Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

CONSEIL GÉNÉRAL DE L'ÉCONOMIE
DE L'INDUSTRIE, DE L'ÉNERGIE ET DES TECHNOLOGIES

TELEDOC 792
BATIMENT NECKER
120, RUE DE BERCY
75572 PARIS CEDEX 12

N° 2019/16/CGE/SG

février 2020

Mise en œuvre d'une politique de localisation des données critiques de paiement en Europe

Rapport à

Monsieur le Ministre de l'Economie et des Finances

établi par

Sandrine LEMERY
Ingénieure générale des mines

Rémi STEINER
Ingénieur général des mines

MINISTÈRE DE L'ÉCONOMIE
ET DES FINANCES

SOMMAIRE

SYNTHESE 5

TABLE DES RECOMMANDATIONS 8

Introduction 10

1 Les risques d'atteinte à la souveraineté 11

1.1 Les leçons du passé 11

1.1.1 L'affaire SWIFT (2006) 11

1.1.2 Les révélations de Snowden (2013) 12

1.1.3 Les sanctions américaines en Crimée et en Russie (2014) 13

1.1.4 La panne d'Amazon en 2017 14

1.1.5 L'affaire USA v. Microsoft Corporation (2017 - 2018) 15

1.1.6 L'affaire Cambridge Analytica (2018) 17

1.1.7 Les enseignements et les recommandations du rapport Gauvain (2019) 18

1.2 Différentes formes d'atteintes à la souveraineté 19

1.2.1 Risque politique 20

1.2.2 Risque de soumission des ressortissants européens à des autorités étrangères 20

1.2.3 Risque d'espionnage 20

1.2.4 Risque d'utilisation des données personnelles à des fins commerciales 20

1.2.5 Risque économique 20

1.2.6 Risque de gouvernance des systèmes des paiements internationaux 20

1.2.7 Risque d'affaiblissement de la capacité d'enquête des autorités de police et de justice européennes 20

2 Les pistes de préservation de l'indépendance européenne en matière de paiement 21

2.1 Il existe un assez large consensus en faveur d'une localisation en Europe des données de paiement 21

2.1.1 La criticité des données de paiement au regard des enjeux de souveraineté 21

2.1.2 Des exemples étrangers (Inde, Indonésie, Turquie…) plus ou moins probants, des objections, mais pas d'inconvénient insurmontable 24

2.1.3 Les missionnaires se prononcent en faveur d'une obligation de localisation sur le sol européen des données de paiement 28

2.1.4 La localisation des données en Europe ne constitue qu'une réponse partielle et imparfaite aux enjeux de souveraineté européenne en matière de paiement 29

2.2 La révision du règlement interchange 32
2.2.1 Quelques indications sur le paiement par carte 33
2.2.2 La défense des cartes co-badgées 35
2.2.3 La séparation entre le *scheme* (la définition des règles) et le *processing* (l'exécution des traitements) 38
2.2.4 L'alignement des modèles d'affaires de la carte et de l'*instant payment* 42
2.3 Tirer le meilleur parti des techniques de tokenisation 44
2.3.1 Les différents cas d'utilisation de la *tokenisation* 44
2.3.2 La *tokenisation* de paiement permet la dématérialisation de la carte de paiement 48
2.3.3 La *tokenisation* de paiement facilite pour les sites marchands la répétition des paiements 52
2.4 L'élaboration d'un scheme européen de paiement 54
2.4.1 Plusieurs projets passés de création de nouveaux *schemes* de paiement 54
2.4.2 Le projet EPI de nouveau *scheme* européen 55
2.4.3 Quelques interrogations soulevées par l'élaboration d'un *scheme* européen de paiement 57
2.5 L'harmonisation des exigences de conformité au règlement général sur la protection des données personnelles (RGPD) 59
2.5.1 Quelques rappels sur le RGPD 59
2.5.2 L'application de ces dispositions au contexte du paiement 62
2.5.3 L'obligation de localisation des données favorise le respect du RGPD 65
2.6 La protection des données de paiement stockées sur le cloud 67
2.6.1 Les enjeux liés à l'essor du stockage et du traitement des données sur le *cloud* 67
2.6.2 Les entreprises financières recourent de plus en plus au *cloud* 70
2.6.3 La localisation sur le territoire européen des données de paiement hébergées sur le *cloud* 72
2.7 Les initiatives reposant sur la blockchain 74
2.7.1 Le projet Libra de Facebook 74
2.7.2 Les projets de monnaie digitale de banque centrale 76
2.7.3 Les enjeux de données propres à la *blockchain* 78
ANNEXES 81
Annexe 1 : Lettre de mission 82
Annexe 2 : Liste des acronymes et expressions étrangères utilisés 84
Annexe 3 : Liste des personnes rencontrées ou interrogées 88
Annexe 4 : Pistes de recommandations soumises le 20 novembre 2019 aux interlocuteurs de la mission pour commentaires 94

SYNTHESE

Dans une économie toujours plus ouverte aux influences mondiales, et alors que l'Europe cherche à affirmer son indépendance économique et politique face à des puissances extra-européennes, tant la confiance dans les systèmes de paiement que le contrôle des données liées aux transactions de paiement constituent des enjeux critiques.

En effet, les entreprises extra-européennes jouent dans les services de paiement un rôle croissant et plusieurs événements alarmants, au cours des années passées, ont montré les risques encourus par l'Europe lorsque les données de paiement ne sont pas suffisamment protégées. L'une des orientations de la nouvelle stratégie 2019-2024 du Comité national des paiements scripturaux consiste à concourir à l'ambition européenne d'un marché unique des paiements et à créer les conditions d'une indépendance européenne dans ce domaine. L'une des actions proposées consiste en l'étude des modalités d'une obligation de localisation des données de paiement de détail sur le territoire européen.

Le présent rapport a pour ambition de donner des éléments d'appréciation sur la faisabilité, sur les conséquences et sur les limites d'une telle obligation qui serait faite aux acteurs du paiement, établissements financiers, commerçants et leurs sous-traitants, sur la foi de discussions avec un panel d'interlocuteurs actifs en France et représentatifs de la diversité des acteurs concernés. Si cette obligation ne se conçoit pas sans une volonté politique forte et largement partagée au sein des pays de l'Union européenne, elle paraît, dans son principe, assez favorablement accueillie en France. Seuls un petit nombre d'acteurs très internationaux y a élevé des objections, et ces objections ne paraissent pas insurmontables.

La mission n'estime pas pertinent de discriminer pour une même opération de paiement des données qui seraient critiques d'autres qui ne le seraient pas. Elle estime au contraire que l'obligation de localisation devrait porter sur toutes les données liées à une transaction de paiement, dès que deux conditions sont réunies : en premier lieu, la transaction intervient entre deux parties localisées en Europe ; en second lieu, ces données peuvent être rattachées directement ou indirectement à une personne physique, par l'intermédiaire de données de sécurité personnalisées telles qu'un identifiant de compte, de carte ou de tout autre instrument de paiement (que cet identifiant figure en clair ou sous forme de pseudonyme).

Selon les cas, les données ainsi définies, désignées dans la suite par l'expression « données de paiement », seraient plus ou moins nombreuses et plus ou moins variées : les coordonnées du commerçant, l'heure et le détail des achats, la géolocalisation ou l'adresse IP du consommateur…

L'obligation de localisation s'imposerait à l'ensemble des acteurs économiques, qu'ils soient ou non régulés. Elle aurait un double effet à leur égard : les données de paiement devraient être stockées sur le territoire européen, d'une part ; et elles ne pourraient être transférées hors des frontières européennes, d'autre part. L'obligation pourrait prendre place dans le RGPD, sous la surveillance des autorités de contrôle de la protection des données à caractère personnel.

Si elle présente un intérêt en termes de souveraineté européenne, cette obligation de localisation, pour autant, ne constituerait pas à elle seule une parade efficace contre l'ensemble des menaces pouvant affecter les systèmes ou les données de paiement. En outre les délais nécessaires à l'incorporation dans le droit de l'Union d'une obligation générale de localisation des paiements ne sont pas à négliger. Pour ces deux raisons, d'autres pistes de renforcement de la souveraineté européenne en matière de paiement ont été examinées, conduisant soit à des mesures complémentaires, soit à une mise en œuvre par étapes de l'obligation de localisation.

Dans le champ du paiement par carte, qui représente une part très importante des paiements de détail, la révision imminente du règlement 2015/751, relatif aux commissions d'interchange, ouvre à cet égard des opportunités. Deux dispositions de ce règlement ont retenu plus particulièrement l'attention de la mission en ce qu'elles ont préparé et pourraient faciliter la prise en considération d'objectifs de renforcement de l'indépendance européenne en matière de paiement de détail.

La première, dans une logique de renforcement de la concurrence et de baisse du coût des paiements pour les commerçants, a obligé ce qu'on appelle les *schemes*[1] de paiement par carte (Visa, MasterCard, groupement Carte Bancaire…) à prévoir une séparation entre l'entité qui assure la gouvernance (elle fixe les règles de fonctionnement, de résolution des litiges…) et celle qui effectue le traitement des transactions. Un prolongement assez naturel de cette obligation de séparation, cohérent avec l'obligation de localisation, consisterait à ce que l'entité qui assure le traitement des opérations – ainsi que les données qu'elle traite -– soit localisée sur le territoire européen.

La seconde disposition du règlement interchange qui a retenu l'attention de la mission concerne la situation particulière des cartes co-badgées, très utilisées en France et dans plusieurs autres pays européens. La particularité de ces cartes consiste à donner à leur utilisateur un accès à deux systèmes de paiement : un *scheme* de paiement international, tel que Visa ou MasterCard, et un *scheme* domestique, tel que le groupement Carte bancaire en France. L'intention du législateur européen était que les deux marques représentées sur une carte co-badgée soient concurrentes, plutôt que complémentaires. Mais les nouvelles offres de dématérialisation des cartes co-badgées dans un smartphone (Apple Pay, Google Pay, Samsung Pay…) pourraient, contrairement à l'esprit du règlement, porter préjudice au *scheme* domestique, ce qui ne paraît pas acceptable. Le règlement, modifié en tant que de besoin, devrait garantir une stricte équivalence entre les deux marques associées à une carte co-badgée.

La dématérialisation des cartes bancaires constitue une des multiples applications de la *tokenisation*, qui vise à substituer à une donnée sensible (telle qu'un numéro de compte ou de carte bancaire) un pseudonyme. Ces applications sont utiles et variées ; elles peuvent jouer un rôle de renforcement de la sécurité dans l'environnement immédiat d'un site de commerce (on parle alors de *token* de sécurité) ou dans toutes les étapes de traitement d'une transaction de paiement (on parle alors de *token* de paiement). Dans tous les cas, une attention particulière devrait être apportée aux données manipulées par le *token service provider* (TSP), c'est-à-dire l'entité qui assure la *tokenisation* et, le cas échéant, la *de-tokenisation*.

Depuis plusieurs mois, des grandes banques européennes ont engagé un projet, désormais baptisé EPI, de création d'un *scheme* pan-européen de paiement, qui constituerait une alternative aux *schemes* internationaux américains ou chinois. Cette initiative procède des mêmes préoccupations que celles qui sont à l'origine du présent rapport. Son résultat est encore incertain. Du point de vue des pouvoirs publics, il serait souhaitable que le projet affiche d'emblée des ambitions fortes : une marque de paiement européenne qui s'appuierait sur un réseau d'acceptation non seulement en Europe, mais aussi hors des frontières européennes, et qui prendrait progressivement toute sa place dans les instances internationales de gouvernance des systèmes de paiement par carte (EMVCo, PCI-SSC).

Par ailleurs, il paraît opportun à la mission d'engager une réflexion sur une évolution du statut juridique des *schemes* nationaux, leur transformation en sociétés de capitaux étant susceptible de favoriser un meilleur alignement des intérêts de ces *schemes* et de ceux de leurs actionnaires, des rapprochements capitalistiques entre eux, ainsi que la valorisation par les banques de leurs investissements passés au profit de nouvelles ambitions pan-européennes.

En outre, le principal enjeu de la révision du règlement interchange (la question du plafond des commissions) n'est pas sans lien avec les préoccupations de la mission. Celle-ci estime que le plafonnement actuel des commissions d'interchange permet de répondre (au moins à court terme)

[1] Ensemble des règles de fonctionnement, de responsabilité, de résolution des litiges, etc… instituées par des acteurs du paiement tels que Visa ou MasterCard afin d'assurer le traitement des transactions de paiement

aux réserves de la Commission à l'égard du principe de telles commissions multilatérales. Mais il ne faudrait pas que l'existence de commissions d'interchange, favorable au modèle d'affaire du paiement par carte, entrave l'émergence de systèmes de paiement plus innovants et plus européens fondés sur le paiement instantané. Il conviendrait donc d'assurer des conditions neutres de concurrence entre un paiement par carte traditionnel et d'autres formes de règlements qui se déboucleraient par un paiement instantané, lesquelles devraient alors donner lieu au même plafond autorisé de commissions d'interchange.

La mission a aussi examiné les enjeux d'une obligation de localisation des paiements sous l'angle des règles de protection des données à caractère personnel. Si les personnes qui se trouvent sur le territoire de l'Union européenne sont toutes protégées par le règlement général sur la protection des données personnelles (RGPD), indépendamment du lieu de stockage et de traitement des données des données qui les concernent, l'obligation de localisation des données de paiement (qui sont des données à caractère personnel) améliorerait, les chances de caractériser des manquements aux règles du RGPD et de poursuivre une entreprise fautive. Elle conduirait, par voie de conséquence, à un meilleur *level playing field* entre toutes les entreprises, qu'elles soient européennes ou non, traitant de données de paiement.

Par ailleurs, le RGPD pose des principes qui sont interprétés avec plus ou moins de rigueur selon l'histoire et la culture de chaque Etat. Ceci semble particulièrement vrai en ce qui concerne les données de paiement. L'entité chargée d'assurer la cohérence de l'interprétation et de la mise en œuvre des principes du RGPD est le Comité Européen de la Protection des Données (CEPD), qu'il serait opportun de saisir afin de garantir une communauté de vues sur des sujets tels que celui du partage des responsabilités entre les protagonistes d'une transaction de paiement, celui des conditions de licéité d'une valorisation commerciale des données de paiement et celui de la durée de conservation des données de transaction par les intermédiaires de la chaîne du paiement.

Le stockage et le traitement des données tendent à s'appuyer de plus en plus sur des infrastructures de *cloud* public, souvent proposées par de grandes entreprises américaines. Cette tendance ne semble pas incompatible avec la mise en œuvre d'une décision de localisation des données de paiement sur le territoire européen. Tout d'abord, des solutions permettent à une entreprise d'utiliser plusieurs prestataires de *cloud* public différents (multi-*cloud*) et d'associer ses propres serveurs et ceux qu'elle loue à des tiers (*cloud* hybride). Ensuite, les préoccupations de souveraineté peuvent favoriser l'essor de prestataires européens de services *cloud* et conduire de grands fournisseurs internationaux de services *cloud* à prendre des engagements de localisation des données qu'ils traitent. Enfin, de nouvelles techniques de chiffrement, dit homomorphe, permettent désormais des calculs sur des données chiffrées, sans que le prestataire de services *cloud* ait accès aux données d'origine.

Dans ces conditions, les établissements financiers régulés qui ont recours au *cloud* pourraient être plus fermement incités, par un renforcement des lignes directrices édictées par l'Autorité Bancaire Européenne (EBA), à assurer la localisation sur le territoire européen des données de paiement.

Enfin, la mission évoque la question de l'utilisation d'une *blockchain* publique pour gérer des transactions de paiement entre personnes physiques (sur le modèle, par exemple du bitcoin). Celle-ci apparaît, par nature, difficilement conciliable avec la mise en œuvre d'une obligation de localisation des données de paiement – et peut-être même avec le RGPD. Mais il existe de multiples possibilités de mise en œuvre de la technologie *blockchain*, de sorte qu'aucune appréciation définitive ne peut être portée. A ce stade, les projets de *stablecoins* (tels que le Libra) comme ceux de monnaie digitale de banque centrale de détail apparaissent trop peu avancés pour une analyse plus approfondie d'éventuels enjeux spécifiques de localisation des données.

*

* *

TABLE DES RECOMMANDATIONS

Recommandation n° 1. Instituer à l'échelle de l'Espace économique européen une obligation de localisation sur le sol européen des données relatives à des paiements intra-européens, lorsque ces données sont liées aux données de sécurité personnalisées d'une personne physique.

Cette obligation serait stricte, c'est-à-dire que les données de paiement soumises à l'obligation de localisation ne pourraient être transférées hors des frontières européennes, et elle s'appliquerait à l'ensemble des acteurs économiques, qu'ils soient ou non régulés.

Ces règles s'inscriraient dans le cadre du règlement 2016/679 (RGPD). 29

Recommandation n° 2. En cohérence avec la Recommandation n° 1, saisir l'opportunité de la prochaine révision du règlement 2015/751 (interchanges) pour préciser que les entités de traitement (au sens de l'article 7) sont tenues de localiser les données de paiement sur le sol européen. 42

Recommandation n° 3. En cohérence avec la Recommandation n° 1, veiller à ce que les solutions *X-Pay* de dématérialisation des cartes bancaires sur un terminal mobile (*smartphone*, tablette…) ne donnent pas lieu, à l'occasion d'une transaction intra-européenne, au transfert hors des frontières européennes de données de paiement. 50

Recommandation n° 4. Les banques émettrices de cartes co-badgées, qui associent deux *schemes* de paiement pour lesquels existent des services de *tokenisation*, devraient garantir que tout service permettant la dématérialisation de la carte sur un terminal mobile (*smartphone*, tablette…) donne lieu à la création de deux *tokens* de paiement et respecte une stricte équivalence entre les deux marques associées à la carte bancaire.

Le législateur européen devrait, si nécessaire, préciser à cet effet l'article 8 du règlement 2015/751 lors de sa prochaine révision. 51

Recommandation n° 5. Le Comité Européen de la Protection des Données (CEPD) devrait se prononcer sur l'interprétation des règles du RGPD à retenir en matière de paiement, s'agissant notamment :

- du statut des acteurs de la chaîne de paiement (sous-traitant ou co-responsable de traitement) et des conséquences de ce statut ;

- des conditions de licéité d'une valorisation commerciale des données de paiement ;

- de la durée de conservation des données de transaction par les intermédiaires de la chaîne du paiement. 65

Recommandation n° 6. Lorsque des établissements financiers européens externalisent le stockage ou le traitement de données de paiement sur le *cloud,* ils devraient être incités :

- à recourir de préférence à un prestataire européen de services *cloud* ;

- à défaut, à exiger que le prestataire *cloud* s'engage contractuellement à ce que les données soient détenues et traitées en Europe ;

- à exiger que les données de paiement soient chiffrées dans des conditions telles que le prestataire de services *cloud* ne puisse lui-même les décrypter. 74

INTRODUCTION

Une stratégie nationale sur les moyens de paiement scripturaux pour les années 2019 à 2024 a été approuvée par le Comité National des Paiements Scripturaux le 18 février 2019. L'une des trois grandes orientations de ce plan consiste à concourir à l'ambition européenne d'un approfondissement du marché unique des paiements de détail et, tout particulièrement, à créer les conditions d'une indépendance européenne dans ce domaine.

Les actions proposées à ce titre consistent en une analyse des interdépendances du marché européen des paiements, notamment vis-à-vis des acteurs extra-européens, en l'étude des modalités d'une politique de localisation au sein de l'Union européenne des données de paiement et en un renforcement de la coopération entre le GIE Carte Bancaire et les autres *schemes* nationaux de paiement par carte.

C'est dans ce contexte que, le 19 juin 2019, le Ministre de l'économie et des finances a saisi le vice-président du Conseil général de l'économie de la demande d'une mission visant à étudier la mise en œuvre d'une politique de localisation des données de paiement en Europe, le rapport et les recommandations devant être présentés avant la fin de l'année 2019.

Le Conseil général de l'économie était invité à apprécier l'importance et la sensibilité des traitements extra-européens portant sur des données critiques de paiement, ainsi que les enjeux de souveraineté associés à ces traitements, à la lumière à la fois des profondes évolutions de l'offre de services de paiements et de l'entrée en vigueur de deux textes européens importants : le règlement général sur la protection des données personnelles (RGPD) et la deuxième directive sur les services de paiement (DSP2).

La mission a auditionné un grand nombre d'acteurs représentatifs de la chaîne des paiements : organismes publics, organisations professionnelles, établissements régulés (banques et établissements de paiement), entreprises du commerce et prestataires de services spécialisés dans le domaine du paiement. Elle a été conviée à une réunion des membres de l'OCBF le 3 septembre 2019, au Conseil d'administration de l'Association du Paiement le 3 novembre 2019 et à une réunion du bureau d'orientation des moyens de paiements (BCOMP) de la FBF le 12 décembre 2019. Le 20 novembre, un document synthétisant les principales pistes de recommandations identifiées par la mission[2] a été envoyé pour réaction à ses premiers interlocuteurs (près de 50 à ce stade).

Le rapport ci-dessous constitue le rapport définitif de la mission, issu des entretiens menés par les rapporteurs et de la consultation indiquée ci-dessus. Les recommandations formulées sont destinées à alimenter les travaux du Comité national des paiements scripturaux. Elles ne se limitent pas à la seule question de la localisation des données, qu'il est apparu difficile d'isoler d'autres questions inhérentes aux conditions d'une indépendance européenne en matière de paiement.

Elles s'inscrivent dans la perspective de propositions qui pourraient être promues par la France et endossées par l'Union européenne ; mais dans les délais impartis, les missionnaires ont dû limiter leurs auditions à un échantillon d'interlocuteurs basés en France.

[2] Cf. Annexe 4 : Pistes de recommandations soumises le 20 novembre 2019 aux interlocuteurs de la mission pour commentaires, p. 94 et suivantes

1 LES RISQUES D'ATTEINTE A LA SOUVERAINETE

1.1 Les leçons du passé

L'objet de ce chapitre consiste à rappeler différents événements susceptibles d'illustrer la variété des menaces qui pourraient justifier une obligation de localisation sur le territoire européen des données de paiement.

1.1.1 L'affaire SWIFT (2006)

SWIFT est une société coopérative établie en Belgique, active dans le traitement de messages associés à des opérations de transfert financiers. Elle possédait au début des années 2000 deux centres de traitement – l'un en Europe, l'autre aux États-Unis – où tous les messages traités dans le cadre de son service SWIFTNet FIN étaient stockés "en miroir" pendant 124 jours. Au lendemain des attentats du 11 septembre 2001, le département du Trésor des Etats-Unis (*US Department of the Treasury*) a adressé plusieurs sommations au centre de traitement de SWIFT situé aux États-Unis visant à la communication des informations détenues par SWIFT.

La société SWIFT ne s'est pas opposée à ces sommations, mais a négocié en privé avec le Trésor américain un arrangement sur la manière de s'y conformer : le centre de traitement situé aux Etats-Unis a organisé le transfert en masse de données à caractère personnel depuis la base de données de SWIFT vers une "boîte noire" à la disposition de l'*US Department of the Treasury*, permettant à ce dernier d'effectuer des recherches ciblées[3].

Le 23 juin 2006, le New-York Times a révélé que la société de droit belge SWIFT collaborait avec la CIA et avec les agences de renseignement des États-Unis, en leur transférant depuis plus de quatre ans des copies des messages échangés entre les institutions financières du monde entier, dont SWIFT assurait le transport et l'archivage temporaire.

Ce transfert était décrit comme l'élément principal d'un programme gouvernemental secret de surveillance généralisée des transactions financières, dans le cadre de la politique de lutte pour la sécurité menée par les Etats-Unis. Le manque d'égard pour les libertés et les droits fondamentaux des personnes, comme l'étendue des pouvoirs d'exception accordés au Gouvernement américain, étaient critiqués[4].

