti dans un délai raisonnable sans préjudice des prescriptions légales ; • une clause selon laquelle en cas d'incident, de besoins réglementaires, ou autre demande spécifique, l'assujetti doit disposer d'un moyen de contact adapté auprès du tiers (la procédure de mise en relation est dûment documentée dans le contrat) ; • une clause octroyant au régulateur un droit d'audit inconditionnel sur la chaîne de sous-traitance dans le cadre des services utilisés par un établissement relevant de sa surveillance lorsque l'activité sous-traité est matérielle. Ce droit d'audit pour l'autorité compétente comprend notamment (i) un accès aux données et systèmes de l'établissement assujetti hébergés sur une infrastructure de Cloud ; (ii) un accès à la documentation pertinente du tiers (cette documentation comprend notamment les rapports d'audit, les rapports de certification, les politiques, les procédures) ; (iii) un accès au personnel du tiers, sous réserve d'une notification préalable dans un délai raisonnable ; (iv) la possibilité de mener des contrôles sur place ; et (v) la possibilité de communiquer les observations à l'établissement assujetti ; et • une clause prévoyant que l'établissement assujetti conserve un droit d'audit sur le tiers.	

Juridiction	Position de l'autorité de supervision	Conformité aux Orientations ABE
	Le site internet de la CSSF précise qu'une révision de la circulaire est en cours compte tenu de l'adoption des Orientations ABE 2019[261]. En outre, la circulaire CSSF 17/656 traite de l'organisation administrative et comptable de la sous-traitance informatique. Cette dernière (i) pose des exigences générales en matière de sous-traitance et (ii) précise les conditions pour recourir à une sous-traitance informatique autre que celle répondant à la circulaire CSSF 17/654 précitée. Nous n'avons pas d'informations quant aux sanctions applicables en cas de manquement à ces obligations.	
Pays-Bas	La *DeNederlandscheBank* (**"DNB"**) a publié sur son internet le 25 juin 2018 une notice[262] de bonnes pratiques sur la façon de gérer les risques en cas d'externalisation. Cette notice prévoit notamment que l'établissement assujetti doit informer préalablement le régulateur en cas d'externalisation d'une activité essentielle. Par ailleurs, les établissements assujettis doivent spécifiquement prévenir la DNB de toutes mesures prises en matière de Cloud, peu importe que les activités externalisées soient essentielles ou non. Concernant cette notification préalable, la DNB a publié un rapport fournissant des indications détaillées quant aux données à mentionner dans la notification et la manière de soumettre la notification à la DNB. La notification doit notamment comprendre (i) des informations sur l'établissement assujetti, (ii) des informations générales sur l'externalisation envisagée et la chaîne d'externalisation, (iii) des informations sur le contrat d'externalisation et (iv) une évaluation des risques. S'agissant **des clauses à intégrer dans le contrat d'externalisation**, la notice prévoit que le contrat doit comprendre : • une description claire de l'activité externalisée ; • les exigences de *reporting* auxquelles le tiers doit se conformer ;	Selon le tableau de conformité de l'ABE, la DNB a déclaré avoir l'intention de s'y conformer ; le droit local exclut actuellement de la supervision de la DNB les opérations d'externalisation intragroupes lorsqu'elles concernent des entités du groupe situées en UE/dans l'EEE, il faut donc modifier le droit en vigueur pour se conformer aux Orientations ABE 2019.