Le 6 juillet 2006, le Parlement européen a adopté une résolution demandant que toute la vérité soit faite sur cette affaire[5]. Le 28 septembre 2006, la Commission belge de protection de la vie privée a estimé[6] que SWIFT, qui est domiciliée en Belgique, avait violé la loi belge en coopérant à l'insu de ses clients avec les autorités américaines dans le cadre de la lutte contre le terrorisme.

---

[3] Cf. l'avis du contrôleur européen de la protection des données sur le rôle de la Banque centrale européenne dans l'affaire SWIFT, §25 et 26
https://edps.europa.eu/sites/edp/files/publication/07-02-01_opinion_ecb_role_swift_fr.pdf

[4] Cf. l'article Wikipedia consacré au « *Terrorist Finance Tracking Program* » et la décision du 9 décembre 2008 de la Commission de la protection de la vie privée, §8 et 9
https://en.wikipedia.org/wiki/Terrorist_Finance_Tracking_Program

[5] Résolution du 6 juillet 2006 du Parlement européen sur l'interception des données des virements bancaires du système SWIFT par les services secrets américains
http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2006-0317+0+DOC+XML+V0//FR

[6] Avis du 27 septembre 2006 de la Commission de la protection de la vie privée relatif à la transmission de données à caractère personnel par la SCRL SWIFT suite aux sommations de l'UST (OFAC)
https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/avis_37_2006_0.pdf

Le 22 novembre 2006, le Groupe de coordination des autorités de protection des données de l'Union européenne (dit « G29 ») a rendu un avis qui met en cause la société SWIFT : « *SWIFT n'a pas respecté les règles européennes de protection des données, en acceptant de communiquer aux autorités américaines les données bancaires transitant par son réseau* ».

A la décharge de SWIFT, seules certaines catégories de messages interbancaires, et pour des périodes déterminées, ont été mises à la disposition de l'*Office of Foreign Assets Control* (OFAC), une division de l'*US Department of the Treasury*. Ces transferts ont été effectués en exécution d'injonctions (*subpoenas*) légales et contraignantes adressées par l'*US Department of the Treasury* à la succursale de SWIFT assurant l'exploitation du centre opérationnel américain.

Ces injonctions successives (64 au moment où l'information a été rendue publique) étaient expressément motivées, non seulement par des dispositions légales américaines, mais aussi par l'exécution d'obligations faites aux États par les Résolutions 1333 et 1373 du Conseil de sécurité des Nations-Unies. Il faut également noter que SWIFT avait informé en 2002 les banques du groupe des 10 (G10)[7] des données qu'elle transférait aux autorités américaines, mais que le G10 avait alors estimé que cette question ne relevait pas de sa mission de surveillance.

Tirant la leçon de sa mise en cause, le Conseil d'administration de SWIFT a décidé en septembre 2007 de modifier l'architecture de son réseau et de créer un nouveau centre opérationnel en Suisse. Cette réorganisation de l'architecture a consisté à régionaliser les opérations réalisées par SWIFT dans le cadre de ses services, y compris le service de *back up*. L'objectif consiste à ne plus traiter et archiver les messages échangés entre les clients européens de SWIFT que dans des centres opérationnels établis en Europe, à l'exclusion du centre basé aux Etats-Unis.

Par ailleurs, un *Privacy Officer* a été désigné, les procédures encadrant l'exercice de leurs droits par les personnes concernées ont été formalisées et les contrats liant SWIFT à ses utilisateurs et à ses clients ont été revus. Dans ces conditions, la procédure engagée le 23 mai 2007 par la Commission de la protection de la vie privée a été close le 9 décembre 2008[8]. Dans la perspective du présent rapport, il est intéressant de noter l'appréciation portée par la Commission de la protection de la vie privée dans sa décision :

« *Il ne semble pas contestable que* ***SWIFT était obligée de donner suite aux injonctions de l'US Department of the Treasury et ne pouvait matériellement s'y soustraire, notamment parce qu'un de ses deux centres de traitement et d'archivage (et les informations qui y sont physiquement conservées) est situé sur le territoire des Etats-Unis****. A tout le moins, il n'est pas critiquable que le conseil d'administration de SWIFT soit arrivé à cette conclusion après avoir manifesté ses objections et obtenu des garanties limitant l'exploitation des données transférées.* ***Il en aurait été manifestement autrement si, se prévalant des effets extraterritoriaux que le législateur américain a entendu donner aux dispositions légales appliquées, l'US Department of the Treasury avait enjoint SWIFT de communiquer des données physiquement conservées hors du territoire des Etats-Unis***[9]. »

1.1.2 Les révélations de Snowden (2013)

Edward Snowden est un lanceur d'alerte américain. Informaticien, ancien employé de la Central Intelligence Agency (CIA) et de la National Security Agency (NSA), il a révélé les détails de plusieurs programmes de surveillance de masse américains et britanniques. Les révélations d'Edward Snowden

[7] Les banques du Groupe des dix (G10) sont la Banque nationale de Belgique, la Banque du Canada, la Deutsche Bundesbank, la Banque centrale européenne, la Banque de France, la Banque d'Italie, la Banque du Japon, la Banque des Pays-Bas, la Sveriges Riksbank, la Banque nationale suisse, la Banque d'Angleterre et la Réserve fédérale des États-Unis, représentée par la Federal Reserve Bank of New York et le conseil des gouverneurs de la Réserve fédérale.

[8] Décision du 9 décembre 2008 de la Commission de la protection de la vie privée https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/swift_decision_09_12_2008.pdf

[9] Cf. Décision du 9 décembre 2008 de la Commission de la protection de la vie privée, §232

résultent de la divulgation d'un important volume de documents[10] progressivement rendus publics à partir du 6 juin 2013 à travers plusieurs titres de presse. Elles concernent la surveillance mondiale d'internet, mais aussi des téléphones portables et autres moyens de communications, principalement par la NSA. En 2013, 2014 et 2015, les révélations ont continué à faire connaître au grand public l'ampleur des renseignements collectés par les services secrets américains et britanniques.

Les documents divulgués par Snowden mettent très majoritairement en évidence l'espionnage de communications. Mais ils portent aussi sur l'espionnage de données de paiement. Un article du SPIEGEL[11] suggère que la National Security Agency a surveillé largement les paiements internationaux, les transactions bancaires et les transactions par carte de crédit. La NSA avait constitué une base de données appelée "Tracfin"[12], qui comportait 180 millions d'enregistrements en 2011. Environ 84 % des données provenaient de transactions par carte de crédit. L'objectif était de « *collecter, analyser et ingérer des données transactionnelles pour les associations de cartes de crédit prioritaires, en se concentrant sur les régions géographiques prioritaires, l'Europe, le Moyen-Orient et l'Afrique* ».

La banque de données Tracfin de la NSA était également alimentée par les données transitant par le réseau SWIFT, utilisé par des milliers de banques pour échanger en toute sécurité des informations sur les transactions. Un document cité par le SPIEGEL rapporte que, selon des employés de la NSA qui s'en inquiétaient, la collecte, le stockage et le partage de données politiquement sensibles constituaient une grave atteinte à la vie privée et impliquaient des données de masse comportant de riches informations personnelles, dont une grande partie ne concernait pas les cibles « officielles » de la NSA.

1.1.3 Les sanctions américaines en Crimée et en Russie (2014)

Des manifestations pro-européennes en Ukraine, à partir du 21 novembre 2013, ont fait suite à la décision du gouvernement ukrainien de ne pas signer un accord d'association avec l'Union européenne. Ces manifestations ont dégénéré en affrontements persistants jusqu'à la fuite le 22 février 2014 du président ukrainien, sa destitution et la mise en place d'un nouveau gouvernement. Un référendum tenu en République autonome de Crimée et dans la ville de Sébastopol le 16 mars 2014 a été déclaré invalide par une résolution[13] de l'Assemblée générale des Nations Unies le 27 mars 2014.

Le 4 juin 2014, un communiqué[14] des dirigeants du G7 a condamné « *la violation continue par la Fédération de Russie de la souveraineté et de l'intégrité territoriale de l'Ukraine* », en estimant que « *l'annexion illégale de la Crimée par la Russie et les actions de déstabilisation de l'est de l'Ukraine étaient inacceptables et devaient cesser* ». Il a exhorté la Fédération de Russie « *à achever le retrait de ses forces militaires à la frontière avec l'Ukraine, à arrêter le flux d'armes et de militants à travers la frontière et à exercer son influence parmi les séparatistes armés pour déposer leurs armes et renoncer à la violence* ».

---

[10] cf. par exemple le recensement « *Snowden Revelations* », Lawfare
https://www.lawfareblog.com/snowden-revelations

[11] « *NSA Spies on International Payments* », SPIEGEL International, 15 septembre 2013
https://www.spiegel.de/international/world/spiegel-exclusive-nsa-spies-on-international-bank-transactions-a-922276.html

[12] Sans rapport, naturellement, avec l'organisme du ministère de l'Économie et des Finances, chargé de la lutte contre la fraude, le blanchiment d'argent et le financement du terrorisme, Tracfin (acronyme de « *Traitement du renseignement et action contre les circuits financiers clandestins* »)

[13] « *Résolution adoptée par l'Assemblée générale le 27 mars 2014, 68/262. Intégrité territoriale de l'Ukraine* »
https://undocs.org/pdf?symbol=fr/A/RES/68/262

[14] Communiqué des dirigeants du G7, 4 juin 2014
https://ec.europa.eu/commission/presscorner/detail/en/IP_14_637

Dès le mois de mars 2014, les Etats-Unis et l'Union européenne ont imposé des sanctions[15] à l'encontre des personnes et des entités qui ont pris une part active à la violation de la souveraineté et de l'intégrité territoriale de l'Ukraine, ou qui menaçaient la paix, la sécurité et la stabilité de cet Etat. Le gouvernement américain a notamment imposé des sanctions sectorielles contre les plus grandes banques d'État russes. Ces sanctions ont restreint la capacité des sociétés basées aux États-Unis, telles que Visa et MasterCard, à fournir des services à certains particuliers et entreprises russes.

Visa et Mastercard ont appliqué les sanctions occidentales contre la Russie en cessant de fournir leurs services aux clients de sept banques russes en mars 2014[16], lesquelles étaient liées à des personnalités russes visées par les sanctions occidentales. En outre, Visa a annoncé le 26 décembre 2014 qu'elle devait cesser ses activités en Crimée, du fait de nouvelles sanctions prises une semaine plus tôt par les États-Unis : « *il est désormais interdit à Visa d'offrir des produits et des services de marque Visa en Crimée. Cela signifie que nous ne pouvons plus prendre en charge les services d'émission de cartes et d'acquisition de paiement en Crimée* »[17].

1.1.4 La panne d'Amazon en 2017

Les origines de l'activité de prestataire de services *cloud* d'Amazon remontent à 2003[18]. L'entreprise est alors en train de passer du statut de libraire en ligne à celui de distributeur multiproduit. Le groupe commence à construire ses propres *datacenters* et à développer ses propres logiciels, car ceux disponibles sur le marché ne suffisent pas à répondre à ses besoins de rapidité et de flexibilité. L'idée de rentabiliser les investissements et de partager les outils avec d'autres entreprises a été rendue possible par internet et les communications à haut débit. Le stockage et le traitement des données sont mis en œuvre sur des serveurs partagés entre plusieurs utilisateurs, facturés en fonction du temps de traitement et des volumes de données utilisés : c'est le concept de *cloud* public.

Amazon Web Services, lancé en 2006, s'est développé de façon spectaculaire, au point de représenter aujourd'hui le principal centre de profit du groupe. Les services informatiques se sont diversifiés bien au-delà du simple stockage de données, notamment vers la mise à disposition d'algorithmes d'intelligence artificielle (qu'Amazon utilise non seulement pour optimiser l'utilisation de ses serveurs informatiques, mais aussi pour ses besoins propres de gestion des stocks, de publicité personnalisée et de profilage de sa clientèle, de détection de la contrefaçon et de la fraude…). Aujourd'hui, 20 % de l'informatique d'entreprise serait dans le *cloud* et Amazon représente 48 % d'un marché de 32,4 milliards de dollars (cf. Le marché du cloud, chapitre 2.6.1.1 p. 67). Engie, Netflix, Airbus, Goldman Sachs, Veolia, AXA, Unilever, General Electric, Deloitte, la Securities Exchange Commission ou la CIA sont des exemples de clients d'AWS.

C'est dire les enjeux économiques d'une panne telle que celle qui est intervenue pendant quatre heures[19] le 28 février 2017 sur une partie du territoire américain à la suite d'une erreur humaine (« *un*

---

[15] S'agissant des Etats-Unis : Executive Order 13660 of March 6, 2014, Executive Order 13661 of March 16, 2014, Executive Order 13662 of March 20, 2014, Executive Order 13685 of December 19, 2014

[16] « *Mastercard et Visa dans le viseur de Poutine* », France 24, 27 mars 2014 https://www.france24.com/fr/20140327-mastercard-visa-poutine-systeme-paiement-russie-ukraine-sanction-crimee-unipay-carte-credit

[17] "*Visa says can't support bank cards in Crimea due to U.S. sanctions*", Reuters, December 26, 2014 https://www.reuters.com/article/russia-crisis-visa-crimea/visa-says-cant-support-bank-cards-in-crimea-due-to-u-s-sanctions-idUSL6N0UA0UX20141226

[18] « *AWS, le nuage en or d'Amazon* », les Echos, 2 janvier 2020 https://www.lesechos.fr/idees-debats/editos-analyses/aws-le-nuage-en-or-damazon-1159890

[19] "*AWS's S3 outage was so bad Amazon couldn't get into its own dashboard to warn the world*", the Register; "*How a typo took down S3, the backbone of the internet*", the Verge ; **«** *Une panne du cloud d'Amazon a impacté une centaine de milliers de sites web* », les Echos**, 1er** et 2 mars 2017 https://www.theregister.co.uk/2017/03/01/aws_s3_outage/

membre autorisé de l'équipe S3 utilisant un playbook établi a exécuté une commande destinée à supprimer un petit nombre de serveurs pour l'un des sous-systèmes S3 utilisé par le processus de facturation S3. Malheureusement, l'une des entrées de la commande a été entrée incorrectement et un ensemble de serveurs plus important a été supprimé que prévu... »)[20], ce qui a impacté plus d'une centaine de milliers de sites *web*.

L'intérêt de cet incident n'est pas de mettre en cause la fiabilité des services de tel ou tel prestataire, mais de mettre en lumière les effets possiblement systémiques d'une panne, toujours possible, affectant un acteur représentant une part de marché très importante sur une activité critique pour l'économie. La difficulté pour des autorités nationales d'imposer une obligation de résilience à l'égard de services essentiels, de prendre la mesure d'une crise quand elle advient, de décider d'éventuelles mesures d'urgence… serait certainement accrue dans le cas d'un acteur dont les centres de décision sont à l'étranger.

1.1.5 L'affaire USA v. Microsoft Corporation (2017 - 2018)[21]

La loi fédérale américaine *Electronic Communications Privacy Act* de 1986, dans son titre II (*Stored Communications Act* ou *SCA*), protège les communications confiées à des fournisseurs de courrier électronique contre des menaces telles qu'un accès non autorisé par des pirates informatiques et des employés voyous, la divulgation volontaire d'informations par un fournisseur de services, les perquisitions et les saisies gouvernementales non autorisées.

Elle régit les conditions dans lesquelles les autorités de police peuvent légalement accéder au contenu des messages : la section 2703 leur permet, sous réserve de la délivrance d'un mandat par le tribunal compétent, d'exiger d'un fournisseur de services de communications le détail des messages. A cet effet, les autorités de police doivent caractériser avec précision les messages en cause et convaincre le tribunal qu'ils peuvent contribuer à élucider un crime.

En décembre 2013, des agents fédéraux ont obtenu du tribunal du district sud de l'État de New York un mandat relatif à la section 2703 obligeant Microsoft à communiquer tous les courriels stockés dans le compte de messagerie de l'un de ses clients, soupçonné de se livrer au trafic de drogue, dans la mesure où ces informations *« sont sous la possession, la garde ou le contrôle de* [Microsoft] ». Or les messages électroniques faisant l'objet du mandat étaient stockés dans un emplacement unique : un centre de données situé à Dublin, en Irlande, où les messages sont protégés par les lois irlandaise et européenne de protection des données personnelles.

Microsoft expose ainsi ses procédures[22] : en cas d'ordre licite des autorités américaines, un employé de Microsoft détermine l'emplacement du centre de données où les messages sont stockés. Pour la correspondance stockée aux États-Unis, l'employé copie les courriels du serveur national et les transmet aux autorités américaines, comme l'exige le mandat. Mais quand les autorités américaines veulent accéder à des emails stockés à Dublin, Microsoft les renvoie à l'application du Traité d'entraide

---

https://www.theverge.com/2017/3/2/14792442/amazon-s3-outage-cause-typo-internet-server
https://www.lesechos.fr/2017/03/une-panne-du-cloud-damazon-a-impacte-une-centaine-de-milliers-de-sites-web-163325

[20] « *Summary of the Amazon S3 Service Disruption in the Northern Virginia (US-EAST-1) Region* », communiqué d'Amazon du 1er mars 2017
https://aws.amazon.com/fr/message/41926/

[21] Ce chapitre repose sur l'exploitation des pièces d'instruction de la procédure engagée devant la Cour Suprême des Etats-Unis, disponibles à l'adresse web ci-dessous. Ces pièces ne comportent, à côté des mémoires des parties, un ensemble instructif de contributions émanant notamment de la Commission Européenne, de l'Irlande et du Royaume-Uni, en tant *qu'amicus curiae*
https://www.supremecourt.gov/search.aspx?filename=/docket/docketfiles/html/public/17-2.html

[22] USA v. Microsoft Corporation, brief for respondent, Jan 11, 2018

judiciaire États-Unis-Irlande (*mutual legal assistance treaty* ou *MLAT*), qui permet au gouvernement américain d'obtenir des courriers électroniques par l'intermédiaire du Ministère irlandais de la justice.

Dans un mémoire en tant qu'*amicus curiae*[23], l'Irlande prend acte de ce que le mandat discuté devant la Cour Suprême ordonne à Microsoft de produire aux États-Unis des documents qui, selon la société, sont situés en Irlande. Elle soutient que les tribunaux étrangers sont tenus de respecter la souveraineté irlandaise (et celle de tous les autres États souverains), que l'Irlande soit ou non partie à la procédure. L'Irlande rappelle sa coopération avec d'autres États, y compris les États-Unis, dans la lutte contre le crime et affirme que le Traité d'entraide judiciaire entre le gouvernement de l'Irlande et le gouvernement des États-Unis conclu le 18 janvier 2001 représente le moyen approprié pour traiter la demande des autorités de police américaines objet du litige.

Au contraire le Royaume-Uni[24] considère qu'une loi qui tiendrait compte de critères de localisation des données pour autoriser les autorités à y accéder serait inefficace. Les autorités de police, si elles en ont le mandat, devraient pouvoir accéder aux communications électroniques concernant les citoyens de leur juridiction, où que ces communications soient stockées. Une demande de communications électroniques stockées à l'étranger par un fournisseur, mais accessible dans le pays demandeur, ne devrait pas entraîner l'exercice d'une compétence extraterritoriale. Le Royaume-Uni envisage un accord avec les États-Unis dans lequel les autorités de police de chacun des deux Etats pourraient accéder aux communications détenues par les fournisseurs situés dans la juridiction de l'autre Etat. Cet accès réciproque porterait ses effets quel que soit le lieu où les communications recherchées sont effectivement stockées.

La Commission européenne, en tant qu'*amicus curiae*[25], a exposé les grandes lignes du RGPD[26], qui était à cette date publié mais pas encore applicable. Elle présente l'article 48 du RGPD qui énonce qu'une « *décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant d'un responsable du traitement ou d'un sous-traitant qu'il transfère ou divulgue des données à caractère personnel ne peut être reconnue ou rendue exécutoire de quelque manière que ce soit qu'à la condition qu'elle soit fondée sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un État membre, sans préjudice d'autres motifs de transfert en vertu du présent chapitre* ».

Si, en vertu de cet article, une décision de justice étrangère qui ne serait pas fondée sur un accord international ne justifie pas un transfert de données personnelles, la Commission a laissé entendre, ce qui est discutable[27], que l'article 49 (« *dérogations pour des situations particulières* ») pourrait néanmoins permettre un tel transfert dans des cas où celui-ci serait « *nécessaire pour des motifs importants d'intérêt public* » ou « *nécessaire aux fins des intérêts légitimes impérieux poursuivis par le responsable du traitement sur lesquels ne prévalent pas les intérêts ou les droits et libertés de la personne concernée* ».

---

[23] USA v. Microsoft Corporation, brief of Ireland as *amicus curiae* in support of neither party, Dec 13, 2017

[24] USA v. Microsoft Corporation, brief of the government of United Kingdom of Great Britain and Northen Ireland as *amicus curiae* in support of neither party, Dec 13, 2017

[25] USA v. Microsoft Corporation, brief of the European Commission on behalf of the European Union as *amicus curiae* in support of neither party, Dec 13, 2017

[26] Règlement 2016/679 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

[27] Cf. lettre du 10 juillet 2019 de l'European Data Protection Board (Subject: LIBE Committee letters to the EDPS and the EDPB regarding legal assessment of the impact of the US Cloud Act on the European legal framework for personal data protection) : "*We are of the view that currently, unless a US CLOUD Act warrant is recognised or made enforceable on the basis of an international agreement, the lawfulness of such transfers of personal data cannot be ascertained, without prejudice to exceptional circumstances where processing is necessary in order to protect the vital interests of the data subject…*"
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_edps_joint_response_us_cloudact_coverletter.pdf

Le litige entre le gouvernement des Etats-Unis et Microsoft s'est prolongé pendant plusieurs années, sans que jamais les autorités de police adoptent la voie de l'entraide judiciaire. Alors que depuis le 27 juin 2017 l'affaire était soumise à l'avis de la Cour Suprême, le Congrès est intervenu : le 23 mars 2018 était promulguée la loi *Clarifying Lawful Overseas Use of Data Act* (*CLOUD Act*).

Le *CLOUD Act* modifie le *Stored Communications Act* en ajoutant la disposition suivante : « *Un [fournisseur de services] doit respecter les obligations du présent chapitre concernant la conservation, la sauvegarde ou la divulgation du contenu d'une communication filaire ou électronique, ainsi que de tout enregistrement ou autre information concernant un client ou un abonné en sa possession, sa garde ou son contrôle, que cette communication, enregistrement ou autre information soit située aux États-Unis ou à l'extérieur* ». La procédure engagée devant la Cour Suprême est devenue sans objet[28] et Microsoft s'est conformé au *CLOUD Act*.

Toutefois, le *Stored Communications Act* tel que modifié par le *CLOUD Act* ne donne pas carte blanche aux autorités américaines pour accéder à l'ensemble des données confiées aux fournisseurs de services de communication, traitement et stockage électroniques de données placés sous la juridiction des Etats-Unis. Les autorités américaines ne peuvent requérir la communication de données que dans le cadre de procédures judiciaires, si elles peuvent justifier d'une présomption sérieuse que la personne concernée a commis ou est sur le point de commettre une infraction pénale.[29]

Il convient de noter que le Conseil européen a adopté le 6 juin 2019 un mandat autorisant la Commission à négocier au nom de l'Union européenne un accord avec les États-Unis afin de faciliter l'accès aux preuves électroniques à des fins de coopération judiciaire en matière pénale. L'objectif serait de faciliter l'accès aux preuves électroniques, comme les courriels ou les documents stockés dans le *cloud*, pour les utiliser dans le cadre de procédures pénales.[30]

1.1.6 L'affaire Cambridge Analytica (2018)

La collecte illicite de données personnelles par la société Cambridge Analytica a été signalée pour la première fois en décembre 2015 par le Guardian[31]. Il était révélé qu'une société d'analyse de données peu connue du public a eu recours à des chercheurs de l'Université de Cambridge pour collecter, à très grande échelle et sans leur consentement, les données Facebook des électeurs américains, puis de les exploiter dans le but d'influencer leur vote.

L'utilisation des données des médias sociaux pour modéliser le comportement humain est issue d'un projet de recherche mené dès 2014 à l'Université de Cambridge. Un large échantillon d'utilisateurs de Facebook a été sollicité pour répondre à un questionnaire de personnalité et pour donner accès à leur profil Facebook. Des dizaines de milliers de données démographiques d'individus – noms, lieux, anniversaires, genres – ainsi que leurs *likes* Facebook et leurs messages, qui exposent leurs idées personnelles. Surtout, les contacts Facebook de ces individus ont donné lieu, sans leur consentement, à la même collecte, de sorte que la taille de la base de données a pu croître exponentiellement.

Les données Facebook ont donné lieu à des analyses psychologiques approfondies permettant de distinguer différents types de personnalités. Une exploitation commerciale de ce modèle a été entreprise, la société Global Science Research (GSR), liée à Cambridge Analytica, se targuant à l'été

---

[28] USA v. Microsoft Corporation, opinion, April 17, 2018

[29] « *Faut-il avoir peur du Cloud Act ?* », Emmanuelle Mignon, August Debouzy Avocats, 29 juin 2018 https://www.august-debouzy.com/fr/blog/1193-faut-il-avoir-peur-du-cloud-act

[30] « *Le Conseil donne mandat à la Commission pour négocier des accords internationaux concernant les preuves électroniques en matière pénale* », Communiqué du Conseil de l'UE, 6 juin 2019 https://www.consilium.europa.eu/fr/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/

[31] "*Ted Cruz using firm that harvested data on millions of unwitting Facebook users*", the Guardian, December 11, 2015 https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data

2014 de posséder « *un énorme pool de données de plus de 40 millions de personnes aux États-Unis – pour chacune desquelles nous avons généré des profils de caractéristiques et de traits détaillés* ». Cambridge Analytica s'est développée en permettant aux hommes politiques américains d'élaborer des messages de campagne ciblés sur des questions très spécifiques et de communiquer de différentes manières à différents publics en fonction des informations personnelles que la société détient à leur sujet : « *plus vous en savez sur quelqu'un, plus vous pouvez aligner une campagne sur ses exigences, ses désirs ou ses besoins* ».

C'est en mars 2018 que le scandale a éclaté, à partir du témoignage – saisissant – d'un lanceur d'alerte[32]. Selon lui, plus de 50 millions de profils, représentant environ un tiers des utilisateurs actifs de Facebook en Amérique du Nord et près d'un quart des électeurs potentiels aux États-Unis, ont été réunis dans l'une des plus importantes violations de données jamais enregistrées. « *Nous avons exploité Facebook pour récolter des millions de profils de personnes. Et construit des modèles pour exploiter ce que nous savions d'eux et cibler leurs démons intérieurs. C'est sur cette base que l'ensemble de l'entreprise s'est construit* ».

Le but explicite de Cambridge Analytica consistait à influencer les électeurs : « *Si vous voulez changer de politique, il faut d'abord changer la culture, parce que la politique découle de la culture. Et si vous voulez changer la culture, il faut en premier lieu comprendre ce qu'est la culture à l'échelle individuelle : les gens, qui sont l'échelon élémentaire de la culture. Donc si vous voulez changer la politique, il faut changer les gens, pour changer la culture* ».

La nature, le ton, la fréquence des messages susceptibles de faire évoluer l'opinion des électeurs en fonction de leur profil étaient déterminés. « *A côté des analystes de données, des psychologues et des stratèges, ils avaient des équipes entières de créateurs, de designers, de vidéographes, de photographes… qui créaient des contenus. Les contenus étaient ensuite transmis à des équipes de ciblage qui les injectaient sur internet. On créait des sites web, des blogs… tout ce à quoi le profil ciblé nous semblait réceptif* ».

L'affaire Cambridge Analytica a été décrite comme un tournant décisif dans la compréhension par le public des enjeux de données personnelles. Elle met en évidence la relative facilité et la modestie des investissements requis (en l'espèce, de l'ordre d'un million de dollar au départ) pour exploiter et monnayer de larges bases de données personnelles trop facilement accessibles. De manière comparable, des données de paiement seraient, à l'évidence, propices à une exploitation marchande et à des stratégies d'influence.

1.1.7 Les enseignements et les recommandations du rapport Gauvain (2019)

Le député Raphaël Gauvain a été nommé parlementaire en mission et chargé le 11 juillet 2018 d'une mission portant sur les mesures de protection des entreprises françaises confrontées à des procédures judiciaires ou administratives donnant effet à des législations de portée extraterritoriale. Son rapport[33] documente précisément les menaces et le mode opératoire selon lequel s'appliquent les législations extraterritoriales d'origine américaine.

La force des lois américaines relatives aux infractions économiques et financières réside dans l'introduction de critères de compétence aux contours flous et dans l'interprétation extrêmement large de ces critères. L'existence d'un lien de rattachement entre une infraction et le territoire des États-Unis n'est généralement pas défini par la loi et les autorités américaines peuvent l'interpréter de

---

[32] "*Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*", the Guardian, March 17, 2018
https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

[33] « *Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et mesures à portée extraterritoriale* », R. Gauvain, Rapport au Premier Ministre, 26 juin 2019
https://www.vie-publique.fr/rapport/38473-proteger-nos-entreprises-des-lois-et-mesures-portee-extraterritoriale

manières variées, au gré des circonstances de l'affaire ; et même lorsque le lien de rattachement est précis dans la loi, il est interprété de manière large par les autorités américaines.

Les autorités de poursuite américaines, notamment le Département de la Justice (DoJ), ne sont pas indépendantes : il existe une grande proximité aux États-Unis entre les milieux économiques et les autorités fédérales ; elle est accentuée dans le cas du DoJ par de nombreuses passerelles entre le monde des entreprises, les *private practice*, le monde politique, les services de renseignement et l'appareil judiciaire.

Le DoJ est une autorité administrative et non juridictionnelle, qui conduit des enquêtes dans le cadre de procédures transactionnelles. Le DoJ initie systématiquement ses procédures par une négociation « informelle » avec la partie mise en cause, hors de tout cadre procédural et de tout contrôle judiciaire, sans garantie en matière de protection des droits de la défense.

Cette négociation a pour but d'aboutir à un accord, dans lequel l'entreprise va reconnaître un certain nombre de faits (relatifs à la corruption d'agents publics étrangers, au blanchiment d'argent ou au financement du terrorisme, à la violation de sanctions internationales ou de règles fiscales applicables aux citoyens américains non-résidents…), payer une lourde amende aux autorités de poursuites concernées en échange d'un arrêt ou d'un abandon pur et simple des poursuites.

L'un des arguments déployés par le DoJ lors de ces discussions informelles est la peur du juge et d'un jugement définitif en cas de procédure judiciaire, au motif que celle-ci serait plus longue et plus coûteuse *in fine* pour l'entreprise concernée. La discussion informelle se déroule à la marge du cadre juridique normal. Il s'agit d'un « *rapport de force violent et déséquilibré* » entre les autorités américaines et l'entreprise, dont la survie peut dépendre de son accès au marché américain. Ce cadre informel conduit souvent les entreprises à renoncer tant à faire valoir leurs droits, qu'à respecter leurs obligations éventuelles au regard de la législation de leur pays d'origine.

Les procédures de recueil des éléments de preuve, en matière pénale, mais aussi en matière civile et commerciale (procédure de *discovery*), aboutissent à une véritable injonction de communiquer pesant sur les personnes mises en cause au pénal, comme sur les parties à un litige civil ou commercial, quel que soit le lieu où se situent les éléments communiqués. Les preuves transmises par les intéressés sont ainsi transférées sur le territoire américain par les personnes mises en cause et les parties, en dehors des mécanismes d'entraide judiciaire et sans aucun contrôle par les autorités étrangères concernées. Des volumes considérables de données peuvent ainsi être transmis aux autorités américaines

Si une transaction aboutit, l'entreprise s'engage à payer une importante amende, voire à mettre en œuvre un processus de mise en conformité, sous le contrôle d'un moniteur. Elle renonce à se prévaloir de la prescription et à contester les décisions du gouvernement si ce dernier estimait que l'entreprise n'a pas respecté ses engagements ; pour sa part, le procureur renonce à poursuivre l'intéressé ou suspend les poursuites, en l'attente de l'accomplissement des obligations résultant de la transaction pénale. A aucun moment de cette procédure un juge ne se prononce sur la compétence des autorités de poursuite, sur la constitution des infractions en cause ou encore sur la régularité de la procédure.

Les accords transactionnels conduisent souvent les entreprises à accepter l'installation en leur sein d'une équipe d'auditeurs mandatés par l'autorité américaine et à qui elle rapporte directement. Elle aura accès à toute l'activité et à tous les secrets de l'entreprise pendant la durée de son mandat et elle rendra compte de l'action de l'entreprise à intervalles réguliers.

1.2 Différentes formes d'atteintes à la souveraineté

Les paiements domestiques en France se sont longtemps appuyés sur des infrastructures contrôlées par les banques, telles que le GIE Carte Bancaire, qui traite encore aujourd'hui la très grande majorité des transactions entre un consommateur français et un commerçant français. L'entrée en vigueur du règlement 2015/751, dit règlement interchange (cf. note 53 p. 32 et chapitre 2.2.2 p. 35), a invalidé les règles de partage, telles qu'elles existaient en France, entre un *scheme* domestique et les *schemes* internationaux. Il a progressivement créé entre eux, un certain niveau de concurrence. Il n'a

malheureusement pas conduit à des stratégies d'alliance des *schemes* domestiques ou d'internationalisation de leurs activités en Europe. Certains Etats de l'Union européenne n'ont pas de *scheme* domestique et s'appuient largement sur des acteurs internationaux.

La réalisation d'une opération de paiement en Europe dépend ainsi de plus en plus souvent de la participation d'acteurs tiers (Visa, MasterCard, Apple Pay, etc…), dont les centres de décision sont souvent établis en dehors de la juridiction de l'Union européenne. Cette situation présente potentiellement plusieurs risques d'atteinte à la souveraineté européenne.

1.2.1 Risque politique

Le recours d'une forte proportion des acteurs du paiement à un ou plusieurs prestataires de service qui opèreraient depuis un même pays extra-européen pourrait induire une situation de paralysie, si ce ou ces prestataires étaient enjoints par leur gouvernement de suspendre leurs services.

1.2.2 Risque de soumission des ressortissants européens à des autorités étrangères

Un opérateur extra-européen pourrait accorder des droits à la justice d'un pays tiers sur des données de paiement appartenant à des ressortissant européens, en-dehors des règles de droit international et des traités d'entraide judiciaire.

1.2.3 Risque d'espionnage

Un opérateur extra-européen pourrait ne pas assurer une protection adéquate aux données de paiement de ses clients européens, vis-à-vis notamment des services de renseignements du pays dans lequel il opère.

1.2.4 Risque d'utilisation des données personnelles à des fins commerciales

Un opérateur extra-européen pourrait exploiter les données de paiement de ses clients européens à des fins commerciales, en contravention avec le RGPD, ou faire preuve d'une moindre exigence de conformité à l'égard des règles du RGPD, en tirant parti de ce que son extranéité rend le contrôle et la sanction d'éventuels manquements plus difficiles à assurer.

1.2.5 Risque économique

Un opérateur extra-européen bénéficiant d'un fort pouvoir de marché pourrait abuser de sa position dominante et écarter ses concurrents locaux par des moyens déloyaux, par exemple en cassant les prix, pour ensuite renchérir significativement le coût de ses prestations – et donc le coût des paiements en Europe.

1.2.6 Risque de gouvernance des systèmes des paiements internationaux

L'absence d'acteurs européens dans les instances de fixation des standards internationaux de paiement pourrait conduire à défavoriser les acteurs européens.

1.2.7 Risque d'affaiblissement de la capacité d'enquête des autorités de police et de justice européennes

Un opérateur extra-européen pourrait ne pas répondre aux réquisitions d'une autorité judiciaire européenne portant sur des données critiques de paiement, alors que l'émetteur et/ou le bénéficiaire de ces paiements sont dans le ressort de cette juridiction européenne.

2 LES PISTES DE PRESERVATION DE L'INDEPENDANCE EUROPEENNE EN MATIERE DE PAIEMENT

2.1 Il existe un assez large consensus en faveur d'une localisation en Europe des données de paiement

2.1.1 La criticité des données de paiement au regard des enjeux de souveraineté

Pour assurer l'indépendance du marché et des acteurs européens dans le domaine du paiement, la stratégie nationale des moyens de paiement scripturaux met en avant l'intérêt de cantonner sur le territoire de l'Union européenne le traitement des données critiques relatives au paiement ; mais la stratégie s'abstient d'expliciter cette **notion de données critiques de paiement**. Il s'agit ici d'apporter quelques éléments de réflexion à cet égard.

Indiquons d'emblée que les données de paiement, dans la mesure où elles se rattachent à des personnes physiques européennes, sont placées sous les règles générales de protection des données à caractère personnel prévue par le RGPD[34] ; mais que si ce texte prévoit des obligations renforcées à l'égard de certaines catégories particulières de données à caractère personnel, dites sensibles[35], ce n'est pas le cas des données de paiement en tant que telles (sauf à considérer qu'elles sont toujours susceptibles de révéler, par le biais du paiement d'une cotisation comportant un intitulé explicite, un engagement syndical ou religieux).

Les développements qui suivent ont vocation à s'appliquer à l'ensemble des moyens de paiement et à l'ensemble des cas d'usage de paiement de détail. Mais au risque de restreindre la généralité du propos et par commodité de langage, on se réfèrera principalement dans la suite à la situation où l'émetteur d'un paiement est une personne physique agissant dans le cadre d'un achat privé (un « consommateur ») et où le bénéficiaire peut être désigné par le vocable de « commerçant ».

2.1.1.1 Les données propres à un instrument de paiement sont protégées par la DSP2

La deuxième directive sur les services de paiement (DSP2) définit les « *données de sécurité personnalisées* » : ce sont les données personnalisées fournies à un utilisateur de services de paiement à des fins d'authentification. Elle définit également les « *données de paiement sensibles* » qui sont, de manière plus large, les données susceptibles d'être utilisées pour commettre une fraude.

Un prestataire de services de paiement doit s'assurer que les données de sécurité personnalisées ne sont pas divulguées à des tiers ; la description du processus qu'il met en place pour enregistrer, surveiller et restreindre l'accès aux données de paiement sensibles et garder la trace de ces accès constitue l'une des conditions de son agrément.

Ces données de paiement sensibles, au premier rang desquelles les données de sécurité personnalisées, servent notamment à identifier les comptes (IBAN) ou les moyens de paiement (PAN pour les cartes) des parties engagées dans une transaction, ainsi que les prestataires de service de paiement impliqués dans les transactions (Bank Identifier Code, BIC). Elles soulèvent d'importants enjeux de sécurité et sont au cœur du dispositif de contrôle interne des établissements régulés.

---

[34] Règlement 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 (RGPD), https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679

[35] Article 9 : « *le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique* »

Pour autant, il ne semble pas que ces données d'identification soulèvent, au-delà d'importants enjeux de sécurité, des enjeux de souveraineté justifiant qu'on exige leur cantonnement sur le territoire européen. En particulier, les instruments de paiement utilisés en Europe doivent pouvoir être utilisés hors d'Europe, notamment dans le cas du commerce en ligne, ce qui suppose que les identifiants de paiement des consommateurs européens puissent être utilisés, lorsqu'ils le souhaitent, par des commerçants extra-européens. Il n'est évidemment pas question de restreindre la liberté d'utiliser à travers le monde un instrument de paiement tel qu'une carte bancaire internationale.

2.1.1.2 Les données qui soulèvent des enjeux de souveraineté sont celles qui ont trait aux transactions de paiement

La compréhension par un commerçant des habitudes de consommation de ses clients est un levier évident d'amélioration de ses ventes. L'analyse de ces habitudes suppose qu'il sache faire le lien entre différents achats, intervenant à des dates différentes, éventuellement dans des points de vente différents de la même enseigne.

Dans le cas du commerce traditionnel, une carte de fidélité peut servir à établir le lien ; dans le cas du e-commerce, le consommateur accepte souvent de s'identifier à travers la création d'un compte comportant son nom et son adresse de livraison. Dans les deux cas, un identifiant commun (numéro de carte de fidélité, numéro de client…) permet d'analyser des historiques de consommations de plusieurs années.

Mais les caractéristiques d'un instrument de paiement, telles qu'un numéro de compte bancaire ou de carte de paiement, permettent plus efficacement encore qu'un numéro de carte de fidélité ou un numéro de client de relier entre eux les achats d'un même consommateur. L'analyse des transactions de paiement peut devenir par elle-même une activité marchande : la référence à un instrument de paiement permet à deux commerçants d'échanger des informations sur les habitudes de leurs clients mutuels et facilite les ventes croisées.

A une plus grande échelle, un acteur important de la chaîne des paiements, tel qu'une plateforme d'achat, dispose d'une masse de données qui lui procure une certaine capacité à prédire et à influencer les actes d'achat. S'il procède à une exploitation commerciale des données de paiement et s'il apporte son expertise à certains commerçants plutôt qu'à d'autres, il peut affecter notablement, positivement ou négativement, les ventes des uns et des autres.

C'est la présence des caractéristiques de l'instrument de paiement (les données de sécurité personnalisées) qui confère à une base de données client une sensibilité particulière, dans la mesure où elle permet de croiser et d'enrichir les données relatives aux mêmes clients chez plusieurs commerçants ; elle permet d'établir des « *patterns* » ou des habitudes de consommation, que celles-ci soient propres à un consommateur nommément identifiable ou propres à des familles homogènes de consommateurs sensibles aux mêmes envies et aux mêmes sollicitations commerciales.

La mission n'a pas su faire ressortir un critère de distinction, parmi les données liées à une transaction, entre celles qui devraient être intrinsèquement regardées comme « critiques » et d'autres qui seraient par nature anodines. Elle estime au contraire que, dès lors qu'une base de données clients inclut les caractéristiques d'un instrument de paiement, l'ensemble des données de cette base devraient être regardées comme méritant une protection particulière.

> **Dans le présent rapport donc, on entend dorénavant par données de paiement l'ensemble des données attachées à une transaction de paiement, dès lors que ces données demeurent liées directement ou indirectement à une personne physique, par l'intermédiaire d'un identifiant de compte, de carte ou de tout autre instrument de paiement, que cet identifiant figure en clair ou qu'il soit masqué par un**

pseudonyme[36]. Selon les cas, les données de paiement peuvent être plus ou moins nombreuses et plus ou moins variées. Elles peuvent par exemple comporter les coordonnées du commerçant, un horodatage, la géolocalisation, l'adresse IP du consommateur, éventuellement le détail des achats… Les données de paiement ainsi entendues constituent des données à caractère personnel au sens du RGPD[37].

A titre d'illustration, dans le cas d'un paiement par carte, plusieurs étapes du traitement donnent lieu à de tels flux de données de paiement : l'authentification du consommateur, l'autorisation du paiement, le règlement et la compensation du montant (cf. ci-dessous, chapitre 2.2.1 p. 33).

2.1.1.3 Des règles de localisation ne doivent s'appliquer que si à la fois l'émetteur et le bénéficiaire d'un paiement sont localisés en Europe

Une règle imposant la localisation en Europe des données de paiement porterait atteinte à la souveraineté d'un pays tiers si elle prétendait s'appliquer à des situations où soit l'émetteur du paiement, soit le bénéficiaire est localisé dans ce pays. Par ailleurs, l'immense majorité des paiements de détail intervenant en Europe (probablement plus de 95 %) sont intra-européens, c'est-à-dire qu'à la fois l'émetteur et le bénéficiaire du paiement sont localisés en Europe. Pour ces deux raisons, l'obligation de localisation des données de paiement envisagée dans le présent rapport devrait s'appliquer aux seules transactions de paiement intra-européennes.

L'institution d'une règle de localisation des données de paiement nécessiterait de lever toute ambiguïté sur le champ de cette mesure : elle devrait probablement porter sur toutes les monnaies de l'Union européenne et non sur les seules transactions en euros. La règle de localisation pourrait être étendue aux transactions de paiement impliquant l'Islande, la Norvège ou le Liechtenstein, membres de l'espace économique européen (EEE) mais pas de l'Union européenne. Dans ce cas, la localisation de données de paiements intra-européennes dans l'un de ces trois pays serait admise. Enfin, l'attention de la mission a été attirée sur la question d'une extension à la Suisse du périmètre de localisation des données de paiement.

2.1.1.4 Les paiements au bénéfice d'une personne physique semblent éligibles aux mêmes règles de localisation que les paiements qu'elle émet

La situation où une personne physique localisée en Europe n'est pas l'émettrice d'un paiement, mais en est le bénéficiaire (par exemple dans le cas d'un paiement de personne à personne, d'un versement de salaire, du règlement d'une pension de retraite ou d'une prestation sociale…) n'a pas été spécifiquement abordé au cours des entretiens menés par la mission.

Toutefois, il ne lui semble pas exister d'inconvénient ou de difficulté majeure à assimiler cette situation à la précédente : si l'émetteur d'un paiement est localisé en Europe, les données qui se rattacheraient directement ou indirectement à ce paiement par l'intermédiaire d'une donnée de sécurité personnalisée seraient obligatoirement localisées en Europe. Cette obligation s'appliquerait par exemple à un prestataire de services extra-européen spécialisé dans la confection et l'édition des bulletins de paye.

En revanche, la mission n'a pas du tout expertisé la question des paiements de personne morale à personne morale, typiquement de PME à PME. Les entretiens menés ne permettent ni d'éclairer cette question, ni d'écarter la possibilité d'enjeux spécifiques qui resteraient à élucider. En outre, la mission considère qu'il y a beaucoup d'avantages à considérer qu'une obligation de localisation des données

[36] Cf. Les différents cas d'utilisation de la tokenisation, chapitre 2.3.1, p. 44 et suivantes

[37] Cf. Quelques rappels sur le RGPD, chapitre 2.5.1, p. 59 et suivantes

de paiement vienne en complément des règles du RGPD, avec le même champ d'application et sous le contrôle des CNIL européennes.

2.1.2 Des exemples étrangers (Inde, Indonésie, Turquie…) plus ou moins probants, des objections, mais pas d'inconvénient insurmontable

2.1.2.1 Un grand nombre d'exemples étrangers

Selon une publication[38] de mars 2019 de l'Institute of International Finance[39], les restrictions à la circulation des données à travers les frontières nationales se sont multipliées au cours de la dernière décennie, en résistance au développement du stockage, du traitement et du partage des données. Pour des raisons de police, de sécurité nationale, de protection des données personnelles ou de protectionnisme économique, un nombre croissant de juridictions ont introduit ou renforcé des restrictions au traitement à l'extérieur de leurs frontières des données générées sur leur territoire. Cette tendance est particulièrement prononcée dans la région Asie-Pacifique (Inde, Indonésie et Vietnam notamment).

Le champ d'application et le degré d'exigence des contraintes de localisation des données sont variables. Alors que certains Etats imposeraient des restrictions à presque toutes les données, d'autres Etats auraient ciblé leurs exigences sur certaines catégories de données (telles que les données personnelles, les données commerciales, les données financières, les données publiques ou les informations de santé) ou sur des secteurs économiques spécifiques (typiquement, les services financiers, les fournisseurs de services en ligne, le secteur public et les télécommunications).