[261] https://www.cssf.lu/fr/gouvernance-psf-support/

[262] https://www.toezicht.dnb.nl/en/2/51-237257.jsp

Juridiction	Position de l'autorité de supervision	Conformité aux Orientations ABE
	• en cas d'externalisation d'activité essentielle, le contrat doit également comprendre une clause permettant la révocation et résiliation du contrat. Ceci permettra à l'établissement assujetti de sous-traiter à un autre prestataire, ou de reprendre à sa charge les activités qui faisaient l'objet de sous-traitance ; • une clause traitant de la protection des données ; • une obligation pour le prestataire de fournir des rapports d'assurance sur son contrôle interne à intervalles réguliers. Cela peut se faire par le biais d'un audit à réaliser chez le prestataire de services au nom de l'établissement assujetti, ou le prestataire peut fournir un rapport d'assurance certifié par un fournisseur d'assurance indépendant. En outre, conformément au décret sur les règles prudentielles[263], les banques doivent veiller à ce que les droits et obligations respectifs de l'établissement assujetti et du prestataire soient clairement attribués et énoncés dans un accord écrit qui doit couvrir les points suivants : • l'échange mutuel d'informations, y compris des accords sur la fourniture d'informations demandées par les régulateurs dans le cadre de l'exécution de leurs tâches statutaires ; • la possibilité pour l'établissement assujetti de modifier la manière dont les activités sont exercées par le prestataire de services tiers ; • l'obligation pour le prestataire de permettre à l'assujetti de continuer à se conformer aux règles qui lui sont applicables ; • la possibilité pour les régulateurs de mener une enquête dans les locaux/systèmes du prestataire ; et • la manière dont l'accord est résilié et la manière dont il est garanti que l'établissement assujetti soit en mesure, après la résiliation de l'accord, d'exercer à nouveau les activités lui-même ou de	

[263] *Besluit prudentiële regels Wft, voir section 5 (ici, en néerlandais uniquement).*

Juridiction	Position de l'autorité de supervision	Conformité aux Orientations ABE
	faire exercer les activités par un autre prestataire de services tiers. Des sanctions peuvent être prononcées à l'encontre d'un établissement assujetti ne se conformant pas à ses obligations en matière d'externalisation.	
Pologne	L'Autorité polonaise de supervision financière ("**UKNF**") a publié une position le 12 avril 2018 sur le recours au Cloud par les entités sous sa supervision. Selon la position du 12 avril 2018, l'établissement assujetti doit mener une analyse préalable avant de procéder à l'externalisation (la position donne les éléments à revoir dans le cadre de cette analyse, notamment sur les informations dont doit disposer l'établissement assujetti sur le prestataire en amont de l'externalisation et sur les éléments à prendre en compte dans le cadre de l'étude coûts-bénéfices). Par ailleurs, avant de procéder à l'externalisation, l'établissement assujetti doit procéder à une évaluation des risques et élaborer une politique pour faire face auxdits risques. S'agissant de la convention à conclure entre le prestataire et l'établissement assujetti, la position du 12 avril 2018 prévoit que doivent y figurer les clauses suivantes : • l'étendue de la responsabilité des parties ; • l'étendue des informations et de la documentation fournies par le prestataire relatives à la fourniture des services d'externalisation ; • une déclaration selon laquelle les services d'externalisation seront fournis conformément aux exigences prévues par les lois, les réglementations applicables et les normes adoptées par l'entité contrôlée ; • la possibilité de modifier les conditions de l'externalisation, les mécanismes permettant de modifier le champ d'application et les domaines de mise en œuvre de l'accord, l'extension de son champ d'application, l'ajout de nouvelles fonctionnalités ; • les conditions de résiliation ;	Non - selon le tableau de conformité de l'ABE, la PFSA a déclaré avoir l'intention de s'y conformer d'ici le 28 décembre 2020, hormis les recommandations en matière de Cloud.

Juridiction	Position de l'autorité de supervision	Conformité aux Orientations ABE
	• le délai de préavis et les procédures pour mettre fin à la collaboration en toute sécurité, y compris le retour et l'effacement des données ; • le droit de procéder à un audit ou à une certification par l'établissement assujetti, y compris le droit de procéder à des inspections dans les lieux où les données sont stockées et traitées ; • la possibilité pour le régulateur d'exercer son contrôle ; • les garanties, cautions et dommages-intérêts liquidés, la définition de la force majeure, les événements de force majeure et les procédures à suivre en cas de survenance de tels événements ; • la détermination de l'étendue de la responsabilité pour les dommages subis par les clients, conformément au droit applicable ; • les règles de licence et des droits de propriété intellectuelle ; • la détermination de la langue, de la forme, des conditions et de l'objet de la prestation externalisée, ainsi que du support de cette prestation ; • les règles et la procédure de gestion des problèmes signalés concernant les services fournis ; • l'obligation d'assurer un niveau adéquat de sécurité et de protection des données confiées, détermination de l'emplacement des centres où les données seront stockées et traitées, en particulier là où les sous-traitants traiteront les données ; • les paramètres de qualité et de continuité des services ; • les règles d'échange et de protection des informations, y compris les conditions d'octroi de l'accès aux informations aux employés de tiers ; • les exigences en matière de protection et de sécurité des informations, y compris les conditions supplémentaires d'octroi de l'accès aux	

Juridiction	Position de l'autorité de supervision	Conformité aux Orientations ABE
	informations avec un niveau élevé de confidentialité ; • la garantie que les tâches, l'étendue de la responsabilité et l'obligation de rendre compte des activités entreprises par tout sous-traitant, agent, intermédiaire ou personne ayant accès aux données et participant à leur traitement ou à leur transformation soient transparentes et puissent être clairement identifiées par l'établissement assujetti à tout moment ; • les règles de sous-traitance ; • une liste des sous-traitants avec l'emplacement, la qualification et l'étendue des activités exercées par les sous-traitants ; • la spécification des exigences relatives aux processus informatiques du prestataire, y compris la sécurité, la maintenance, la gestion de l'exploitation et du développement, ainsi que les exigences de sécurité relatives à la gestion des ressources humaines ; • des procédures de gestion des incidents et de coopération à cet égard, incluant à la fois les employés de l'établissement assujetti et les prestataires de services, en veillant à ce que les parties soient rapidement informées et que les activités réalisées soient adaptées à l'incident ; • les services de soutien offerts par le prestataire : l'établissement assujetti doit considérer que, du fait que les services fournis par le prestataire sont souvent globaux, les accords peuvent ne pas déterminer les fuseaux horaires ou peuvent déterminer ces fuseaux de manière désavantageuse pour l'entité contrôlée et donc l'établissement assujetti doit s'assurer que la période de résolution des problèmes dans le cadre du soutien offert sera couverte par le niveau garanti des services fournis ; et • le droit applicable à la convention. L'UKNF a publié en janvier 2020 des recommandations sur le recours au *Cloud computing* (public et hybride) par les entités sous sa supervision. Ces recommandations reprennent en partie les clauses	

Juridiction	Position de l'autorité de supervision	Conformité aux Orientations ABE
	devant être intégrées dans la convention d'externalisation[264]. En outre, selon les recommandations de janvier 2020, l'établissement assujetti doit notifier au régulateur, dans les 14 jours précédant le début du traitement des données par Cloud (et si l'externalisation est déjà en place, la notification doit avoir lieu avant le 1er août 2020). Dans le cadre de cette notification, il faut informer le régulateur (i) du type d'informations qui vont être traitées ; (ii) du nom du prestataire de Cloud et le type de services de Cloud fournis ; (iii) de la date de signature de la convention d'externalisation et son terme ; (iv) de la localisation du centre de traitement des données fournissant le service Cloud ; (v) de la conformité de la convention avec les conditions posées par les recommandations et (vi) des points de contact. Un modèle de formulaire de notification est en annexe des recommandations. Nous n'avons pas d'informations quant aux sanctions applicables en cas de manquement à ces obligations.	
Royaume-Uni	Après une période de consultation, la *Financial Conduct Authority* (**"FCA"**) a publié en juillet 2016[265] des recommandations pour les entreprises (hors établissements de crédit et entreprises d'investissement dans le champ de CRR) ayant recours à des prestataires de Cloud. Deux consultations ont été lancées par l'Autorité de supervision prudentielle britannique (**"PRA"**)[266] et la FCA[267] en décembre 2019, ayant pour objectif notamment de se mettre en conformité avec les Orientations ABE 2019, et prendre en compte les recommandations de l'AEAPP. La période de consultation, qui devrait se clôturer le 1er octobre 2020	Non – selon le tableau de conformité de l'ABE, la PRA et la FCA ont toutes deux déclaré avoir l'intention de s'y conformer.