En fonction de leur rigueur, les exigences de localisation des données peuvent être classées en trois catégories : i. restrictions conditionnelles aux transferts internationaux de données ; ii. réplication permanente des données sur le sol national et iii. stockage, transmission et traitement des données exclusivement sur le sol national. Par ailleurs, un recensement des mesures limitant le transfert transfrontalier de données[40] a été effectué en 2017 sous l'égide de l'*European Centre for International Political Economy* (ECIPE)[41].

i. Restrictions conditionnelles aux transferts internationaux de données

Certains territoires, parmi lesquelles l'Union européenne avec le RGPD, subordonnent la possibilité d'effectuer des transferts de données à l'extérieur de leur frontière à des conditions reposant soit sur l'entreprise effectuant le transfert (clauses contractuelles avec le destinataire du transfert, consentement éclairé des clients…), soit sur le pays destinataire (existence de règles de protection des données, modalités d'accès des autorités aux données…). Ces restrictions peuvent empêcher le transfert de données vers certains sites ou réduire les avantages économiques d'un traitement des données hors des frontières. L'approche de l'Union européenne en matière de transferts de données

---

[38] "*Data flows across borders overcoming data localization restrictions, Institute of International Finance*", March 2019 https://www.iif.com/Portals/0/Files/32370132_iif_data_flows_across_borders_march2019.pdf

[39] L'*Institute of International Finance* est l'association mondiale de l'industrie financière, avec plus de 450 membres de plus de 70 pays. Sa mission est d'accompagner l'industrie financière dans la gestion prudente des risques; développer de saines pratiques industrielles; et de plaider pour des politiques réglementaires, financières et économiques qui soient dans l'intérêt général de ses membres et favorisent la stabilité financière mondiale et une croissance économique durable. Les membres de l'IIF comprennent des banques commerciales et d'investissement, des gestionnaires d'actifs, des compagnies d'assurance, des fonds souverains, des fonds spéculatifs, des banques centrales et des banques de développement.

[40] Source : Digital Trade Estimates (DTE) Database https://ecipe.org/dte/database/?country=&chapter=829&subchapter=

[41] Cf. également "*Restrictions to Cross-Border Data Flows: a Taxonomy*", ECIPE, Martina F. Ferracane, November 2017 https://ecipe.org/publications/restrictions-to-cross-border-data-flows-a-taxonomy/

à caractère personnel inspire d'autres pays en dehors de l'Union européenne (l'Argentine et le Brésil notamment).

ii. Exigence d'une réplication permanente des données sur le sol national

D'autres pays ont établi des règles visant à obliger les entreprises à conserver à tout moment une copie de leurs données sur des serveurs ou dans des centres de données locaux. Cela ne les prive pas de la faculté de transmettre et de traiter les données à l'étranger, pour autant que les informations soient constamment répliquées et mises à jour sur le territoire national. En règle générale, l'entreprise doit en outre disposer de capacités de traitement locales, à des fins de *back-up*. Le coût de mise en œuvre de ces obligations diminue dans une certaine mesure l'intérêt pour l'entreprise d'une délocalisation de ses traitements de données.

Un projet de loi sur la protection des données personnelles (« *draft Personal Data Protection Bill, 2018* ») est actuellement à l'étude en Inde ; il oblige les entreprises à stocker sur un serveur ou sur un centre de données situé en Inde une copie des données personnelles collectées, publiées, partagées ou traitées dans le pays. Le gouvernement pourrait imposer un traitement exclusivement local de données identifiées comme des « données personnelles critiques ». Au Vietnam, les fournisseurs de services en ligne sont tenus de stocker les données personnelles des citoyens nationaux à l'intérieur du pays. En Argentine, la banque centrale a subordonné l'externalisation de services informatiques à la conservation de certains ensembles de données dans le pays.

La Chine a introduit en 2017 des mesures législatives de localisation des données. Les données personnelles et les « données importantes » détenues par les « opérateurs d'infrastructures d'informations critiques » doivent être stockées sur le sol national. Bien que le traitement à l'étranger de ces données ne soit pas explicitement interdit, les transferts internationaux ne sont autorisés que s'il existe un « besoin réel pour des raisons de nécessité opérationnelle » et ils sont soumis à des évaluations de sécurité, à une approbation réglementaire préalable et à un consentement éclairé du client.

iii. Stockage, transmission et traitement des données exclusivement sur le sol national

Les pays les plus exigeants en matière de localisation de données contraignent leurs entreprises à stocker, à transmettre et à traiter leurs données exclusivement sur le territoire national (par l'effet soit d'une obligation de traitement local, soit d'une interdiction des transferts internationaux de données). La Russie imposerait ce type de restriction à l'égard de larges catégories de données. L'enregistrement, la collecte, le stockage, la mise à jour, la modification et la récupération des données personnelles des citoyens russes doivent être effectués à l'aide de bases de données et de réseaux situés dans le pays. Ce serait une obligation de traiter les données en Russie « en premier lieu », bien que les transferts de données ultérieurs ne soient pas toujours exclus.

D'autres pays n'imposeraient des restrictions strictes qu'à des secteurs ou à des catégories de données plus spécifiques, les services financiers étant communément visés. Par exemple, la Banque populaire de Chine interdirait l'analyse, le traitement et le stockage des informations financières personnelles à l'extérieur du pays (à l'exception de certains transferts de données vers les sièges ou les succursales offshore). De même, la Turquie exigerait des banques et des systèmes de paiement que leurs systèmes d'information soient sur le territoire national. La Reserve Bank of India (RBI) obligerait depuis octobre 2018 les fournisseurs de systèmes de paiement à stocker leurs données exclusivement en Inde.

Des contraintes fortes de localisation des données seraient actuellement à l'étude en Indonésie, où le gouvernement exigerait que les « données électroniques stratégiques » soient traitées, transmises et stockées sur le territoire national, avec une interdiction de communiquer ces données à l'étranger (selon les règles actuelles, les données peuvent être traitées à l'étranger mais une copie et des centres de *back-up* doivent exister en Indonésie).

2.1.2.2 *Des objections au principe d'une localisation des données de paiement en Europe essentiellement limitées aux grands* schemes *internationaux*

La mission a mené des entretiens approfondis avec un large éventail d'interlocuteurs, représentatifs de la diversité des acteurs de la chaîne des paiements opérant en France. Hormis l'opposition des grands *schemes* internationaux de paiements (Visa et MasterCard) et l'inquiétude d'un acteur tel qu'Apple[42], nos interlocuteurs ont exprimé peu d'objections au principe d'une obligation de localisation sur le sol européen des données de paiement correspondant à des transactions européennes.

Au contraire, de nombreux interlocuteurs nous ont fait part de leur adhésion à ce principe ; et ils nous ont souvent signalé une forte sensibilité des commerçants à l'égard du lieu où leurs données de paiement sont stockées, tant pour des raisons de confidentialité que d'image de marque, ce qui se traduit souvent par de stricts engagements contractuels avec les acteurs du paiement.

Une objection fréquente, émanant notamment des banques, tient au caractère défensif, voire protectionniste, d'une obligation de localisation des données de paiement, ainsi qu'au risque d'une efficacité limitée. La création d'un *scheme* de paiement européen (cf. chapitre 2.4, p. 54 et suivantes) nous a été présentée comme une alternative à la fois plus positive et plus efficace.

Visa et MasterCard nous ont présenté trois types d'arguments : i. les effets négatifs sur la croissance économique des politiques de restriction à la libre circulation des données ; ii. les avantages d'une organisation mondiale pour garantir des performances élevées, notamment en matière de lutte contre la fraude, contre le blanchiment d'argent sale et contre la lutte contre le terrorisme ; et iii. le coût élevé pour eux d'une fragmentation de leur organisation.

i. Les effets négatifs sur la croissance économique des politiques de restriction à la libre circulation des données ;

Différentes études tendent à étayer, parfois sans nuance, l'effet négatif sur la croissance des restrictions à la libre circulation des données.

« *Les résultats montrent qu'une perturbation des flux de données transfrontaliers produit des effets négatifs qui ne doivent pas être ignorés. Dans une économie mondialisée, des restrictions commerciales unilatérales constituent une stratégie contre-productive qui se retourne contre le pays concerné, et l'impact négatif à long terme ne peut en être atténué. Les politiques de localisation forcée des données sont souvent le produit d'une analyse économique médiocre ou unilatérale, avec des objectifs protectionnistes dissimulés. Les gains résultant de la localisation des données sont trop faibles pour compenser les pertes en termes de bien-être et de production dans l'économie générale*.[43] »

« *Les données sont l'élément vital de l'économie mondiale moderne. On peut s'attendre à ce que le commerce numérique et les flux de données transfrontières continuent à croître plus vite que le commerce mondial. Les entreprises utilisent les données pour créer de la valeur, et beaucoup d'entre elles ne peuvent maximiser cette valeur que lorsque les données peuvent circuler librement à travers les frontières. Pourtant, un nombre croissant de pays mettent en place des barrières qui rendent plus coûteux et plus long, sinon illégal, le transfert de données à l'étranger. Certains pays fondent leurs décisions d'ériger de telles barrières sur la justification erronée que cela atténuera les problèmes de confidentialité et de cybersécurité; d'autres le font pour des raisons purement mercantilistes. Toutefois, quelle qu'en soit la motivation, comme le montre ce rapport, les coûts de ces politiques sont importants,*

[42] La mission n'a rencontré ni Google, ni Samsung, ni Amazon qui partageraient probablement l'inquiétude d'Apple

[43] Extrait du Summary de l'article : "*The costs of data localisation: Friendly fire on economic recovery*", ECIPE Occasional Paper, No. 3/2014, Provided in Cooperation with European Centre for International Political Economy (ECIPE) https://www.econstor.eu/bitstream/10419/174726/1/ecipe-op-2014-3.pdf

non seulement pour l'économie mondiale, mais pour les Etats concernés qui « se tirent une balle dans le pied » en recourant à ces politiques.[44] »

ii. Le coût élevé pour les grands *schemes* internationaux d'une fragmentation de leur organisation

Les grands *schemes* internationaux de paiement disposent de plateformes technologiques, comprenant des logiciels, du matériel, des centres de données et une importante infrastructure de télécommunications, dotées de technologies de sécurité et de protection sophistiquées. Ces systèmes assurent toutes les fonctions du traitement des transactions (autorisation, compensation et règlement) ainsi que des services à valeur ajoutée (évaluation des risques, *tokenisation*…) dans le cadre d'une exploitation mondiale. Les contraintes de continuité d'exploitation imposent un niveau élevé de redondance. Les données de paiement sont systématiquement enregistrées sur un petit nombre de *datacenters* qui fonctionnent en miroir et qui sont susceptibles de prendre le relais les uns des autres à tout instant.

De telles organisations sont conçues pour fonctionner de manière globale, à l'échelle mondiale. Les *datacenters* représentent des charges d'investissement et de maintenance importantes, leur multiplication et leur dispersion géographique irait à l'encontre de la recherche d'un optimum technique et financier. La fragmentation induite par des obligations réglementaires de localisation des données fait ainsi partie des risques identifiés par Visa dans sa communication financière :

« *Les restrictions imposées par le gouvernement sur les systèmes de paiement internationaux peuvent nous empêcher de rivaliser avec les fournisseurs de certains pays, y compris des marchés importants tels que la Chine, l'Inde et la Russie*. […] *En général, les lois nationales qui protègent les fournisseurs nationaux ou le traitement peuvent augmenter nos coûts; diminuer nos volumes de paiements et influer sur les revenus que nous générons dans ces pays ; diminuer le nombre de produits Visa délivrés ou traités ; nous empêcher d'utiliser nos capacités de traitement mondiales et de contrôler la qualité des services soutenant nos marques ; restreindre nos activités ; limiter notre croissance et notre capacité à introduire de nouveaux produits, services et innovations ; nous obliger à quitter des pays ou nous empêcher d'entrer sur de nouveaux marchés ; et créer de nouveaux concurrents, qui pourraient nuire à notre entreprise*.[45] »

iii. Les avantages d'une organisation mondiale pour garantir des performances élevées, notamment en matière de lutte contre la fraude, contre le blanchiment d'argent sale et contre le financement du terrorisme

Les grands *schemes* internationaux mettent en avant leur expertise et leur contribution à la lutte contre la fraude, contre le blanchiment d'argent sale et contre le financement du terrorisme. Leurs efforts en matière de sécurité protègent l'intégrité de l'écosystème des paiements, en aidant les institutions financières et les commerçants à détecter et à écarter les menaces de fraude.

Ils plaident que la sophistication croissante des techniques de fraude justifient un pilotage et un traitement centralisés : si un schéma de fraude fonctionne dans une partie du monde, il ne s'écoulerait que quelques instants avant qu'il soit répliqué dans d'autres zones géographiques. Une tour de contrôle mondiale présenterait un avantage décisif. Une obligation de localisation des données de paiement pourrait induire une moindre réactivité et une moindre efficacité de la lutte contre la fraude.

---

[44] Extrait de "*Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?*", The Information Technology and Innovation Foundation (ITIF), May 1, 2017
https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost

Cf. également "*Regulating for a digital economy: Understanding the importance of cross-border data flows in Asia*", Global economy & development working paper 113, Brookings, March 20, 2018
https://www.brookings.edu/wp-content/uploads/2018/03/digital-economy_meltzer_lovelock_web.pdf

[45] Visa Annual report 2019, Item 1A: Risk Factors, p. 24 et 25
https://s1.q4cdn.com/050606653/files/doc_financials/2019/ar/Visa-Inc.-Fiscal-2019-Annual-Report.pdf

2.1.3 Les missionnaires se prononcent en faveur d'une obligation de localisation sur le sol européen des données de paiement

Les arguments qui s'opposeraient à une obligation de localisation des paiements n'ont pas emporté la conviction de la mission, qui estime que les effets négatifs sur la croissance économique des politiques de restriction à la libre circulation des données, s'ils sont crédibles dans le cas d'un Etat de taille modeste, le sont moins à l'échelle de l'Union européenne. Les données de paiement, seules en cause ici, représentent un ensemble limité de données. Il existe, avec ou sans obligation de localisation, des facteurs culturels et réglementaires qui limitent en tout état de cause les perspectives de valorisation économique de ces données. La localisation des données de paiement apparaît comme de faible impact au regard d'autres menaces qui affectent le commerce multilatéral ; et, précisément, l'ampleur et l'imprévisibilité des atteintes au multilatéralisme actuellement perceptibles constituent un argument fort en faveur d'une préservation des capacités technologiques européennes en matière de paiement.

S'agissant de la lutte contre la fraude, contre le blanchiment d'argent d'origine criminelle et contre le financement du terrorisme, la situation actuelle de la France et de l'Espagne où, pour des raisons historiques, une très forte proportion des paiements sont traités localement, conduit à relativiser l'intérêt d'une détection à l'échelle mondiale des risques. En particulier, les statistiques de l'observatoire de la sécurité des moyens de paiement constituent un élément de référence rassurant :

« *Après une année de baisse en 2017, la fraude sur les transactions nationales s'est accrue de 8,4 % en 2018. Le montant de la fraude sur les transactions de paiement et de retrait effectuées en France avec des cartes françaises s'établit à 245,6 millions d'euros cette année, contre 226,5 millions d'euros en 2017. Toutefois, sous l'effet de la croissance des transactions nationales (+ 5,2 % en valeur par rapport à 2017), le taux de fraude reste à un niveau relativement bas, quasiment identique à celui de 2017, soit à 0,038 % (contre 0,037 % en 2017), ce qui représente l'équivalent d'un euro de fraude pour environ 2 600 euros de transactions. En ce qui concerne les transactions internationales, la fraude est également en progression de 9,2 % en 2018, avec un montant total de fraude s'élevant à 291,9 millions d'euros, et résulte largement de la dynamique des transactions internationales qui affichent une croissance de 13,4 % en valeur par rapport à 2017. On constate donc une meilleure maîtrise de la fraude sur les transactions internationales avec un taux de fraude qui ressort en baisse à 0,270 %, contre 0,281 % en 2017, soit à son plus bas niveau historique. Toutefois, il est à noter que ce taux de fraude demeure toujours élevé au regard du montant des opérations concernées puisque les transactions internationales représentent 54 % du montant total de la fraude alors qu'elles ne comptent que pour 14 % de la valeur totale des transactions*.[46] »

Les enjeux financiers et les contraintes d'une obligation de localisation des données de paiement pour les grand *schemes* internationaux ne doivent pas être minorés, en particulier si ceux-ci devaient à brève échéance investir dans la mise en place de centres de traitement localisés sur le sol européen. Il importe de prendre ces enjeux en considération et de ne pas accréditer, par une mise en œuvre excessivement contraignante, le soupçon que cette mesure serait en réalité inspirée par un motif de protectionnisme économique.

Toujours est-il qu'à l'issue de plus de cinquante entretiens menés avec une grande diversité d'interlocuteurs représentatifs de l'écosystème des paiements, au vu des événements et des enjeux présentés au 1er chapitre de ce rapport, après avoir entendu et analysé les objections relevées ci-dessus, **les missionnaires estiment possible et souhaitable d'instituer à l'échelle de l'Espace économique européen (et éventuellement de la Suisse) une obligation de localisation sur le sol européen des données de paiement**, telles que définies ci-dessus au § 2.1.1.2, p. 22, lorsque les paiements interviennent entre deux parties européennes. Cette obligation serait stricte, c'est-à-dire que les données de paiement soumises à cette obligation de localisation ne pourraient être transférées

[46] Extrait du Rapport annuel 2018 de l'observatoire de la sécurité des moyens de paiement https://www.banque-france.fr/sites/default/files/medias/documents/819172_osmp2018_web_3.pdf

hors des frontières européennes, et elle s'appliquerait à l'ensemble des acteurs économiques, qu'ils soient ou non régulés.

En outre, l'objectif ne devrait pas seulement consister à assurer le traitement des données de paiement sur le sol européen, dès lors que les deux parties sont elles-mêmes européennes, mais aussi à interdire le transfert hors des frontières européennes de ces données de paiement. Il paraîtrait en effet déraisonnable d'instituer une contrainte aussi lourde et structurante que l'obligation de localisation des données, si on autorisait par ailleurs leur fuite légale.

De même, il n'apparaît pas souhaitable de restreindre l'obligation de localisation aux seuls acteurs ayant une taille critique, quelle que soit cette taille critique ; cette situation se traduirait en effet par des effets de seuil et par une forte distorsion de concurrence. Enfin, pour le même motif d'égalité de concurrence, l'obligation de localisation ne devrait pas s'imposer aux seuls établissements financiers régulés, mais également aux commerçants et aux prestataires de services qui agissent pour leur compte.

Recommandation n° 1. Instituer à l'échelle de l'Espace économique européen une obligation de localisation sur le sol européen des données relatives à des paiements intra-européens, lorsque ces données sont liées aux données de sécurité personnalisées d'une personne physique. Cette obligation serait stricte, c'est-à-dire que les données de paiement soumises à l'obligation de localisation ne pourraient être transférées hors des frontières européennes, et elle s'appliquerait à l'ensemble des acteurs économiques, qu'ils soient ou non régulés. Ces règles s'inscriraient dans le cadre du règlement 2016/679 (RGPD).

2.1.4 La localisation des données en Europe ne constitue qu'une réponse partielle et imparfaite aux enjeux de souveraineté européenne en matière de paiement

2.1.4.1 Les effets bénéfiques d'une localisation des données de paiement

L'obligation de localisation sur le sol européen des données de paiement constitue une précaution utile pour l'avenir. Elle peut dans une certaine mesure prémunir les ressortissants européens contre des évolutions potentiellement néfastes et irréversibles des systèmes de paiement qui, à travers l'exploitation à grande échelle des données de paiement, pourraient conduire à une dépendance politique, économique et culturelle accrues au profit d'acteurs et/ou d'autorités extra-européennes, à une perte de *soft power* européen.

Même si, dans de très nombreux cas, des entreprises qui ne sont pas européennes, mais qui sont présentes sur le territoire européen sous la forme d'une succursale, coopèrent aujourd'hui sans réserve avec les autorités européennes, la localisation des données de paiement est de nature à faciliter le contrôle et la sanction de manquements aux règles de protection des données personnelles (cf. ci-dessus § 1.2.4, p. 20), ainsi que l'action des représentants de l'ordre (réquisition judiciaire…) et celle de Tracfin[47].

A l'inverse, une localisation des données de paiement assortie d'une interdiction de transférer ces données hors des frontières européennes pourrait, dans une certaine mesure, tenir à distance les

[47] Tracfin est un service de renseignement placé sous l'autorité du Ministère de l'Action et des Comptes publics. Il concourt au développement d'une économie saine en luttant contre les circuits financiers clandestins, le blanchiment d'argent et le financement du terrorisme.

autorités étrangères qui voudraient collecter des données de paiement en dehors du cadre des traités d'assistance mutuelle (MLAT).

A cet égard, il est intéressant de noter deux points de fait importants dans le mémoire établi par le gouvernement américain à l'occasion de l'action qu'il engageait contre Microsoft devant la Cour Suprême (cf. ci-dessus § 1.1.5, p. 15) : d'une part, les informations stockées dans le *datacenter* de Microsoft à Dublin, circulaient librement : « *l'équipe Global Criminal Compliance de Microsoft peut accéder aux informations de compte stockées n'importe où dans le réseau mondial de Microsoft depuis ses bureaux aux États-Unis*[48] » ; d'autre part, Microsoft ne s'était pas engagé vis-à-vis de ses clients à ne pas transférer leurs données aux Etats-Unis.

En d'autres termes, les autorités américaines étaient d'autant plus acharnées à faire valoir ce qu'elles estimaient être leur bon droit que leur demande de communication leur paraissait dépourvue de difficulté et qu'elles ne comprenaient pas les réticences de Microsoft. Le cantonnement technique et juridique des données incriminées sur le sol européen aurait peut-être changé leur appréciation.

Même depuis l'entrée en vigueur du CLOUD Act, il est possible que l'obligation de localisation des données de paiement sur le sol européen et l'absence de procédure de transfert suffise dans certains cas à gêner la communication de données aux autorités américaines. Le CLOUD Act prévoit en effet que le fournisseur de services auquel les données sont demandées a toujours la possibilité de s'y opposer au motif que la demande, si elle devait être satisfaite, le conduirait à méconnaître la législation d'un pays étranger et l'exposerait à des sanctions.[49]

Par ailleurs, si des dispositions techniques empêchent le transfert des données de paiement hors d'Europe, la moindre circulation de ces données limite le risque d'espionnage.

2.1.4.2 L'obligation de localisation des données de paiement ne suffit pas à assurer la primauté des lois européennes

Sauf à imposer par surcroît que les données de paiement européennes ne soient traitées que par des acteurs eux-mêmes européens et sur lesquels aucun gouvernement étranger n'aurait de prise, la localisation des données de paiement n'apporte pas une garantie absolue de protection. Un acteur soumis à la fois à l'obligation européenne de localisation des données de paiement et à une loi étrangère contraire pourrait estimer devoir privilégier la seconde. Il n'est nullement acquis, notamment, que toutes les entreprises américaines feraient primer l'obligation européenne de localisation des données sur le CLOUD Act.

Au-delà des enjeux de données de paiement *stricto sensu*, le respect par un acteur extra-européen de l'obligation de localisation des données de paiement n'écarte pas tout risque politique (cf. ci-dessus § 1.2.1, p. 20). A titre d'illustration, il nous a été signalé que Visa, en tant qu'entreprise américaine, demande aux banques françaises de contrôler si les porteurs de cartes figurent sur la liste de *l'Office of Foreign Assets Control* (OFAC) des personnalités soumises à des sanctions américaines[50] – même quand la carte est co-badgée et utilisée sur le *scheme* GIE CB.