[264] *Page 15 et seq.*

[265] *Ce document a été mis à jour à plusieurs reprises, la dernière version datant de septembre 2019.*

[266] *https://www.bankofengland.co.uk/prudential-regulation/publication/2019/outsourcing-and-third-party-risk-management*

[267] *https://www.fca.org.uk/publications/consultation-papers/cp-19-32-building-operational-resilience-impact-tolerances-important-business-services*

Juridiction	Position de l'autorité de supervision	Conformité aux Orientations ABE
	a été prolongée en raison de la crise sanitaire née de l'épidémie de Covid-19.	

II. États-Unis

Position de l'autorité de supervision
Le *Federal Financial Institutions Examination Council* (FFIEC) a publié une note le 10 juillet 2012 dans laquelle elle indique que les établissements bancaires et financiers souhaitant avoir recours au Cloud doivent se référer aux risques sur l'externalisation indiqués dans une autre publication du FFIEC de décembre 2011. Afin de pallier ces risques, le FFIEC indique (i) qu'il faut procéder à une évaluation des risques, (ii) procéder à un audit du sous-traitant, (iii) revoir ou mettre en place des politiques de sécurité informatique, (v) identifier les risques réputationnels, juridiques et règlementaires, (vi) prévoir une politique de continuité des opérations en cas de perturbation.

III. Chine

Position de l'autorité de supervision
L'externalisation à des prestataires de Cloud par des établissements bancaires et financiers n'est pas encadrée de manière spécifique, mais est abordée dans différentes règlementations, notamment celles traitant de la cybersécurité, des mesures de protection des clients de services financiers et de la lutte anti-blanchiment. Il semblerait qu'une notice traitant de la gestion efficace des technologies par les établissements assujettis ait été préparée par les régulateurs bancaires chinois, toutefois cette notice n'est pas disponible au public[268].

[268] https://www.pkulaw.com/en_law/6a55b5a0600676e0bdfb.html?keyword=%e4%b8%ad%e5%9b%bd%e4%ba%ba%e6%b0%91%e9%93%b6%e8%a1%8c%e5%85%b3%e4%ba%8e%e5%8f%91%e5%b8%83%e9%87%91%e8%9e%8d%e8%a1%8c%e4%b8%9a%e6%a0%87%e5%87%86%e5%81%9a%e5%a5%bd%e4%b8%aa%e4%ba%ba%e9%87%91%e8%9e%8d%e4%bf%a1%e6%81%af%e4%bf%9d%e6%8a%a4%e6%8a%80%e6%9c%af%e7%ae%a1%e7%90%86%e5%b7%a5%e4%bd%9c%e7%9a%84%e9%80%9a%e7%9f%a5

ANNEXE 4

Aperçu des principales différences entre les orientations sur l'externalisation et le projet de règlement DORA

ANNEXE 4
APERÇU DES PRINCIPALES DIFFÉRENCES ENTRE LES ORIENTATIONS SUR L'EXTERNALISATION ET LE PROJET DE RÈGLEMENT DORA

		Orientations sur l'Externalisation	Règlement DORA	Commentaires
1.	**Nature juridique et champ d'application**			
1.1	Nature juridique	Contraignantes pour les établissements assujettis dès lors que leurs autorités de supervision compétentes ont déclaré s'y conformer et les intégrer dans leurs pratiques de supervision.	Effet direct dans le droit interne des États membres.	Le Règlement DORA d'application directe permettra une application harmonisée de ses exigences (alors que la force contraignante des Orientations sur l'Externalisation relève du choix opéré par chaque autorité nationale compétente).
1.2	Champ d'application *rationae personae*	Établissements assujettis : • établissements de crédit ; • entreprises d'investissement (soumis à CRD IV) ; • établissements de paiement ; et • établissements de monnaie électronique. Mise en place sur base individuelle et consolidée.	Tous les établissements et les professionnels réglementés des secteurs bancaire, financier et assurantiel ainsi que les prestataires de services de TIC[269], dont les prestataires de Cloud (Les prestataires TIC). Mise en place sur base individuelle et consolidée.	Le Règlement DORA a un champ d'application *rationae personae* plus étendu que celui des Orientations sur l'Externalisation.
1.3	Champ d'application *rationae materiae*	Activités externalisées.	Fonctions et activités liées aux TIC confiées à des prestataires TIC (même s'il ne s'agit pas d'activités "externalisées").	Le Règlement DORA a un champ d'application *rationae materiae* : • plus réduit concernant le type de fonction ou d'activité exercée