L'OFAC publie en effet sous sa seule autorité une liste de personnes et d'entreprises détenues, contrôlées, ou agissant pour le compte de certains pays. L'OFAC répertorie également des individus, des groupes et des entités, suspectés de terrorisme ou de trafic de stupéfiants, désignés dans le cadre de programmes qui ne sont pas spécifiques à un pays. Collectivement, ces individus et sociétés sont

---

[48] USA v. Microsoft Corporation, Brief for the United States, December 6, 2017

[49] Cf. note 29 « *Faut-il avoir peur du CLOUD Act ?* », Emmanuelle Mignon, August Debouzy Avocats, 29 juin 2018

[50] Specially Designated Nationals and Blocked Persons list ("*SDN List*"), Foreign Sanctions Evaders List, List of Persons Identified as Blocked Solely Pursuant to E.O. 13599, Non-SDN Iran Sanctions Act List, Part 561 list, Sectoral Sanctions Identifications List and Non-SDN Palestinian Legislative Council List

appelés « ressortissants spécialement désignés » ou « SDN ». Leurs actifs sont bloqués et il est généralement interdit aux personnes américaines de traiter avec eux.

Mais vis-à-vis des établissements européens, seuls l'ONU et le Conseil de l'Union européenne ont le pouvoir d'adopter des mesures restrictives financières ou commerciales à l'encontre de personnes physiques ou morales, que ces mesures prennent la forme d'interdictions et de restrictions au commerce de biens, de technologies ou de services ciblés avec certains pays, de mesures de gel des fonds et ressources économiques ou de restrictions à l'accès aux services financiers.[51]

2.1.4.3 Il pourrait exister de meilleurs critères que la localisation pour assurer la maîtrise des données de paiement

Certains interlocuteurs de la mission doutent de l'efficacité du critère de localisation, en arguant que le contrôle des données devrait davantage porter sur les modalités d'accès à ces données que sur leur localisation physique. Selon leur thèse, les exigences de localisation des données – imposant que certaines données des utilisateurs soient conservées à l'intérieur des frontières nationales – refléteraient une méconnaissance des évolutions récentes et à venir des systèmes informatiques et porteraient atteinte à la compétitivité économique des acteurs soumis à ces exigences.

De nombreuses raisons contribuent en effet à rendre la notion de localisation inefficace[52] : pour optimiser l'utilisation des serveurs, si une région a du mal à répondre à un surcroît d'activité, une partie de cette activité est transférée vers une autre région ; les données relatives à un individu peuvent être réparties de manière dynamique en fragments (*shards*), distribuées, copiées et sauvegardées sur plusieurs machines, afin d'améliorer la performance et l'efficacité (équilibrage dynamique de charge) ; l'assurance d'un haut degré d'intégrité des données nécessite leur réplication dans différents centres de données et dans différentes régions, à l'abri d'une catastrophe naturelle ou de la perturbation physique d'un centre de données…

Mais, d'une part, la notion de contrôle des données, si elle est plus pertinente, apparaît aussi plus difficile à énoncer, à implémenter et à faire respecter que celle de localisation physique des données ; et d'autre part, les inconvénients de cette approche semblent devoir être relativisés par la dimension de l'espace européen et, au contraire, par le caractère très modeste des données auxquelles s'appliquerait l'obligation de localisation.

2.1.4.4 Les infractions aux règles de localisation devraient donner lieu à des amendes dissuasives

Les violations de l'interdiction de transfert des données de paiement peuvent être difficiles à déceler, même par les personnes concernées. L'obligation de localisation des données de paiement, qui viendrait compléter les règles de protection des données personnelles prévues par le RGPD, devrait reposer sur la responsabilité des acteurs et entrer dans le champ de la mission du délégué à la protection des données des entreprises concernées, quand il a été désigné. La violation des règles de localisation des données de paiement devrait être passible, comme la violation des dispositions du RGPD, de sanctions élevées (dans le cas du RGPD, des amendes administratives pouvant atteindre 20 000 000 € ou 4 % du chiffre d'affaires annuel mondial). De telles sanctions présentent l'intérêt d'être dissuasives aussi bien à l'égard des contrevenants que, semble-t-il, des autorités étrangères.

On citera à cet égard le rapport établi par le député Gauvain à propos de la loi de blocage : « *Le caractère dérisoire des sanctions encourues a été signalé à la mission par de nombreux juristes ou*

---

[51] Cf. « *Sanctions économiques internationales* »
https://www.tresor.economie.gouv.fr/services-aux-entreprises/sanctions-economiques

[52] Cf. par exemple "*Where Is Your Data, Really?: The Technical Case Against Data Localization*", Lawfare, Dillon Reisman, May 22, 2017
https://www.lawfareblog.com/where-your-data-really-technical-case-against-data-localization

cabinets d'avocats comme un des éléments qui, aujourd'hui, nuit à la crédibilité de la loi de 1968 aux yeux des autorités étrangères, notamment américaines. En effet, ces dernières pour analyser la légitimité de l'excuse légale que pourrait invoquer l'entreprise française qui refuse de faire droit à une demande d'information ou de transmission de documents, examinent la réalité de la sanction encourue par l'entreprise dans son propre pays avec deux critères principaux : le montant de la sanction et son caractère effectif (les sanctions déjà prononcées dans le passé). »

2.2 La révision du règlement interchange

La localisation des données de paiement, telle qu'elle est envisagée au chapitre précédent, constitue une mesure de caractère très général, dans la mesure où elle devrait s'appliquer à toute entreprise, régulée ou non, susceptible de détenir ou de contrôler des données de paiement ; cette mesure présente une forte spécialité par rapport au RGPD puisqu'elle ne s'appliquerait qu'à des données de nature très particulière, les données de paiement. A supposer qu'un consensus européen se forme, il faudra encore déterminer quel véhicule législatif européen se prêterait à la mise en œuvre et dans quel délai.

C'est l'intérêt de réfléchir également à des mesures de portée plus modeste mais dont l'implémentation serait plus facile. L'importance des paiements par carte en Europe et l'essor de grands *schemes* internationaux américains, chinois et russes amènent naturellement à des réflexions spécifiques. L'importance du règlement interchange[53] pour les transactions par carte et l'établissement en 2020 d'un rapport de la Commission sur son application y contribuent également.

Le règlement interchange a constitué, avec la 2ème directive sur les services de paiement, un « paquet » de propositions législatives présenté par la Commission européenne le 24 juillet 2013. Le règlement portait sur les paiements par carte et avait essentiellement pour objectif de plafonner les commissions d'interchange (cf. ci-dessous, chapitre 2.2.1.5 p. 35), honnies par la Commission. Deux dispositions ont également pour but de renforcer la concurrence et l'harmonisation du marché des services de paiement au sein de l'Union européenne :

- l'une (« *co-badgeage et choix de l'application de paiement* ») vise à ce que le choix de l'application de paiement, dans le cas d'une carte co-badgée (MasterCard/CB, Visa/CB…), revienne au consommateur et ne puisse pas être imposé à l'avance au moyen de mécanismes automatiques insérés dans l'instrument ou l'équipement du point de vente ;
- l'autre (« *séparation entre scheme et entité de traitement* ») pose un principe de séparation, au niveau organisationnel, entre les *schemes* et les entités de traitement des opérations (et d'interdiction de la discrimination territoriale dans les règles de traitement, tout en rendant obligatoire l'interopérabilité technique entre les systèmes des entités de traitement).

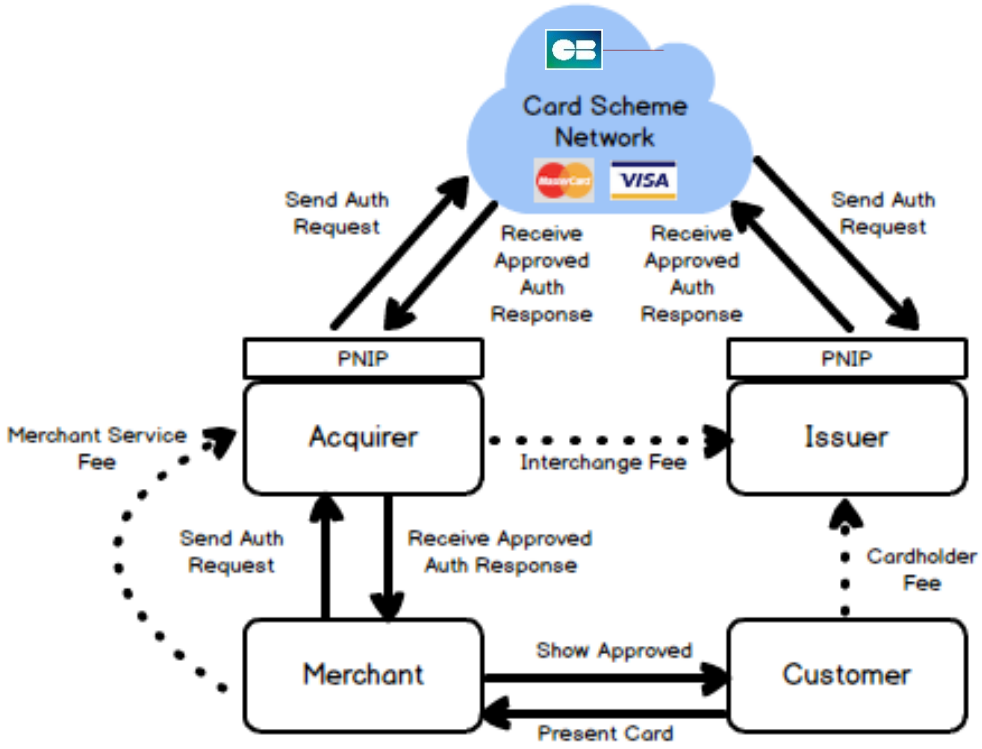
Ces deux dispositions sont explicitement dans le champ du rapport attendu de la Commission (les effets du co-badgeage sur la facilité d'utilisation ; l'application en pratique des règles sur la séparation du schéma de cartes de paiement et du traitement, et la nécessité de réexaminer la séparation juridique[54]). Elles présentent des liens étroits avec l'objet du présent rapport. Par ailleurs, la question d'une nouvelle réduction des interchanges, voire de leur suppression, est ouverte « *en prenant en compte l'utilisation et le coût des différents moyens de paiement et le niveau d'entrée sur le marché de nouveaux acteurs, de nouvelles technologies et de modèles commerciaux innovants* ».

[53] Règlement 2015/751 du 29 avril 2015 relatif aux commissions d'interchange pour les opérations de paiement liées à une carte, également désigné comme le règlement IFR (interchange fees regulation) https://eur-lex.europa.eu/legal-content/fr/TXT/?uri=CELEX:32015R0751

[54] cf. points f) et j) de l'article 17 du règlement 2015/751 (Clause de réexamen)

2.2.1 Quelques indications sur le paiement par carte

2.2.1.1 Le schéma général d'une transaction



Le schéma ci-dessus[55] illustre le traitement d'un paiement par carte et le rôle des différents acteurs. Une transaction de paiement doit être acheminée entre un client (*customer*), qu'on appelle indifféremment dans la suite consommateur ou payeur, et un commerçant (*merchant*). La banque[56] du client, qui a émis la carte bancaire, s'appelle la banque émettrice (*issuer*), celle du commerçant la banque acquéreur (*acquirer*). Les banques sont reliées entre elles par un réseau, organisé selon les règles d'un *scheme* (tel que Visa, MasterCard ou le Groupement Carte Bancaire) et qui assure entre elles la circulation des informations. Si, par exception, la banque acquéreur se trouve aussi être la banque émettrice, le réseau associé au scheme n'est pas nécessaire : on parle de transaction *on-us*.

2.2.1.2 L'authentification du porteur de la carte

On peut distinguer deux situations assez différentes, selon que le consommateur et le commerçant sont face-à-face, sur le lieu de vente ; ou que la transaction a lieu à distance, sur un site de e-commerce (également appelé site marchand).

Dans le premier cas, la carte bancaire est introduite dans un terminal de paiement (TPE) ou, dans le cas du paiement sans contact, placée à sa proximité immédiate. Le TPE peut ou non être interfacé avec la caisse enregistreuse. La transaction est traitée par différents prestataires techniques (prestataires d'acceptation technique, ou PAT) qui peuvent jouer un rôle de détection de cas de fraude, de choix de

---

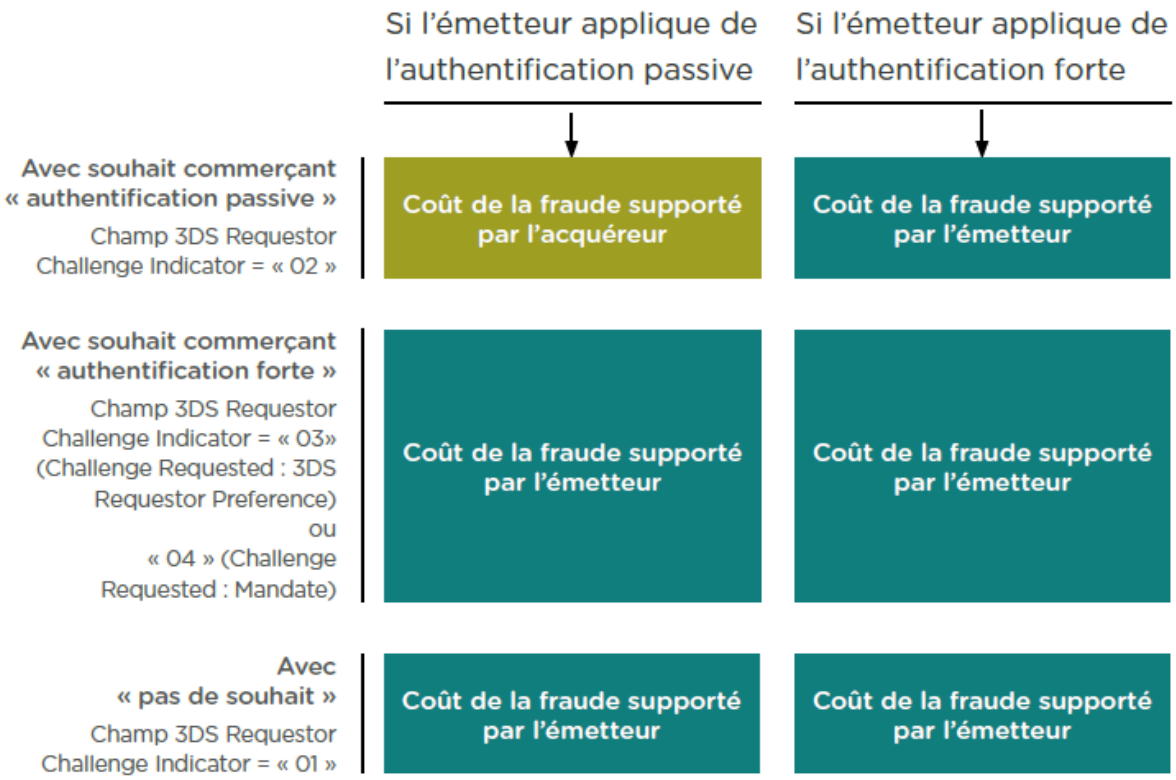
[55] Ce schéma, issu d'un article de blog : "*How Credit Card Transactions Work*", Darren Smith, November 29, 2017, a été choisi pour sa clarté https://blog.darrensmith.com.au/how-credit-card-transactions-work-88a5acc9e3c

[56] Le terme de banque est utilisé par abus et par commodité, il faudrait en réalité parler de prestataire de service de paiement, qui peut être soit une banque, soit un établissement de paiement

la banque, de transfert sécurisé des caractéristiques du paiement, etc. L'existence dans la carte d'une puce électronique permet l'authentification du consommateur, dès lors qu'il compose sur un clavier un code, dit code PIN (l'authentification n'est toutefois pas systématique dans le cas du paiement sans contact, du fait de la petitesse des montants).

Dans le second cas, le site de e-commerce, au moment du paiement, bascule l'internaute sur une page de paiement gérée par un prestataire technique. L'identité du consommateur peut être authentifiée par sa banque, la banque émettrice (aujourd'hui, souvent, par l'envoi d'un SMS sur son téléphone portable ; demain par la mise en jeu d'une authentification dite forte, définie par la deuxième directive sur les services de paiement (DSP2)[57] et par un règlement délégué qui en précise les modalités technique d'application[58]. L'authentification du consommateur par sa banque s'appuie sur un protocole sécurisé de paiement sur internet, 3D Secure, appelé à évoluer d'une version 3DS 1.0 à une version 3DS 2.1 (puis 2.2 fin 2020) du fait des nouvelles obligations d'authentification forte[59].

Dans l'ancien dispositif, le e-commerçant pouvait choisir de ne pas recourir à 3D Secure (et d'assumer le risque de non-paiement) ; dans le nouveau, sauf exceptions, le e-commerçant ne dispose pas de la décision finale d'authentifier son client (il peut seulement indiquer sa préférence). La décision appartient à la banque du client qui a émis la carte (l'émetteur). C'est la raison pour laquelle le protocole 3DS 2.1 organise le partage tout au long de la chaîne de paiement d'un grand nombre de données personnelles décrivant le contexte de la transaction.



[57] Directive 2015/2366 du 25 novembre 2015 concernant les services de paiement dans le marché intérieur

[58] Règlement délégué 2018/389 du 27 novembre 2017 complétant la directive 2015/2366 par des normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication

[59] Cf. par exemple « *Sécurité des paiements à distance et mise en œuvre de la DSP2* », FEVAD, 18 juillet 2019 ; cf. aussi « *Comment se préparer à la DSP2 avec Fast'R by CB* »
https://www.fevad.com/securite-des-paiements-a-distance-et-mise-en-oeuvre-de-la-dsp2/
http://www.cartes-bancaires.com/wp-content/uploads/2019/10/BROCHURE-IMPLEMENTATION-FASTR2_plancheWEB.pdf

2.2.1.3 L'acceptation du paiement

Le commerçant transmet une demande de paiement par l'intermédiaire de son prestataire d'acquisition technique et de la banque acquéreur. Le *scheme* reconnaît, à travers le numéro de la carte (le PAN) quelle est la banque émettrice (identifiée par les premiers chiffres du numéro de carte) et transmet à celle-ci la demande de paiement. La banque émettrice vérifie la régularité du compte et l'existence d'une provision avant, le cas échéant, de valider la transaction. Cette information de validation du paiement remonte la chaîne jusqu'au commerçant.

2.2.1.4 La compensation et le règlement

C'est en général le traitement par lot d'un ensemble de paiements par cartes qui assure en définitive le règlement du commerçant. Ce traitement est assuré par une plate-forme de compensation interbancaire, telle que la STET.

2.2.1.5 Les commissions d'interchange

Le modèle d'affaires du paiement par carte repose sur l'idée que le commerçant accepte plus volontiers que le consommateur de supporter les coûts de transaction. La banque émettrice pourrait s'en trouver pénalisée, alors qu'elle supporte à la fois le coût de distribution des cartes et la charge consistant à accepter à bon escient les paiements.

De longue date, les *schemes* ont institué le principe de commissions multilatérales d'interchange (CMI) : toutes les banques participant au *scheme* acceptent le principe d'un reversement forfaitaire de la banque acquéreur à la banque émettrice. Ainsi, les commerçants payent contractuellement à leur banque acquéreur une commission globale, le *merchant service fee* sur le schéma de la page 33. Une partie de cette commission est rétrocédée sous forme de commission d'interchange (*interchange fee*) à la banque émettrice. La banque émettrice a une double source de revenus : les commissions d'interchange et les cotisations annuelles (*cardholder fees*) payées par les porteurs de cartes (mais les cartes sont parfois distribuées gratuitement).

Le *merchant service fee*, de manière plus ou moins transparente, rémunère à la fois la banque acquéreur, la banque émettrice (par l'intermédiaire des commissions d'interchange) et le *scheme* (*scheme fees*), à la fois au titre de son rôle de chef d'orchestre et au titre du traitement des transactions.

2.2.2 La défense des cartes co-badgées

2.2.2.1 La raison d'être du co-badgeage

Le co-badgeage constitue dans plusieurs pays de l'Union européenne le cadre traditionnel de coopération entre un *scheme* domestique (GIE CB en France, Bancomat en Italie, Girocard en Allemagne…) et un *scheme* international (Visa ou MasterCard). Dans le cas de la France, la règle a longtemps prévalu qu'une transaction domestique par carte (*i.e.* entre un consommateur français et un commerçant français détenant chacun un compte dans une banque française) devait être traitée selon les règles du GIE CB. Si par contre le consommateur ou le commerçant était étranger, ou affilié à une banque étrangère, et seulement dans ces cas, la transaction était gérée par le *scheme* international, Visa ou MasterCard.

Cette règle de partage assurait un degré élevé de souveraineté nationale sur les transactions domestiques ; elle garantissait notamment que les données de paiement correspondantes étaient localisées sur le sol français. Pour autant, avec les mêmes cartes co-badgées et avec une grande commodité, les consommateurs français étaient en mesure de procéder à des achats partout dans le

monde, de même que les TPE des commerçants français leur permettaient de recevoir des paiements de clients de toutes nationalités, grâce aux *schemes* internationaux Visa et MasterCard.

Toutefois, du point de vue de la Commission européenne, cette organisation du marché des paiements contribuait à pérenniser d'invisibles frontières nationales qui fragmentaient le marché européen et faisaient obstacle à l'émergence du marché unique. Le règlement 2015/751 l'a faite voler en éclats en posant le principe que, désormais, les *schemes* nationaux et internationaux ne devaient plus être complémentaires, mais concurrents. Si une carte est co-badgée, rien ne doit empêcher le porteur de la carte d'utiliser comme bon lui semble l'une ou l'autre des deux marques de paiement. Le commerçant peut choisir un *scheme* de règlement par défaut, mais le consommateur est censé avoir la liberté, à chaque paiement, d'imposer son propre choix.

Cette nouvelle situation affecte profondément les *schemes* nationaux, jusqu'ici protégés à la fois par des règles de droit et par un alignement d'intérêts avec les banques émettrices. L'organisation et le statut même des *schemes* nationaux (en France, la gouvernance du GIE CB repose sur ses membres, qui sont les banques) se prêtent mal au défi qui leur est fait de s'internationaliser, de s'allier et de défendre leurs marques (cf. à cet égard, ci-dessous, le chapitre 2.4.3.3, p. 58).

2.2.2.2 Ce que dit précisément le règlement

L'article 8 du règlement 2015/751 porte sur le co-badgeage et le choix de la marque de paiement ou de l'application de paiement :

« *1. Sont interdites toutes les règles régissant les schémas de cartes de paiement et celles régissant les accords de licence ou les mesures ayant un effet équivalent qui font obstacle ou empêchent un émetteur de co-badger deux ou plusieurs marques de paiement ou applications de paiement sur un instrument de paiement lié à une carte, ou qui y font obstacle.*

2. Lorsqu'il conclut un accord contractuel avec un prestataire de services de paiement, le consommateur peut demander que deux ou plusieurs marques de paiement soient apposées sur un instrument de paiement lié à une carte, à condition qu'un tel service soit proposé par le prestataire de services de paiement. Bien avant la signature du contrat, le prestataire de services de paiement fournit au consommateur des informations claires et objectives sur toutes les marques de paiement disponibles et leurs caractéristiques, y compris leur fonctionnalité, coût et dispositif de sécurité.

3. Toutes les différences de traitement entre émetteurs ou acquéreurs dans les règles régissant les schémas et les règles régissant les accords de licence concernant le co-badgeage de différentes marques de paiement ou applications de paiement sur un instrument de paiement lié à une carte sont objectivement justifiées et non discriminatoires.

4. Les schémas de cartes de paiement ne peuvent imposer d'exigences de déclaration, de paiement de frais ou d'obligations similaires ayant le même objet ou le même effet aux prestataires de services de paiement émetteurs et acquéreurs pour les opérations effectuées avec quelque instrument que ce soit sur lequel leur marque de paiement est apposée si leur schéma n'est pas utilisé lors de ces opérations.

5. Toutes les conditions applicables au routage ou les mesures équivalentes visant à guider les transactions via un canal ou un processus spécifique, ainsi que les autres normes et exigences techniques et de sécurité relatives à la gestion de deux ou de plusieurs marques de paiement et applications de paiement sur un instrument de paiement lié à une carte ou à un appareil de télécommunication numérique ou informatique sont non discriminatoires et s'appliquent sans discriminations.

6. Les schémas de carte, les émetteurs, les acquéreurs, les entités de traitement et les autres prestataires de services techniques n'insèrent aucun mécanisme automatique, logiciel ou dispositif limitant le choix de la marque de paiement et/ou de l'application de paiement par le payeur ou le bénéficiaire qui utilisent un instrument de paiement co-badgé sur ce dernier ou sur l'équipement installé dans le point de vente.

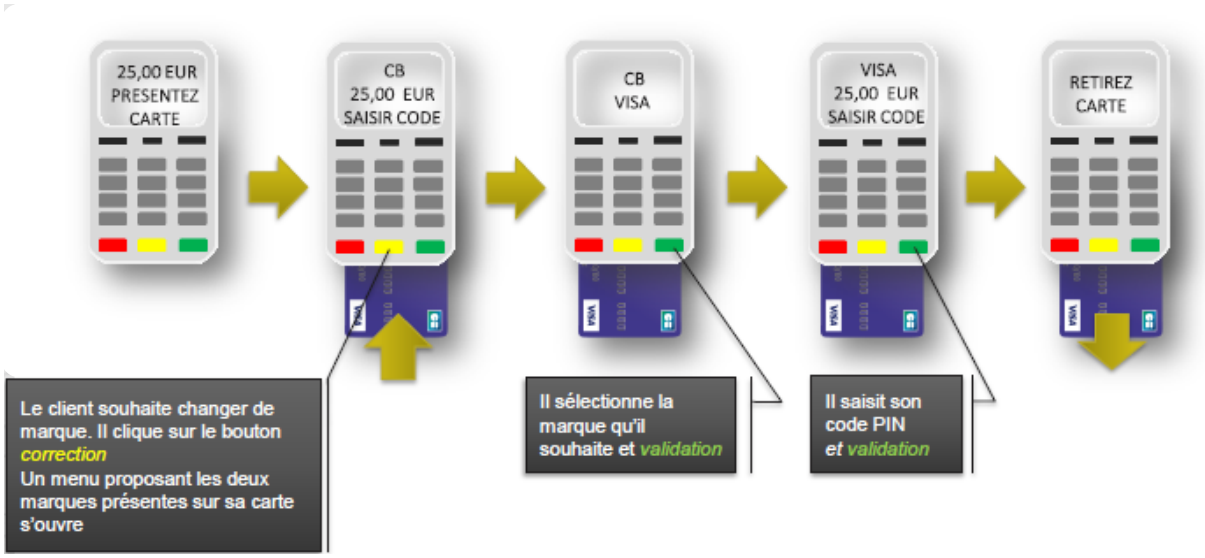
Les bénéficiaires conservent la possibilité d'installer, sur l'équipement utilisé au point de vente, des mécanismes automatiques qui effectuent la sélection prioritaire d'une marque de paiement ou d'une application de paiement spécifique mais les bénéficiaires ne peuvent s'opposer à ce que les payeurs passent outre cette sélection prioritaire automatique effectuée par le bénéficiaire dans son équipement pour les catégories de cartes ou d'instruments de paiement liés acceptés par le bénéficiaire. »

2.2.2.3 La mise en œuvre des nouvelles règles

En contrepartie de la mise en concurrence forcée des *schemes* nationaux, l'article 8 du règlement 2015/751 conforte en premier lieu l'existence du co-badging. Une disposition particulièrement importante tient au paragraphe 6, qui proscrit tout mécanisme automatique, logiciel ou dispositif limitant le choix pour le porteur de la carte de la marque de paiement. Si un *scheme* national ne peut plus bénéficier d'une exclusivité dans certaines situations, il ne peut pas non plus être évincé : c'est un aspect sur lequel nous reviendrons à propos de la *tokenisation* (cf. chapitre 2.3.2.4 p. 51 et Recommandation n° 4).

Le respect d'une absence de discrimination entre les deux marques d'une carte co-badgée et la possibilité pour le porteur de carte de choisir sa marque de paiement (en passant outre tout choix automatique) peuvent être compliqués dans certains cas d'usage : paiement sans contact, cas d'un commerçant qui dispose de comptes dans plusieurs banques acquéreurs et affecte à chaque banque les paiements reçus au moyen de cartes qu'elle a émises (transaction *on-us*), sans recourir à aucun *scheme* intermédiaire…

Au Portugal, le choix entre les deux marques d'une carte co-badgée serait systématiquement offert. En France, une manipulation permet quelquefois au porteur d'une carte co-badgée de changer de *scheme* (sur le point de vente, en appuyant sur la touche jaune du terminal de paiement avant d'entrer le code PIN, comme indiqué sur le schéma ci-dessous[60]). Cette manipulation n'est jamais clairement expliquée et elle est rarement offerte[61].



[60] Cf. « *Paiement en ligne : comment mettre en œuvre le « choix de la marque » sur son site* », FEVAD, 1 décembre 2016 https://www.fevad.com/paiement-ligne-mettre-oeuvre-choix-de-marque-site/

[61] Certains interlocuteurs de la mission estiment que le règlement n'impose pas explicitement de donner systématiquement le choix au consommateur, mais seulement de permettre ce choix (par exemple après une explication entre le client et le commerçant et une manipulation effectuée par le commerçant)

En infraction avec le règlement 2015/751, le choix du *scheme* au moment du paiement est rarement offert au porteur d'une carte co-badgée. Cette observation vaut aussi bien pour le paiement sur le lieu de vente que pour le paiement sur internet. L'inobservation, et peut-être l'inadéquation de cette règle, ne peuvent manquer d'être analysées dans le cadre de la révision du règlement.

2.2.3 La séparation entre le *scheme* (la définition des règles) et le *processing* (l'exécution des traitements)

2.2.3.1 La règle posée par le règlement 2015/751

Le considérant (33) du règlement 2015/751 explique qu' « ***une séparation entre le scheme et l'infrastructure*** [c'est-à-dire l'entité qui effectue les traitements] ***devrait permettre à tous les services de traitement de se disputer la clientèle des schemes***. *Le coût du traitement des paiements représentant une part notable du coût total de l'acceptation des cartes,* ***il importe que cette partie de la chaîne de valeur soit ouverte à une concurrence effective***. *Aux fins de la séparation entre le* scheme *et l'infrastructure, les* schemes *de cartes et les entités de traitement devraient être indépendants sur le plan comptable, organisationnel et décisionnel. Ils ne devraient pas se comporter de manière discriminatoire, par exemple en s'accordant un traitement préférentiel ou en se communiquant des informations privilégiées qui ne sont pas accessibles à leurs concurrents sur leur segment de marché respectif, en imposant des exigences d'information excessives à leurs concurrents sur leur segment de marché respectif, en faisant bénéficier leurs activités respectives de subventions croisées ou en s'appuyant sur des dispositifs de gouvernance communs. De telles pratiques discriminatoires contribuent à la fragmentation du marché, ont un effet négatif sur l'entrée de nouveaux acteurs sur le marché et empêchent l'émergence d'acteurs présents dans toute l'Union*... »

A cet effet, l'article 7 du règlement 2015/751 vise à instituer une séparation entre le scheme de cartes de paiement et les entités de traitement :

« *1. Les schémas de cartes de paiement et les entités de traitement:*

a) sont des entités indépendantes du point de vue de la comptabilité, de l'organisation et des processus décisionnels;

b) ne présentent pas les prix de manière groupée pour les activités liées au schéma de cartes de paiement et au traitement et n'octroient pas de subventions croisées à ces activités;

c) ne pratiquent aucune discrimination entre leurs filiales ou leurs actionnaires, d'une part, et les utilisateurs des schemes de cartes de paiement et d'autres partenaires contractuels, d'autre part, et notamment ne subordonnent aucunement la prestation de services à l'acceptation, par l'autre partenaire contractuel, d'un autre service qu'ils proposent, quel qu'il soit.

2. L'autorité compétente de l'État membre dans lequel le siège statutaire du schéma est situé peut exiger qu'un scheme *de cartes de paiement fournisse un rapport indépendant confirmant qu'il respecte le paragraphe 1.*

3. Les schemes *de cartes de paiement prévoient la possibilité que les messages d'autorisation et de compensation d'opérations de paiement isolées liées à une carte soient distincts et traités par des entités de traitement différentes.*

4. Sont interdites toutes les discriminations territoriales dans les règles de traitement appliquées par les schemes *de cartes de paiement.*

5. Les entités de traitement au sein de l'Union veillent à ce que leur système soit techniquement interopérable avec les systèmes d'autres entités de traitement au sein de l'Union en utilisant des normes élaborées par des organismes de normalisation internationaux ou européens. En outre, les

schemes de cartes de paiement n'adoptent pas ou n'appliquent pas de règles commerciales qui restreignent l'interopérabilité avec d'autres entités de traitement au sein de l'Union. »

Un 6ème point renvoie à un règlement délégué[62] la détermination des exigences que doivent respecter les *schemes* de cartes de paiement et les entités de traitement afin de garantir leur indépendance sur le plan comptable, organisationnel et décisionnel en application de l'article 1a).

2.2.3.2 La portée de cette règle et sa mise en œuvre

L'intention du législateur européen semble claire et la formulation du paragraphe 1a), précisée par surcroît par le règlement délégué, prête peu à ambiguïté ; mais ceci est moins vrai du paragraphe 1c). Il est intéressant de noter qu'une version intermédiaire du texte[63], validée par le Parlement européen, comportait une phrase qui aurait clarifié la règle et complètement répondu à l'objectif de séparation entre le *scheme* et l'infrastructure : "*Scheme rules and rules in licensing agreements or other contracts leading to a restriction on the freedom to choose a processor shall be prohibited*". Mais cette phrase n'a pas été reprise dans la version finale du règlement.

Les "*processing entities*" visées par l'article 1c) sont les entreprises qui, comme STET en France ou Redsys en Espagne, sont susceptibles d'intervenir dans le *processing* interbancaire des transactions par cartes, entre la banque émettrice et la banque acquéreur. Mais dans les faits, un commerçant ou une banque acquéreur n'a pas le choix entre plusieurs entités de *processing*. Les flux de transactions Visa sont traités par Visa et les flux MasterCard sont traités par MasterCard à un petit nombre d'exceptions près.

En d'autres termes, si la séparation fonctionnelle entre le *scheme* de cartes de paiement et les entités de traitement semble bien assurée et emporte des conséquences du point de vue de la comptabilité, de l'organisation, des processus décisionnels et de la facturation des prestations, la concurrence envisagée par le considérant (33) n'est pas effective. L'un des *schemes* internationaux rencontrés par la mission plaide à cet égard qu'une entité de traitement est sujette à autant de risques de conflits d'intérêts et de subventions croisées quand elle est liée à des banques que quand elle est liée à un *scheme*.

2.2.3.3 L'intérêt de la séparation entre le scheme et le processing

La séparation entre le *scheme* et le *processing* a été conçue par le législateur européen à des fins de renforcement de la concurrence et de baisse des coûts pour les commerçants. Mais il existe un autre intérêt à cette séparation, dans la perspective de ce rapport, c'est celui qui consiste à opérer une distinction dans l'activité des *schemes* internationaux de paiement par carte entre un rôle indubitablement international, celui de détermination des règles du *scheme*, et une activité de traitement des transactions de paiement, qui pourrait être soumise à une obligation de localisation sur le sol européen pour les transactions intra-européennes.

Ainsi, la séparation entre le *scheme* et le *processing*, qu'elle soit ou non renforcée à l'occasion de la révision du règlement 2015/751, contribue à faciliter la mise en œuvre de la localisation des données de paiement par les grands *schemes* internationaux de paiement par carte. Cette obligation de localisation peut en effet se traduire pour eux par le choix entre l'implantation de *datacenters* (stockage, traitement, duplication) sur le sol européen ou le recours à un prestataire européen chargé

---

[62] règlement délégué 2018/72 du 4 octobre 2017 complétant le règlement 2015/751 du Parlement européen et du Conseil relatif aux commissions d'interchange pour les opérations de paiement liées à une carte par des normes techniques de réglementation fixant les exigences que doivent respecter les schémas de cartes de paiement et les entités de traitement afin de garantir leur indépendance sur le plan comptable, organisationnel et décisionnel

[63] http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0279

du *processing* des transactions domestiques (c'est-à-dire intervenant entre un consommateur européen et un commerçant européen).

Le renforcement des capacités technologiques européennes en matière de paiement devrait progressivement conduire à ce que les plateformes de compensation et de règlement européennes, qui sont aujourd'hui souvent l'émanation de communautés bancaires nationales, se regroupent, ouvrent leur capital et élargissent leur activité à plusieurs Etats. Une consolidation de ces infrastructures et une plus grande autonomie par rapport aux banques pourrait leur ouvrir l'opportunité de jouer un rôle de sous-traitance des grands *schemes* internationaux pour le *processing* de leurs opérations intra-européennes.

2.2.3.4 L'exemple espagnol

i. il n'existe pas aujourd'hui de *scheme* national espagnol de paiement

De même qu'en France la création du Groupement des Cartes Bancaires CB a conduit en 1984 à un unique système national de paiement par carte, par le rapprochement des réseaux préexistants (Carte Bleue, Crédit Agricole et Crédit Mutuel), les trois systèmes espagnols de paiement par carte ServiRed, Sistema 4B et EURO 6000 ont annoncé leur fusion le 1er février 2018[64]. Ces trois sociétés, filiales de groupes bancaires, exerçaient les mêmes activités de gestion et de supervision d'un système de cartes de paiement, de distributeurs automatiques de billets et de terminaux de paiement. Pratiquement toutes les banques présentes en Espagne (émetteurs de cartes et/ou acquéreurs d'opérations de paiement) étaient affiliées à l'une des trois sociétés fusionnées.

A la différence de la situation française, ServiRed, Sistema 4B et EURO 6000 n'ont pas élaboré un ensemble de règles qui leur auraient été propres et qui constitueraient un ou plusieurs *schemes* domestiques, distincts de ceux de Visa et de MasterCard. Les cartes distribuées par les banques espagnoles ne sont pas co-badgées, mais portent la seule marque Visa ou MasterCard.

Comme l'expose l'analyse établie par l'autorité de la concurrence espagnole[65] « *en Espagne, seuls les systèmes de paiement internationaux (Visa et MasterCard) ont développé leurs propres applications de paiement qui leur permettent d'identifier les transactions effectuées avec eux* ». ServiRed, Sistema 4B et EURO 6000 (les SMP) « *ne constituent pas des systèmes complets de paiement par carte, car ils ne disposent pas de leurs propres applications de paiement, intégrant dans les instruments de paiement émis par leurs membres les applications de paiement Visa et MasterCard, qui constituent les seuls systèmes de paiement par carte quadripartite existant en Espagne. En ce sens, les SMP sont technologiquement dépendantes de ces systèmes internationaux, développant leur activité dans le*

[64] Cf communiqué de l'ECPA du 1er février 2018 : "*Green light to the merger of ServiRed, Sistema 4B and EURO 6000*" https://www.europeancardpaymentassociation.com/wp-content/uploads/2018/02/Green-Light-to-the-merger-of-ServiRed_Sistema-4B_-and_Euro-6000_press-release.pdf

[65] Points (48) et (49) du Rapport de la Comisión Nacional de los Mercados y la Competencia (CNMC), C/0911/17: SERVIRED/ SISTEMA 4B/ EURO 6000, Resolución del Consejo - Autorización 1ª fase con compromisos, 01 Feb 2018, https://www.cnmc.es/expedientes/c091117

domaine domestique des opérations de paiement effectuées avec des cartes Visa et MasterCard en Espagne. »

L'un des objectifs de la fusion consiste précisément à développer un *scheme* espagnol de paiement : *« le nouveau système a l'intention de développer sa propre application de paiement afin d'offrir aux prestataires de services de paiement un système national intégré de paiement par carte au sens de l'article 2, paragraphe 16, du règlement (UE) 2015/751, qui intègre tous les éléments nécessaires pour opérer, en tant que tel, sur le marché intérieur en concurrence avec des systèmes tiers, dont les systèmes internationaux Visa et MasterCard. Les émetteurs de cartes pourront alors intégrer les applications de paiement du nouveau système dans les instruments de paiement avec une ou plusieurs autres applications de paiement appartenant à d'autres systèmes de paiement (cobadging)*[66] ».

ii. les *schemes* internationaux n'assurent pas le *processing* de leurs opérations en Espagne

Une autre particularité de l'organisation des systèmes de paiement par carte en Espagne tient à ce que le *processing* des transactions de paiement par carte, alors même que ces transactions reposent principalement sur les *schemes* Visa ou MasterCard, est assuré à plus de 90 % par la société Redsys[67], entreprise spécialisée dans le traitement et les services liés aux processus de paiement par carte bancaire et mobile, filiale des grands groupes bancaires espagnols.

Redsys présente un grand nombre de points communs avec STET en France ; mais alors que STET gère exclusivement les relations entre banques émettrices et banques acquéreurs selon les règles du *scheme* domestique GIE CB, Redsys prend en compte les différents types de règlements entre les principaux réseaux de systèmes de paiement espagnols et internationaux : ServiRed, Sistema 4B, les règlements inter-réseaux, Visa, MasterCard, Amex, JCB, CUP[68]...

Le cas espagnol est intéressant à plusieurs titres :

- **il semble mettre en évidence à une échelle significative la possibilité effective d'une séparation entre des *schemes* internationaux de paiement par carte et le *processing* de leurs opérations, conformément à l'article 7 du règlement 2015/751 ;**
- **l'organisation du marché des paiements espagnol semble assurer une localisation sur le territoire européen des données correspondant aux paiements domestiques, sans que les *schemes* internationaux aient été contraints à des investissements disproportionnés et, sous réserve de données statistiques probantes, avec de bonnes performances de lutte contre la fraude[69] ;**
- **le rapprochement des systèmes de paiement par carte intervenu en Espagne pourrait constituer une source d'inspiration pour un rapprochement des systèmes nationaux de paiement par carte en Europe.**

[66] Id. points (73) et (74)

[67] Id. point (81)

[68] Cf. le site de Redsys http://www.redsys.es/en/entidades.html

[69] Redsys se targue de contribuer à faire de l'Espagne un des pays où le taux de fraude serait le plus bas dans le monde.

2.2.3.5 Autres exemples de séparation

Visa a confirmé à la mission que les commerçants ou les banques acquéreurs ont la possibilité de déléguer le traitement de transactions Visa nationales (à l'intérieur d'un Etat membre de l'EEE) ou intra-européennes (au sein de l'EEE). Plusieurs exemples nous ont été donnés :

- Redsys (Espagne) et SIA (Italie), processeurs nationaux affiliés à des banques locales, assurent le *processing* de transactions Visa ;
- Trionis, filiale bruxelloise de banques de détail de neuf pays européens et du Groupe des caisses d'épargne européennes, développe, maintient et exploite des services de paiement internationaux pour l'industrie financière ; elle assure le traitement transfrontalier de transactions Visa en Europe ;
- plusieurs banques peuvent avoir un accord commercial avec un même processeur tiers (traitement *on-we*), par exemple Equens Worldline (BeNeLux / Autriche) ;
- lorsqu'une banque ou un groupe de banques est à la fois émetteur et accepteur d'une transaction de paiement par carte, elle peut assurer elle-même le traitement de de ces transactions *on-us*.

Recommandation n° 2.	En cohérence avec la Recommandation n° 1, saisir l'opportunité de la prochaine révision du règlement 2015/751 (interchanges) pour préciser que les entités de traitement (au sens de l'article 7) sont tenues de localiser les données de paiement sur le sol européen.

2.2.4 L'alignement des modèles d'affaires de la carte et de l'*instant payment*

Le règlement est issu d'un combat acharné des autorités européennes de la concurrence contre le principe des commissions d'interchange. L'argumentaire de la Commission européenne est résumé dans les considérants (10) et (11) du règlement 2015/751 :

« *Les commissions d'interchange sont généralement appliquées entre les prestataires de services de paiement acquéreurs et émetteurs de cartes appartenant à un schéma de cartes de paiement donné. Les commissions d'interchange constituent une partie importante des frais facturés aux commerçants par les prestataires de services de paiement acquéreurs pour chaque opération de paiement liée à une carte. Les commerçants, à leur tour, répercutent ces coûts liés aux cartes, comme tous leurs autres coûts, sur le prix global de leurs biens et services. La concurrence entre les schémas de cartes de paiement visant à convaincre les prestataires de services de paiement d'émettre leurs cartes entraîne une hausse, et non une baisse, des commissions d'interchange sur le marché, contrairement à l'effet de discipline sur les prix que la concurrence exerce habituellement dans une économie de marché*[70] […].

La grande diversité existante des commissions d'interchange et leur niveau empêchent l'apparition de nouveaux acteurs présents dans toute l'Union sur la base de modèles économiques caractérisés par des commissions d'interchange plus faibles ou nulles, au détriment des économies d'échelle et de gamme qui pourraient être réalisées et des gains d'efficacité qui pourraient en résulter. Cela a des incidences

[70] Cet argument repose sur les travaux fondateurs de l'Ecole d'Economie de Toulouse sur les marchés bifaces, dont les systèmes de paiement par carte représentent un archétype, cf. "*Platform Competition in Two-Sided Markets*", Jean-Charles Rochet, and Jean Tirole, Journal of the European Economic Association, vol. 1, n. 4, June 2003, pp. 990–1029 ; "*Must-take cards and the Tourist Test*" J.-C. Rochet et J. Tirole (2008) ; « *Payment card regulation and the use of economic analysis in antitrust* », J.Tirole (2011)
https://www.tse-fr.eu/articles/platform-competition-two-sided-markets
http://idei.fr/doc/wp/2008/must_take_cards.pdf
http://idei.fr/doc/by/tirole/tsenotes4.pdf

négatives sur les commerçants et les consommateurs et entrave l'innovation. Le fait que les acteurs présents dans toute l'Union devraient proposer aux banques émettrices au minimum le plus haut niveau de commissions d'interchange pratiqué sur le marché auquel ils souhaitent accéder conduirait aussi au maintien de la fragmentation du marché. Les schémas nationaux existants qui appliquent des commissions d'interchange inférieures ou nulles peuvent également être contraints de quitter le marché en raison de la pression exercée par les banques en vue de tirer des revenus plus élevés desdites commissions d'interchange. En conséquence, les consommateurs et les commerçants sont confrontés à un choix restreint, à une hausse des prix et à une baisse de la qualité des services de paiement, tandis que leur capacité à recourir à des solutions de paiement applicables à toute l'Union est également limitée […] ».

Les préventions de la Commission contre le principe des commissions d'interchange sont telles qu'un autre règlement établissant des exigences techniques et commerciales pour les virements et les prélèvements en euros a proscrit les commissions d'interchange dans les termes suivants : « *il est important d'assurer la sécurité juridique dans le secteur des paiements en ce qui concerne les modèles économiques relatifs aux prélèvements. Il est essentiel de réglementer les commissions multilatérales d'interchange (CMI) pour les prélèvements afin d'assurer des conditions neutres de concurrence entre les prestataires de services de paiement, permettant ainsi le développement d'un marché unique des prélèvements* […]. *Il serait donc utile, pour créer un véritable marché européen des prélèvements, d'interdire les CMI par opération »* à l'exception éventuelle et sous conditions des transactions *« qui sont rejetées, refusées, retournées ou rectifiées ou reversées à défaut de pouvoir être exécutées correctement, ou qui font l'objet d'un traitement exceptionnel*[71] ».