[269] *Technologies de l'information et de la communication (TIC).*

		Orientations sur l'Externalisation	Règlement DORA	Commentaires
				par le tiers concerné ; et • plus étendu concernant le type de rapport/relation juridique avec le tiers concerné que les Orientations sur l'Externalisation.
1.4	Principe de proportionnalité	Prise en compte : • de la complexité, l'importance des fonctions externalisées ; et • du profil de risque individuel, de la nature et du modèle d'entreprise ainsi que de la complexité de leurs activités.	Prise en compte : • de la portée, la complexité et l'importance des fonctions TIC pour lesquelles les établissements assujettis ont identifié une dépendance ; et • du risque associé aux contrats conclus avec des Prestataires TIC.	Différence de critères d'appréciation entre le Règlement DORA et les Orientations sur l'Externalisation.
2.	**Exigences organisationnelles applicables aux établissements et professionnels assujettis**			
2.1	Prise en compte et atténuation du risque de concentration	Obligation de prendre en compte le risque de concentration dans l'évaluation des risques liés à une fonction externalisée.	Définition du risque de concentration[270]. Obligation de prendre en compte le risque de concentration dans l'évaluation des risques liés à une fonction confiée à un prestataire TIC. Obligation de mettre en place et d'appliquer une	Obligation renforcée dans le Règlement DORA par rapport aux Orientations sur l'Externalisation.

[270] *L'exposition à un ou plusieurs prestataires TIC « critiques » créant un degré de dépendance tel vis-à-vis de ces prestataires TIC que l'indisponibilité ou toute autre défaillance de ces derniers met potentiellement en danger la capacité d'une entité financière, et en définitive du système financier de l'Union dans son ensemble, à assurer des fonctions critiques, ou à subir d'autres types d'effets négatifs, y compris des pertes importantes.*

		Orientations sur l'Externalisation	Règlement DORA	Commentaires
			stratégie multi-fournisseurs[271].	
2.2	Politiques internes et fonction dédiée	Obligation d'élaborer et de mettre à jour une politique d'externalisation. Obligation de nommer un responsable dédié à l'externalisation.	Obligation d'élaborer et de mettre à jour une politique relative à l'utilisation de services de TIC fournis par des prestataires TIC[272]. Obligation de nommer un responsable dédié au suivi des fonctions TIC.	Obligations similaires dans le Règlement DORA et les orientations sur l'externalisation (mais plus détaillées à ce stade dans ces orientations).
2.3	Fonction d'audit	Obligation d'élaborer et de mettre à jour des plans d'audits. Conduite d'audits sur la base d'une approche par les risques. Obligations et recommandations relatives aux modalités de conduite des audits (certifications, audits multi-clients). Obligation de s'assurer que les auditeurs disposent de connaissances et de compétences adéquates.	Obligation d'élaborer et de mettre à jour des plans d'audits de leurs fonctions TIC. Conduite d'audits sur la base d'une approche par les risques. Obligation de s'assurer que les auditeurs disposent de connaissances et de compétences adéquates.	Obligations similaires dans le Règlement DORA et les Orientations sur l'Externalisation (mais plus détaillées à ce stade dans ces orientations).
2.4	Documentation	Obligation d'identifier et de documenter les fonctions externalisées. Obligation de consigner les informations sur ces fonctions dans un registre tenu à la disposition des autorités de supervision compétentes sur leur demande.	Obligation d'identifier et de documenter les fonctions qui dépendent de prestataires TIC et les contrats conclus avec ces prestataires TIC. Obligation de consigner les informations sur ces fonctions dans un registre tenu à la disposition des autorités de supervision	Obligations similaires dans le Règlement DORA et les Orientations sur l'Externalisation (mais plus détaillées à ce stade dans ces orientations).