En définitive, le règlement 2015/751 a plafonné les commissions d'interchange applicables aux paiements par carte à 0,2 % de la valeur de l'opération pour toute opération liée à une carte de débit et à 0,3 % de la valeur de l'opération pour toute opération liée à une carte de crédit. Mais cette décision est présentée comme dérogatoire et temporaire (les considérants (66) et (84) de la DSP2 indiquent à cet égard que « *le règlement (UE) 2015/751 impose des limites sur le niveau de commissions d'interchange. Ces limites s'appliqueront avant d'être interdites par la présente directive* » et que « *l'emploi de méthodes de tarification non transparentes devrait être interdit* »).

> **La mission estime que le plafonnement à 0,2 ou 0,3 % des commissions d'interchange permet de répondre au moins à court terme aux réserves de la Commission à l'égard du principe de telles commissions multilatérales et qu'il n'est pas nécessaire de diminuer davantage ces plafonds. Mais il ne faudrait pas que cette disposition favorable au modèle d'affaire du paiement par carte entrave l'émergence et le développement de systèmes de paiement plus innovants et plus européens fondés sur le paiement instantané. Il convient donc d'assurer des conditions neutres de concurrence entre un paiement par carte traditionnel et d'autres formes de règlements qui se déboucleraient par un paiement instantané, lesquelles devraient également pouvoir donner lieu au même plafond autorisé de commissions d'interchange.**

La comparaisons entre différents modes opératoires peut toutefois être compliquée par les particularités de chacun : le paiement par carte est un paiement tiré, à l'initiative du commerçant, basé sur une compensation quotidienne ; le paiement par carte est sous-tendu par un ensemble de contrats (entre le client et la banque émettrice, entre le commerçant et la banque acquéreur, entre les banques

[71] Règlement 260/2012 du 14 mars 2012 établissant des exigences techniques et commerciales pour les virements et les prélèvements en euros, considérant (20)

via les *schemes*...) et ces contrats comportent, au-delà du traitement de la transaction, des notions de garantie (transfert de responsabilité, lutte contre la fraude, garantie de règlement...) et de services (assurance, conciergerie...).

2.3 Tirer le meilleur parti des techniques de tokenisation

L'analyse des enjeux propres à la *tokenisation* constitue un objectif explicite de la nouvelle stratégie nationale sur les moyens de paiement. Celle-ci indique en effet que « *la gestion et la génération des* tokens *se font en large majorité à l'heure actuelle en dehors de l'Union européenne, ce qui rend l'ensemble des acteurs européens de la chaîne de paiement potentiellement dépendants de décisions prises par des acteurs, répondant à des cadres juridiques très différents des exigences définies par l'Union Européenne* ». L'un des points d'action prévus consiste à approfondir les questions de sécurité posées par la gestion des *tokens* et de toute autre donnée similaire, notamment en lien avec les problématiques de données personnelles.

2.3.1 Les différents cas d'utilisation de la *tokenisation*

La *tokenisation* désigne des techniques consistant à substituer à des données sensibles de paiement, telles qu'un numéro de compte (IBAN) ou de carte bancaire (PAN), un pseudonyme appelé *token*. La sécurité apportée par la création d'un *token* tient à la difficulté, voire à l'impossibilité, de reconstituer les données sensibles d'origine (« *de-tokenisation* »). La *tokenisation* fait jouer un rôle important à un acteur chargé d'assurer la conversion entre les données de paiement sensibles et leur substitut : le *token service provider* (TSP). Grâce à ces techniques, on limite la circulation et l'exposition des données sensibles, pour des raisons tant de prévention de la fraude que de confidentialité.

Dans le champ du paiement par carte, on désigne sous le vocable de *tokenisation* deux techniques assez différentes :

- un site marchand (en pratique, l'acquéreur, le commerçant ou le fournisseur de services d'un commerçant) peut choisir de ne pas conserver les numéros de carte bancaire de ses clients, mais de leur substituer systématiquement un ***token* de sécurité** ;

- les ***tokens* de paiement** visent à substituer au numéro de carte bancaire, non seulement dans l'environnement acquéreur, mais aussi sur toute la chaîne de paiement, un numéro de même format ; correspondant en quelque sorte à une sous-carte et ne permettant un paiement que dans un contexte spécifique (paiement initié à partir d'un certain *smartphone*, paiement au profit d'un certain e-commerçant...).

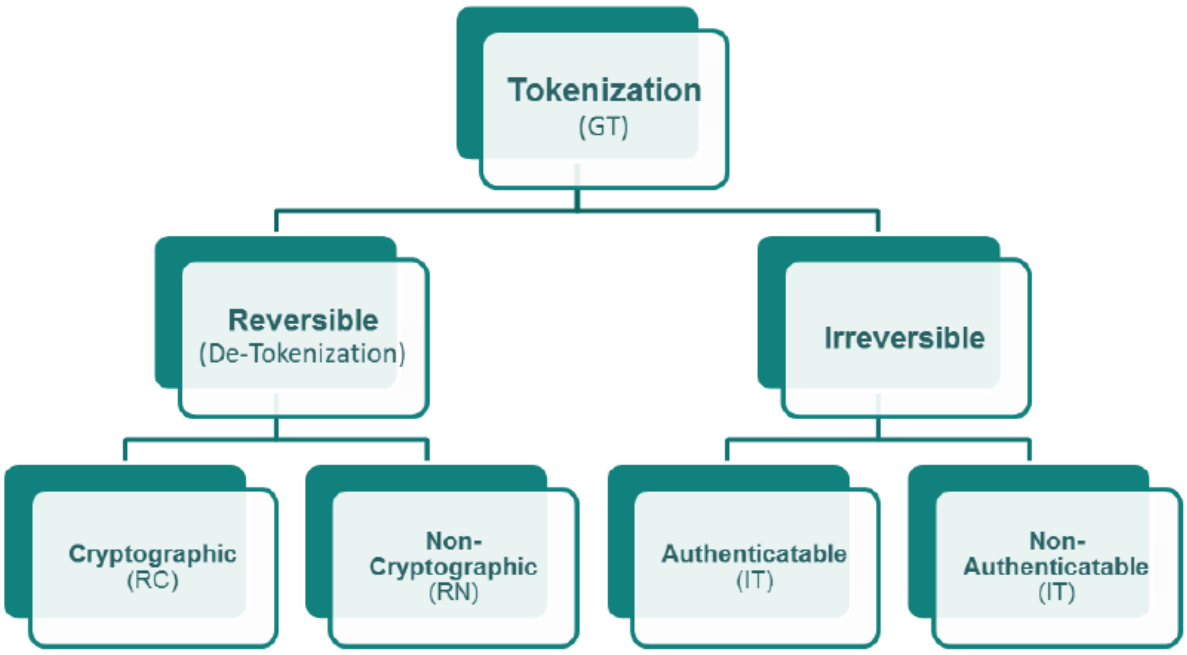
2.3.1.1 Les tokens *de sécurité (« acquirer tokens » ou « security tokens »)*

Les *tokens* de sécurité permettent aux commerçants et à leurs éventuels sous-traitants de conserver et de gérer dans de meilleures conditions de sécurité les données de paiement de leurs clients, en occultant les numéros de cartes bancaires[72]. Le *token* et les caractéristiques du paiement peuvent être échangés entre les commerçants, les passerelles de paiement, les processeurs et les acquéreurs avec des risques limités d'indiscrétion. Le *token* facilite l'analyse par les commerçants des habitudes d'achat de leurs clients et sécurise les paiements récurrents (dans le cadre d'un abonnement ou d'une offre *premium* offrant le paiement en « *1-click* »).

[72] Cf. à cet égard l'article 6 de la délibération n° 2018-303 du 6 septembre 2018 de la CNIL portant adoption d'une recommandation concernant le traitement des données relatives à la carte de paiement en matière de vente de biens ou de fourniture de services à distance : « *Des mesures d'obfuscation (masquage de tout ou partie du numéro de la carte lors de son affichage ou de son stockage) ou de remplacement du numéro de carte par un numéro non signifiant (*tokenisation*) doivent être mises en œuvre afin de limiter l'accès aux numéros de cartes.* »

Les *tokens* de sécurité ont habituellement la forme de longues chaînes de caractères, sans lien apparent avec le numéro de carte d'origine. Seule l'entité qui fournit le service de *tokenisation*, le *token service provider*, détient le numéro de carte bancaire et sait assurer dans un sens et éventuellement dans l'autre la conversion entre ce numéro et le *token*. Lorsque le commerçant reçoit un nouveau paiement d'un client sur lequel il détient un *token*, le TSP peut remplacer le *token* par le numéro de carte d'origine et transmettre l'ordre de paiement à la banque acquéreur.

Toutes les entités qui stockent, traitent ou transmettent des données de paiement par carte sont soumises à des normes exigeantes de sécurité des données de paiement, élaborées par le *Payment Card Industry Security Standards Council*[73] : les *Payment Card Industry Data Security Standards* (PCI DSS). Le recours par un commerçant aux *tokens de sécurité* constitue un moyen de faciliter leur conformité à ces normes. C'est l'objet des *Payment Card Industry Tokenisation Security Guidelines*[74] que de compléter les normes PCI DSS et de présenter les meilleures pratiques mises en œuvre par les commerçants ou leurs prestataires de services.



Ces *guidelines* établissent une typologie des procédés de *tokenisation* d'acquisition. En premier lieu, les *tokens* peuvent ou non permettre de reconstituer la donnée de paiement sensible d'origine. Les procédés de *tokenisation* dits **réversibles**, qu'ils soient basés sur des techniques cryptographiques ou sur de simples tables de correspondance, ouvrent la possibilité de *dé-tokeniser* un jeton. En revanche,

---

[73] Le PCI Security Standards Council (PCI SSC) joue un rôle essentiel dans l'industrie du paiement par carte, en établissant les exigences techniques et opérationnelles de sécurité imposées aux organisations acceptant ou traitant des transactions de paiement, ainsi qu'aux développeurs de logiciels et aux fabricants d'applications et d'appareils utilisés dans ces transactions. Il est régi par American Express, Discover, JCB International, MasterCard et Visa.

[74] "*Information supplement: PCI DSS Tokenization Guidelines*" PCI DSS Version 2.0, August 2011
https://www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf?agreement=true&time=1578521035819
"*Tokenization Product Security Guidelines - Irreversible and Reversible Tokens*" Version 1.0, April 2015
https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf?agreement=true&time=1578521035811
ces documents ne doivent pas être confondus avec « *PCI TSP Security Requirements* », qui ne s'applique pas aux *tokens* d'acquisition mais aux *tokens* de paiement (cf. plus loin chapitre 2.3.1.2 et note 77)

d'autres techniques de *tokenisation*, dites **irréversibles**, ne permettent, par aucun moyen technique et par qui que ce soit, de reconstituer la donnée d'origine à partir du *token*. La *tokenisation* irréversible présente habituellement la propriété d'être authentifiable : un jeton irréversible authentifiable est l'image par une fonction mathématique « à sens unique » de la donnée de paiement sensible que l'on souhaite occulter. Cette fonction produit des résultats reproductibles, mais elle ne peut pas être inversée pour *dé-tokeniser* le jeton obtenu et reconstituer la donnée de paiement sensible d'origine.

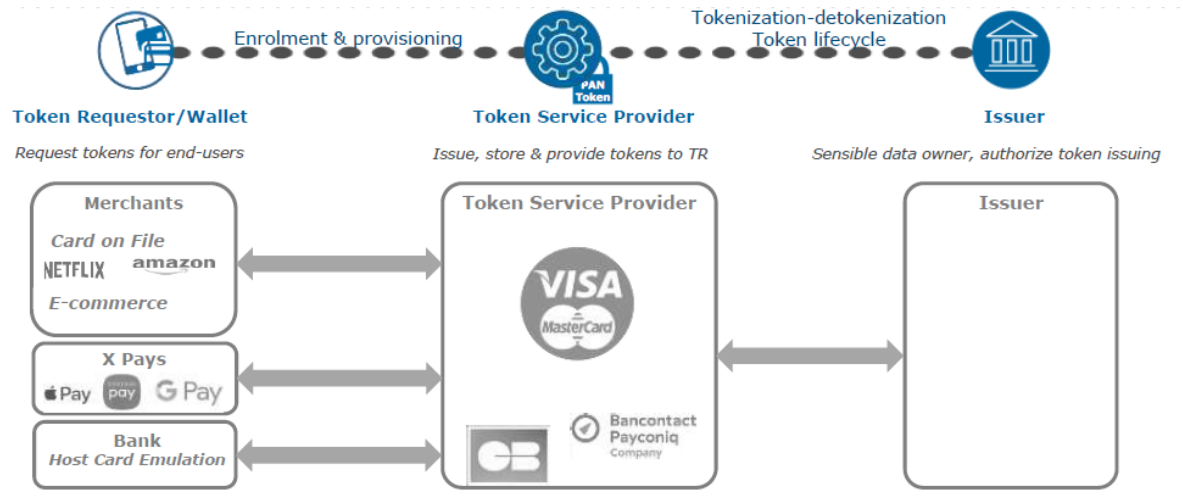
Un procédé de *tokenisation* irréversible et authentifiable permet ainsi à un commerçant de conserver la trace des ventes qu'il a effectuées sans craindre la divulgation des numéros de cartes bancaires de ses clients. Personne ne peut reconstituer à partir des *tokens* qu'il conserve les numéros des cartes utilisées. Mais un client qui, ayant perdu son ticket de caisse, souhaite obtenir un remboursement ou faire jouer une garantie peut apporter la preuve qu'il est bien à l'origine d'un achat : le commerçant peut vérifier que la carte de paiement du client génère le même *token* que celui qu'il a conservé.

> **Les *tokens* de sécurité présentent beaucoup d'avantage en termes de sécurité des systèmes d'information. Leur emploi est recommandé par les normes de sécurité PCI DSS et par la CNIL. Sous l'angle du présent rapport et dans la perspective dessinée par la Recommandation n° 1, les données de vente conservées par les commerçants et par leurs sous-traitants devraient être localisées sur le territoire européen dès lors qu'elles comportent des données de sécurité personnalisées, telles qu'un numéro de carte bancaire ou un *token* réversible.**

Sous réserve d'analyses complémentaires et dans des conditions à préciser, cette obligation de localisation pourrait être levée dans le cas où les données de paiement personnalisées seraient occultées par le recours à un dispositif de *tokenisation* irréversible.

2.3.1.2 Les tokens de paiement (les « payment tokens »)

A la différence des *tokens* de sécurité, dont le bénéfice est restreint à **l'environnement constitué par un commerçant et ses éventuels sous-traitants** et cesse lorsqu'un nouveau paiement est introduit dans le circuit de paiement, les *tokens* de paiement ont vocation à se substituer aux données de paiement personnalisées (l'exemple emblématique étant celui du numéro de carte bancaire) **tout au long du circuit de paiement**, jusqu'à ce que, en bout de chaîne, la banque émettrice ait besoin de convertir le *token* de paiement (en demandant au *token service provider* sa *de-tokenisation*) afin de savoir quel compte de paiement elle doit débiter.



Le recours aux *tokens* de paiement consiste donc à substituer à un numéro de carte bancaire **un alias qui présente les mêmes caractéristiques de format** et qui sera véhiculé dans les systèmes de paiement à la place du numéro de carte bancaire. Un *token* de paiement offre par ailleurs une protection d'autant plus forte que sa validité est restreinte à un contexte de paiement spécifique, lié par exemple à un site de e-commerce, à un terminal mobile (*smartphone*, tablette…), ou encore à une unique opération de paiement. L'existence de tels contrôles d'utilisation (*token domain restriction controls*), qui limitent l'utilisation d'un token de paiement à son utilisation prévue, est une caractéristique essentielle et un intérêt important des *tokens* de paiement.

Le recours aux *tokens* de paiement apporte donc une double sécurité : le numéro de carte ne circule plus qu'entre le *token service provider* et la banque émettrice (comme le met en évidence le schéma ci-dessus[75]) et le *token* est invalide hors du contexte pour lequel il a été créé. Alors que la technique des *tokens de sécurité* ne repose pas sur une approche standardisée et donne lieu à une multitude d'offres de service, dans lesquelles le format et les modalités de gestion des *tokens* sont variables, les *tokens* de paiement font l'objet de spécifications édictées par EMVCo[76] et par PCI SSC[77], ainsi que de recommandations émanant d'une *task force* constituée sous l'égide de l'*european cards stakeholders* group (ECSG)[78].

L'*european cards stakeholders group* a recommandé que l'émetteur soit libre de choisir son fournisseur pour le rôle de *payment token service provider*, sous réserve de l'approbation par le *scheme* de paiement, et plusieurs acteurs s'étaient préparés à offrir ce service de *payment token service provider*. Mais ils en ont manifestement été dissuadés : Visa offre la seule solution de *tokenisation* compatible avec son *scheme*, MasterCard offre la seule solution de *tokenisation* compatible avec le sien.

Au-delà d'un enjeu de concurrence sur l'octroi d'un nouveau service, il existe aussi un enjeu de remise en cause de l'équilibre des rôles entre les *schemes* et les banques émettrices. Dans la situation actuelle, les *schemes* internationaux concèdent des plages de numéros de comptes aux banques émettrices, qui sont libres de l'usage qu'elles en font (fabrication, personnalisation des cartes, co-badging…), à charge simplement pour elles d'en informer les *schemes*.

---

[75] Ce schéma est issu d'une présentation aimablement réalisée pour les besoins de la mission par EquensWorldline

[76] EMVCo est une émanation des six *schemes* suivants : American Express, Discover, JCB, Mastercard, UnionPay et Visa. Elle élabore les spécifications EMV®, qui visent à améliorer l'interopérabilité et l'acceptation des transactions de paiement par carte dans le monde. Les spécifications portent notamment sur l'évaluation des cartes et des terminaux, l'évaluation de la sécurité et la gestion des problèmes d'interopérabilité, la *tokenisation* des paiements et 3-D Secure. Les spécifications désignées ici sont "*EMV® Payment Tokenisation Specification: Technical Framework Version 2.1*" et "*EMV® Payment Tokenisation: A Guide to Use Cases Version 1.0*", 14 June 2019 https://www.emvco.com/emv-technologies/payment-tokenisation/

[77] "*Payment Card Industry (PCI) Token Service Providers – Additional Security Requirements and Assessment Procedures for Token Service Providers (EMV Payment Tokens)*" Version 1.0, December 2015 https://www.pcisecuritystandards.org/documents/PCI_TSP_Requirements_v1.pdf?agreement=true&time=1578829381110

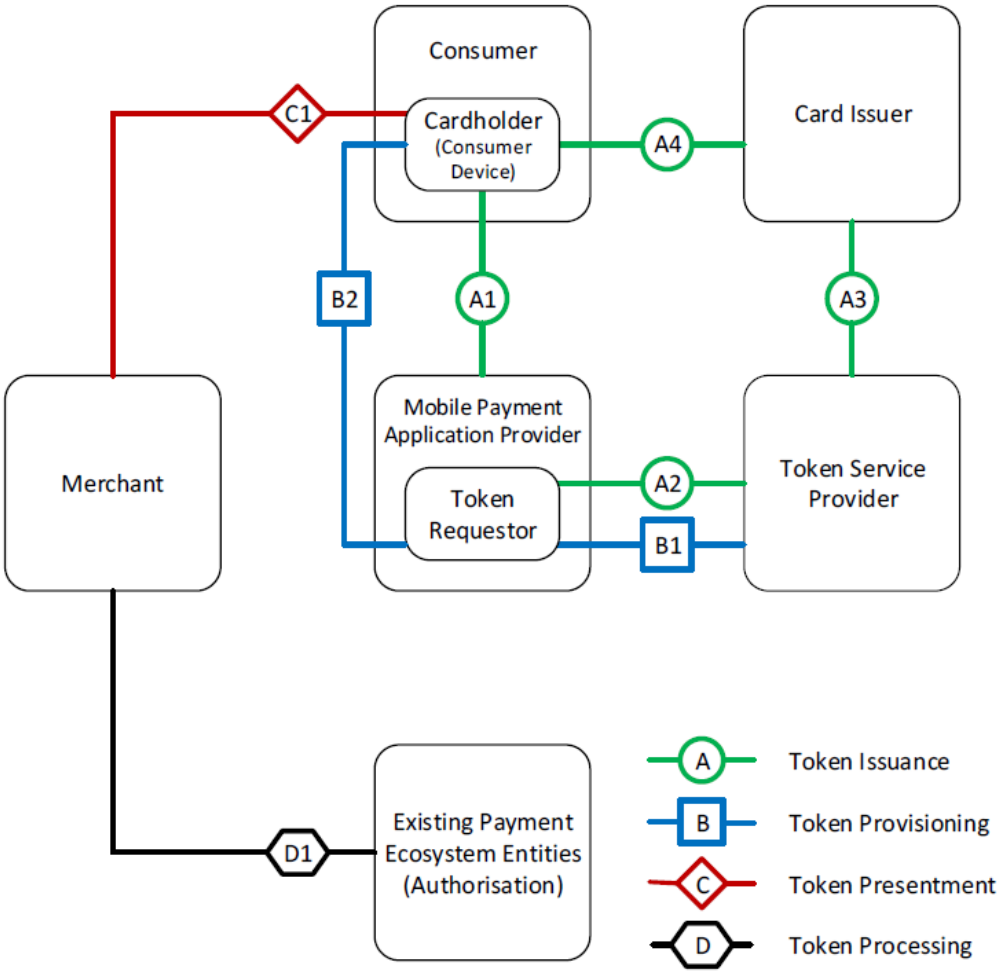
[78] L'ECSG est une association à but non lucratif qui promeut l'harmonisation du paiement par carte dans l'espace unique de paiement en euros (SEPA). L'ECSG est composé de représentants de cinq secteurs de la chaîne de paiement par carte : détaillants / grossistes, fournisseurs (carte, dispositifs de paiement, systèmes informatiques connexes), processeurs de transactions par carte, *schemes* et prestataires de services de paiement. L'objectif de l'ECSG est que les citoyens de l'UE puissent procéder à des paiements par carte et à des retraits DAB avec la même facilité dans tout l'espace SEPA, en éliminant les obstacles techniques, pratiques et commerciaux à l'harmonisation du paiement par carte. Il poursuit cet objectif à travers la maintenance et l'évolution du « *SEPA Cards Standardisation Volume (the Volume)* », un document définissant des lignes directrices pour la normalisation, l'interopérabilité et la sécurité des cartes en Europe. L'ECSG ne fait pas partie du cadre institutionnel de l'UE, mais sa création est soutenue par les institutions de l'Union européenne, qui participent à ses travaux en tant qu'observateurs. Les recommandations relatives à la *tokenisation* (« *Tokenisation Considerations for SEPA Card Payments* ») ont donné lieu à une consultation publique entre le 17 décembre 2018 et le 29 mars 2019, la version finale n'a pas encore été rendue publique.

Surtout, STET affirme qu'aucune décision d'une autorité étrangère ne serait susceptible, techniquement ou juridiquement, de l'empêcher de procéder en France au traitement d'une transaction CB sur une carte physique co-badgée. En revanche, si la *tokenisation* d'une carte ne peut être effectuée que sous le contrôle exclusif de Visa ou de MasterCard, elle donne à ces *schemes* un pouvoir sur le cycle de vie et sur l'utilisation de la carte (ou plutôt de son alias dématérialisé) qu'ils n'ont pas aujourd'hui sur la carte physique. Par l'émission d'un *token*, la carte sort de la sphère de souveraineté européenne. Toutefois, la portée de cette difficulté est réduite dans le cas d'une carte co-badgée si, chaque fois qu'elle est *tokenisée*, deux *tokens* sont émis, correspondant l'un au *scheme* international, l'autre au *scheme* domestique (cf. ci-dessous, p. 51, dans un cas particulier important, la Recommandation n° 4).