[271] La stratégie « multi-fournisseurs » doit mentionner les principales dépendances de l'établissement à l'égard de prestataires TIC et doit exposer les motifs justifiant le recours à plusieurs prestataires TIC distincts.

[272] Le contenu de cette politique sera détaillé dans des règlements délégués de second niveau.

		Orientations sur l'Externalisation	Règlement DORA	Commentaires
			compétentes sur leur demande[273].	
2.5	Information des régulateurs sur les fonctions concernées	Obligation d'informer en temps utile les autorités de supervision compétentes avant d'externaliser des fonctions critiques ou lorsque des fonctions sont devenues critiques. Obligation d'informer l'autorité compétente en cas de changements significatifs ou d'événements graves affectant les dispositifs d'externalisation.	Obligation d'informer en temps utile les autorités de supervision compétentes avant de confier des fonctions critiques à des prestataires TIC ou lorsque ces prestations sont devenues critiques. Obligation d'informer au moins une fois par an l'autorité de supervision compétente à propos des nouveaux contrats conclus avec des prestataires TIC (y compris pour les fonctions non critiques).	Obligation renforcée dans le Règlement DORA par rapport aux Orientations sur l'Externalisation (s'agissant de l'information annuelle des autorités de supervision compétentes au sujet des nouveaux contrats de prestation de services non critiques).
2.6	Diligences préalables	Obligation : • de déterminer si la fonction déléguée à un tiers est une fonction critique ou non ; • d'évaluer si les conditions de la surveillance de l'externalisation sont remplies ; • d'identifier et d'évaluer des risques associés au dispositif d'externalisation (en particulier le risque de concentration, comme mentionné ci-dessus) ; • d'effectuer les vérifications nécessaires afin de déterminer si un prestataire est apte à exercer la fonction ; et	Obligations similaires. Obligation de s'assurer que les prestataires TIC appliquent et respectent des normes de sécurité informatique appropriées et accentuées avant de conclure un contrat de services avec lui.	Obligations similaires dans le Règlement DORA et les Orientations sur l'Externalisation (mais plus détaillées à ce stade dans ces orientations).

[273] *Le format du registre et la liste des informations seront développés dans des règlements délégués de second niveau.*

		Orientations sur l'Externalisation	Règlement DORA	Commentaires
		– d'identifier et d'évaluer l'existence de conflits d'intérêts liés à l'externalisation.		
2.7	Continuité d'activité	Obligation d'élaborer, de mettre à jour et tester des plans de continuité d'activité pour les fonctions externalisées. Obligation d'élaborer et de mettre à jour des mécanismes de contrôle de la sécurité des TIC pour les fonctions externalisées TIC.	Obligation d'élaborer et de mettre à jour une stratégie de résilience opérationnelle[274]. Obligation d'élaborer une politique de continuité d'activité des fonctions TIC. Obligation de mettre en œuvre des systèmes de secours en cas d'indisponibilité des systèmes TIC.	Obligations renforcées dans le Règlement DORA par rapport aux Orientations sur l'Externalisation.
2.8	Stratégie de sortie	Obligation de prévoir une stratégie de sortie (pour les fonctions externalisées essentielles).	Obligation de prévoir une stratégie de sortie (pour toutes les fonctions TIC confiées à des tiers, même non critiques ou importantes).	Obligation renforcée dans le Règlement DORA par rapport aux Orientations sur l'Externalisation (car élargie aux fonctions et activités TIC non critiques ou importantes).
3.	**Exigences concernant la documentation contractuelle**			
3.1	Contenu des contrats de prestation de services	Obligation de prévoir les droits et obligations des parties dans un contrat écrit. Obligation de prévoir dans tous les contrats	Obligation de prévoir les droits et obligations des parties dans un contrat écrit. Obligation de prévoir dans tous les contrats relatifs à des fonctions TIC :	Obligations renforcées dans le Règlement DORA par rapport aux Orientations sur l'Externalisation.

[274] *La stratégie de résilience opérationnelle a pour objet de définir les modalités de mise en œuvre du cadre de la gouvernance des risques liés aux fonctions TIC, notamment concernant l'adéquation des systèmes TIC aux objectifs de sécurité et de performance de l'activité, le niveau d'appétence aux risques, le traitement des incidents de sécurité. Dans le cadre de cette stratégie, les établissements assujettis sont tenus de conduire des tests d'intrusion (thread led penetration testing) tous les trois ans, au moins pour leurs fonctions et services critiques confiés à des prestataires TIC.*

		d'externalisation des clauses relatives : • au contrôle de l'exécution des prestations externalisées par les établissements assujettis (niveaux de services) • au contrôle du prestataire par les établissements assujettis et les autorités compétentes (audit, coopération avec les autorités compétentes) • à la confidentialité, l'accessibilité, la disponibilité, l'intégrité des données et la sécurité des systèmes • au droit de résiliation des établissements et à l'assistance du prestataire de services pour le transfert ou la ré internalisation des prestations externalisées. Obligation de prévoir dans les contrats d'externalisation de prestations essentielles des clauses supplémentaires, notamment des clauses relatives : • aux obligations d'indiquer le lieu d'exécution des prestations externalisées et de stockage/traitement des données et d'informer l'établissement assujetti en cas de modification de ces lieux ;	• les clauses que les Orientations sur l'Externalisation imposent d'insérer dans tous les contrats d'externalisation ; et • certaines clauses que les Orientations sur l'Externalisation imposent d'insérer dans les contrats d'externalisation de prestations essentielles (*i.e.* les clauses listées aux (i), (vii) et (viii) ci-contre). Obligation de prévoir dans les contrats relatifs à des fonctions TIC critiques ou importantes des clauses supplémentaires, notamment : • les clauses que les Orientations sur l'Externalisation imposent d'insérer dans les contrats relatifs à des fonctions TIC critiques ou importantes (à l'exception des clauses listées aux (iii) et (vi) ci-contre) ; et • une clause relative à l'obligation pour les Prestataires TIC de fournir une assistance aux professionnels assujettis en cas d'un incident de sécurité, sans frais supplémentaires ou à des frais déterminés à l'avance.	

		Orientations sur l'Externalisation	Règlement DORA	Commentaires
		• aux obligations de *reporting* du prestataire en cas d'événement affectant l'exécution des prestations externalisées ; • à la reconnaissance des pouvoirs des autorités de résolution compétentes (le cas échéant) ; • aux obligations du prestataire en cas de sous-externalisation ; • à l'obligation pour le prestataire d'appliquer et tester les plans de continuité d'activité ; • à l'obligation pour le prestataire de souscrire une assurance (lorsque cette assurance est obligatoire en vertu de la réglementation applicable) ; • à l'obligation pour le prestataire de garantir l'accès aux données appartenant aux établissements assujettis en cas d'interruption de l'activité ou d'insolvabilité ; et • à l'obligation pour le prestataire d'élaborer, de tester et d'appliquer une stratégie de sortie.		
3.2	Clauses type obligatoires	Pas de clauses type obligatoires.	Obligation pour les professionnels assujettis et les prestataires TIC d'utiliser des clauses types élaborées par la Commission européenne	Obligations renforcées dans le Règlement DORA par rapport aux Orientations sur l'Externalisation.

		Orientations sur l'Externalisation	Règlement DORA	Commentaires
			dans les contrats relatifs aux fonctions TIC[275].	
4.	**Surveillance des prestataires de services**			
4.1	Surveillance directe des prestataires	Pas de surveillance directe des prestataires de services auxquels sont externalisées des prestations.	Surveillance directe des prestataires TIC établis dans l'UE et considérés comme "critiques" par les autorités européennes de supervision (afin de s'assurer que ces prestataires TIC aient des dispositifs de gouvernance suffisamment complets, robustes et efficients pour maîtriser les risques TIC qu'ils occasionnent pour les professionnels assujettis). Interdiction pour les professionnels assujettis d'avoir recours à un prestataire TIC établi dans un pays tiers qui, s'il était établi dans l'UE, serait considéré comme "critique".	Surveillance d'une nouvelle catégorie de prestataires (prestataires TIC "critiques").

[275] *Ces clauses seront adoptées par la voie de règlements délégués de second niveau.*