Par ailleurs, en cohérence avec la Recommandation n° 1, il serait légitime d'exiger la localisation sur le sol européen des *token service providers* si ces entités ont accès, lorsqu'elles assurent une opération de *de-tokenisation*, à l'ensemble des données de paiement liées à chaque transaction.

2.3.2 La *tokenisation* de paiement permet la dématérialisation de la carte de paiement

2.3.2.1 Le principe d'une transaction dématérialisée



L'un des cas d'usages de la *tokenisation* de paiement, détaillé dans "*EMV® Payment Tokenisation: A Guide to Use Cases Version 1.0*", est celui de la dématérialisation d'une carte bancaire dans un terminal mobile (tablette ou *smartphone*). La documentation EMVCo[79] détaille un exemple dans lequel un *smartphone* est utilisé pour un achat dans un commerce physique, en paiement sans contact. Les interactions sont représentées sur le schéma ci-dessous.

Le titulaire de la carte, par l'intermédiaire de son *smartphone*, sollicite préalablement à l'achat, auprès d'un fournisseur d'applications de paiement mobile, l'émission d'un *token* de paiement (A1 à A4 en vert sur le schéma). Le *token service provider* et la banque émettrice (*card issuer*) procèdent à la création d'un *token* dont le numéro, qui ressemble à un numéro de carte, est enregistré sur le *smartphone* ou sur un serveur distant (B1 et B2, en bleu). Le consommateur a alors dématérialisé sa carte bancaire et peut commencer à l'utiliser.

Il présente son *smartphone* (comme il l'aurait fait avec sa carte bancaire) devant le terminal de paiement sans contact du commerçant (C1, en rouge), de sorte que le prestataire d'acceptation technique du commerçant reçoit le jeton de paiement et les données connexes communiquées par le *smartphone*. Dès lors, le terminal de paiement acquiert la transaction de paiement et en transmet les caractéristiques à la banque acquéreur, exactement comme si le *token* était un numéro de carte ordinaire (D1, en noir). De manière très semblable, un paiement à distance peut être effectué par l'intermédiaire du *smartphone*[80].

2.3.2.2 Les premiers cas de dématérialisation de cartes co-badgées

La documentation élaborée par EMVCo, organisme dans lequel les intérêts européens sont peu représentés, n'évoque pas le cas des cartes co-badgées. Le dispositif détaillé ci-dessus a vocation à s'appliquer dans le cas d'une carte mono-marque, par exemple *Visa-only* ou *MasterCard-only*. Les premières offres de cartes dématérialisées en France, à la connaissance de la mission, remontent à l'été 2016, date à laquelle Carrefour Banque et le groupe BPCE ont annoncé[81] la possibilité pour leurs clients respectifs de recourir à Apple Pay.

Pour BPCE, l'intérêt en termes d'image d'une telle annonce a primé sur celui de perpétuer les équilibres existant entre Visa et le groupement Carte Bancaire. En effet, à cette date, Visa avait mis en place une solution de *tokenisation* de paiement, mais pas le groupement Carte Bancaire ; en outre les modalités d'adaptation de la *tokenisation* au cas d'une carte co-badgée restaient à définir.

Dès lors, la dématérialisation sur un iPhone d'une carte Visa / CB émise par une banque du groupe BPCE conduisait à transformer une carte physique co-badgée en une carte dématérialisée *Visa-only*. Les transactions domestiques, traitées jusque-là par le GIE CB et par STET, par l'effet de la dématérialisation, étaient vouées à basculer sur le *scheme* Visa.

Plus généralement, les solutions *X-Pay* de dématérialisation des cartes physiques (Apple Pay, Google Pay, Samsung Pay…) pouvaient apparaître comme une menace sérieuse de perte de parts de marché pour des *schemes* nationaux tels que le groupement Carte Bancaire, comme un important levier de développement pour des *schemes* internationaux tels que Visa ou MasterCard, comme un risque

---

[79] "*EMV® Payment Tokenisation: A Guide to Use Cases Version 1.0*", 14 June 2019, Use Case 1: Proximity at Point of Sale

[80] "*EMV® Payment Tokenisation: A Guide to Use Cases Version 1.0*", 14 June 2019, Use Case 3: In-Application using a Consumer Device

[81] Cf. communiqués de Carrefour du 13 juin 2016 : « *Apple Pay arrive dans les magasins Carrefour en France dès cet été pour mieux satisfaire ses clients et leur offrir un moyen de paiement simple, rapide et sécurisé* » et du groupe BPCE du 16 juillet 2016 : « *Apple Pay disponible pour les clients Banque Populaire* »
https://www.carrefour-banque.fr/sites/default/files/_files/telechargement/Apple Pay-communique-presse-FR.pdf
https://newsroom.groupebpce.fr/actualites/apple-pay-disponible-pour-les-clients-banque-populaire-26b6-7b707.html

d'atteinte à la diversité des systèmes de paiement et comme un facteur de concentration du marché sur un petit nombre d'acteurs extra-européens.

Sous l'angle de la circulation des données, Apple affirme que la solution de paiement Apple Pay a été conçue pour minimiser les flux de données personnelles. Les données de paiement personnalisées (telles que le numéro de carte bancaire) ne sont pas stockées, ni dans l'appareil ni dans les serveurs d'Apple. Le *token* de paiement, qui permet de s'affranchir du numéro de carte bancaire, est enregistré dans un composant sécurisé (*secure element*), une puce dédiée intégrée à l'appareil. Un *token* de paiement doit être regardé comme un identifiant qui confère aux données auxquelles il est attaché le caractère d'une donnée personnelle au sens du RGPD et d'une donnée de paiement au sens du chapitre 2.1.1, p. 21. Mais lors d'un achat par Apple Pay, les données de paiement ne sont pas communiquées à Apple.

La mission n'a pas rencontré les autres fournisseurs de solutions de dématérialisation d'une carte bancaire sur un terminal mobile (Google, Samsung…). Certaines solutions *X-Pay*, à la différence d'Apple Pay, reposent sur le stockage du *token* de paiement sur le cloud plutôt que dans le *smartphone* ou la tablette. Tous les fournisseurs n'affichent pas la même absence d'intérêt qu'Apple à l'égard des données de paiement. Mais la mission, faute de les avoir rencontrés, ne peut rendre compte de leur réaction à l'idée d'une obligation de localisation des données de paiement sur le territoire de l'Union européenne.

Recommandation n° 3. En cohérence avec la Recommandation n° 1, veiller à ce que les solutions *X-Pay* de dématérialisation des cartes bancaires sur un terminal mobile (*smartphone*, tablette…) ne donnent pas lieu, à l'occasion d'une transaction intra-européenne, au transfert hors des frontières européennes de données de paiement.

2.3.2.3 L'état de l'art en matière de dématérialisation de cartes co-badgées

Quand BPCE a commercialisé Apple Pay, il n'existait pas de solution de *tokenisation* compatible avec le *scheme* Carte Bancaire. Les banques françaises ont alors mandaté STET et le GIE Cartes Bancaires pour développer conjointement une plate-forme industrielle permettant aux banques de déployer le paiement mobile de manière sécurisée. STET et le GIE CB se sont associés à IDEMIA (ex- Oberthur Technologie)[82], avec l'objectif de permettre aux clients des banques françaises de dématérialiser leurs cartes de paiement dans les portefeuilles électroniques de tous les fabricants de mobiles compatibles.

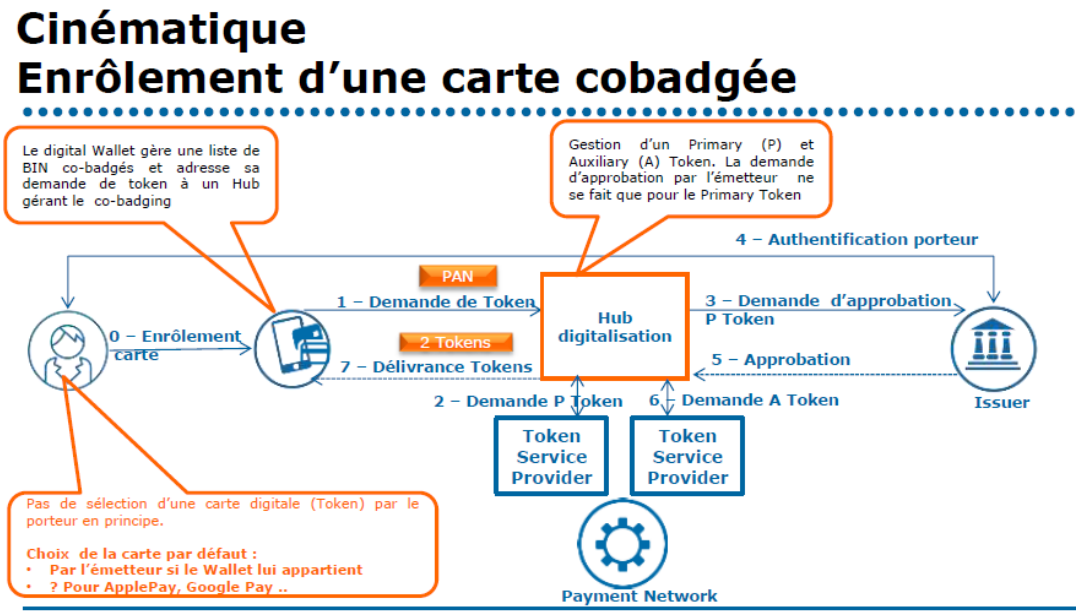
Le 14 février 2018, le groupe Société Générale a pu à son tour lancer Apple Pay. La solution retenue s'est s'appuyée sur la conception par STET d'un service de *tokenisation* de paiement (STET *Digital Solution*, ou SDS), basée sur la *digital enablement platform* (DEP) d'IDEMIA. L'implémentation d'Apple Pay dans les banques du groupe Société Générale respecte la dualité des cartes co-badgées : la dématérialisation sur un iPhone d'une carte émise par la Société Générale se traduit par la création et l'inscription dans le *secure element* de l'iPhone de deux *tokens* au lieu d'un seul, permettant l'un de procéder à un paiement selon le *scheme* Visa, l'autre selon le *scheme* Carte Bancaire.

Comme l'illustre le schéma ci-dessous[83], la dématérialisation d'une carte co-badgée, sensiblement plus compliquée que la dématérialisation d'une carte mono-marque, se traduit par la création d'un

[82] Cf. communiqué du 22 juin 2016 d'IDEMIA : « *Oberthur Technologie partenaire unique de STET et du GIE-CB pour déployer le paiement mobile en France* » https://www.idemia.com/fr/actualite/ot-partenaire-unique-de-stet-et-du-gie-cb-pour-deployer-le-paiement-mobile-en-france-2016-06-22

[83] Schéma extrait d'une présentation réalisée pour les besoins de la mission par EquensWorldline, que nous remercions pour son aide.

portefeuille digital (*digital wallet*) et par deux demandes successives de création d'un *token* de paiement auprès d'un *token service provider* (étapes 2 et 6), au titre de chacune des deux marques de la carte co-badgée. Seule la création du premier *token* donne lieu à l'authentification du porteur de la carte physique (étape 4), ce qui distingue le *primary token* de l'*auxiliary token*. Mais, dès que la dématérialisation de la carte co-badgée est réalisée par la délivrance des deux *tokens* (étape 6), les deux *schemes* de paiement sont complètement équivalents et le choix d'un *scheme* par défaut est librement paramétrable par l'utilisateur.



2.3.2.4 L'incertitude sur la portée du règlement interchange

Le règlement 2015/751 relatif aux commissions d'interchange proscrit dans le cas de cartes co-badgées toute mesure discriminatoire de routage des transactions, ainsi que tout mécanisme automatique, logiciel ou dispositif limitant le choix de la marque de paiement et/ou de l'application de paiement[84] (cf. chapitre 2.2.1 p. 33 et suivantes). Les rapporteurs comprennent que toute nouvelle banque qui viendrait à proposer à sa clientèle une solution *X-Pay* de dématérialisation des cartes bancaires qu'elle a émises devrait respecter, maintenant qu'il est disponible, le schéma de double *token*. Il leur semble également que les banques qui ont offert des systèmes de dématérialisation de cartes selon des modalités qui ne respectent pas une stricte équivalence entre les deux *schemes* devront se mettre en conformité avec l'article 8 du règlement.

Recommandation n° 4. Les banques émettrices de cartes co-badgées, qui associent deux *schemes* de paiement pour lesquels existent des services de *tokenisation*, devraient garantir que tout service permettant la dématérialisation de la carte sur un terminal mobile (*smartphone*, tablette…) donne lieu à la création de deux *tokens* de paiement et respecte une stricte équivalence entre les deux marques associées à la carte bancaire. Le législateur européen devrait, si nécessaire, préciser à cet effet l'article 8 du règlement 2015/751 lors de sa prochaine révision.

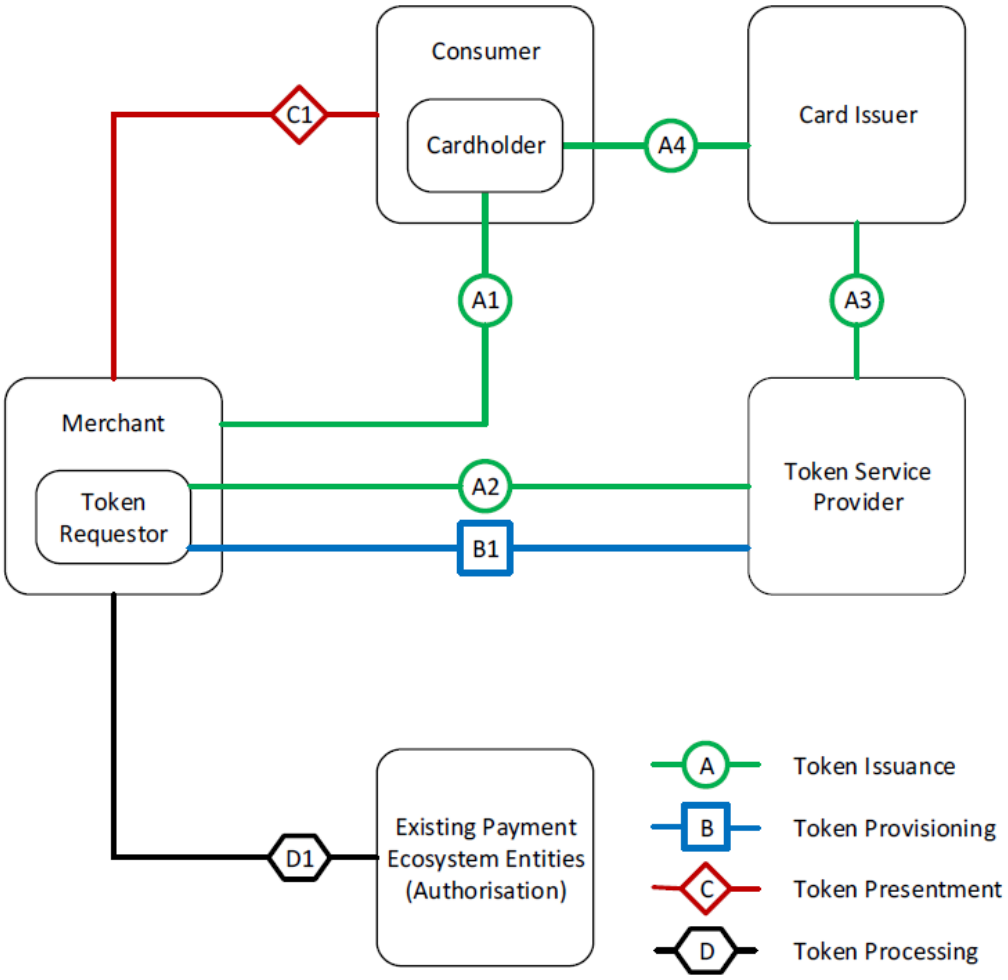
[84] Article 8 du règlement 2015/751 relatif aux commissions d'interchange

2.3.3 La *tokenisation* de paiement facilite pour les sites marchands la répétition des paiements

Le chiffre d'affaires d'un site de e-commerce se développe souvent sur une base de clients récurrents. Il existe un intérêt évident, pour favoriser la fidélité des clients et simplifier les actes d'achat, à ce que les clients ne doivent pas reporter à chaque nouvel achat leurs données de paiement personnalisées, telles que leur numéro de carte bancaire. On appelle transaction *card-on-file* une transaction dans laquelle un titulaire de carte a préalablement autorisé le commerçant à enregistrer, une fois pour toutes, ses informations de paiement. La possibilité de stocker des identifiants de paiement pour de futurs achats est une fonctionnalité essentielle du commerce électronique.

L'utilisation de *tokens de sécurité* réversibles (cf. chapitre 2.3.1.1, p. 44 et suivantes) offre un progrès appréciable en termes de sécurité, puisque les identifiants de paiement conservés par le commerçant ne sont plus directement exploitables par un tiers : une nouvelle transaction de paiement ne peut être acceptée par une banque acquéreur qu'après une opération de *dé-tokenisation* (qu'en principe le *token service provider* qui a créé le *token de sécurité* est seul capable de mener à bien).

La technique des *tokens* de paiement est beaucoup plus protectrice puisque, d'une part, la *dé-tokenisation* n'intervient qu'en toute fin du traitement du paiement, lorsque la banque émettrice de la carte a besoin de savoir à quel client elle doit imputer le débit ; et, d'autre part, l'utilisation du *token* de paiement est limitée à un appareil, un site marchand, un type de transaction ou un canal de paiement spécifique. Subsidiairement, le cycle de vie du *token* de paiement peut être différent de celui de la carte physique, notamment dans le cas où celle-ci est perdue, volée ou arrive à expiration.



La documentation EMVCo[85] présente l'utilisation des *tokens* de paiement dans la situation d'un achat en ligne (cf. schéma ci-dessus). Le consommateur entre lors d'un premier achat son numéro de carte bancaire (A1). C'est, à la différence du schéma de la page 48, le commerçant qui effectue ensuite une demande de *token* (A2 à A4). Le *token* de paiement est ensuite stocké par le commerçant (B1). Il peut être sélectionné par le consommateur (C1) lors de futurs achats. C'est le *token* de paiement, et non le numéro de carte bancaire, qui est alors véhiculé et traité dans le circuit de paiement (D1).

On peut toutefois noter qu'un obstacle à la facilitation des paiements répétés tient à l'entrée en vigueur de la deuxième directive sur les services de paiement (DSP2) et du règlement délégué qui en précise les dispositions relatives à l'authentification forte du client (cf. notes 57 et 58 p. 34).

L'article 97 de la DSP2 impose en effet aux prestataires de services de paiement d'appliquer l'authentification forte du client lorsque le payeur initie une opération de paiement électronique, l'authentification forte étant définie comme un dispositif d'authentification « *reposant sur l'utilisation de deux éléments ou plus appartenant aux catégories «connaissance» (quelque chose que seul l'utilisateur connaît), «possession» (quelque chose que seul l'utilisateur possède) et «inhérence» (quelque chose que l'utilisateur est) et indépendants en ce sens que la compromission de l'un ne remet pas en question la fiabilité des autres, et qui est conçue de manière à protéger la confidentialité des données d'authentification* ».

Selon les cas d'usage, la *tokenisation* de paiement est plus ou moins facile à concilier avec les exigences de la DSP2. Autant la dématérialisation d'une carte de paiement dans un *smartphone* se marie bien avec la mise en œuvre de l'authentification forte (l'utilisateur étant reconnu par la possession de l'appareil mobile et par un dispositif biométrique), autant la mise en œuvre de l'authentification forte est moins évidente dans le cas de paiements répétés sur un site de commerce en ligne.

> **A cet égard, les enjeux d'identification et d'authentification des consommateurs représentent un enjeu majeur, y compris sous l'angle de la souveraineté. Des plateformes nationales, telles que France Connect, pourraient bien un jour être concurrencées par des acteurs mondiaux, capables de reconnaître, voire de qualifier les consommateurs du monde entier. L'intérêt soulevé auprès d'Amazon, de Facebook, de Microsoft, de Paypal, de Visa, de MasterCard… par l'Alliance FIDO[86], qui élabore de nouveaux standards d'authentification, l'atteste.**

Par ailleurs, dans la perspective du présent rapport, un *token* de paiement devrait être considéré comme une donnée de sécurité personnalisée, au même titre qu'un numéro de carte bancaire. Les données qui lui sont rattachées devraient être considérées comme des données de paiement, c'est-à-dire qu'elles devraient être soumises à l'obligation de localisation sur le territoire européen.

---

[85] "*EMV® Payment Tokenisation: A Guide to Use Cases Version 1.0*", 14 June 2019, Use Case 4: Card-On-File E-Commerce

[86] https://fidoalliance.org/

2.4 L'élaboration d'un scheme européen de paiement

2.4.1 Plusieurs projets passés de création de nouveaux *schemes* de paiement

2.4.1.1 L'échec du projet Monnet[87]

En 2010, un consortium de 24 banques issues de 7 pays européens (Belgique, France, Allemagne, Italie, Portugal, Espagne et Grande-Bretagne) ont engagé sous le nom de projet Monnet une coopération visant à établir un système de paiement par carte qui aurait véritablement harmonisé le marché de la carte en Europe. Après une étude de faisabilité de plusieurs mois, les banques partenaires ont conditionné le lancement du projet à l'acceptation par la Commission européenne d'un niveau de commissions d'interchange qu'elles considéraient comme indispensable pour permettre le développement commercial et la rentabilité des investissements requis. Un communiqué de presse[88] à l'en-tête de « the Monnet project », publiait le 15 juin 2011 le plaidoyer suivant :

« Les 24 banques européennes associées au projet Monnet demandent à la Commission européenne de s'engager à apporter des clarifications quant à l'avenir des commissions multilatérales d'interchange (CMI).

Le projet Monnet favoriserait de manière durable la concurrence au sein du marché des paiements, établirait un marché domestique solide pour les paiements par carte en Europe et, in fine, favoriserait la compétitivité de l'économie européenne. Le projet Monnet est la contribution des grandes banques européennes à une mise en œuvre réussie du projet SEPA (single euro payments area - Espace unique de paiement en euros) en harmonisant les paiements, mais également en permettant une avancée importante vers un espace unique pour les paiements par carte bancaire, qui sont aujourd'hui à la traîne derrière les autres moyens de paiement utilisés dans le cadre du projet SEPA.

Le projet Monnet présente de nombreux avantages pour toutes les parties prenantes. D'abord, le principal objectif du projet est de maintenir les niveaux de service existants, tout en proposant des taux de CMI peu élevés pour les commerçants et les détenteurs de carte à l'échelle européenne. Ensuite, le projet Monnet réduirait significativement les fraudes et sécuriserait les paiements des détenteurs de carte et des commerçants. Enfin, Monnet serait un vecteur idéal d'innovation. A travers le projet Monnet, l'Europe profiterait des avantages d'un système unique et englobant de paiements innovants, tels que les paiements en ligne, les micro-paiements et les paiements sans contact pour tous les détenteurs de carte. En outre, la proposition de valeur du projet Monnet a été construite dans la perspective de répondre aux besoins des détenteurs de carte (identifiés sur la base de tests indépendants) et inclura des services à valeur ajoutée comme la possibilité de consulter son solde de compte courant sur les distributeurs automatiques, d'effectuer des paiements P2P ou des options d'épargne et, enfin, de souscrire à un programme de fidélité.

Après une étude de faisabilité de sept mois, les banques partenaires sont prêtes à lancer la carte Monnet, mais uniquement sous certaines conditions. Pour pouvoir compenser et justifier les investissements nécessaires, il est absolument indispensable de disposer d'un modèle économique viable, durable, clair et instaurant une certitude juridique quant aux revenus générés. L'incertitude en ce qui concerne les CMI reste le principal obstacle à l'investissement des banques dans le projet Monnet. Georges Pauget, président du projet Monnet, déclare : « Nous avons mené toutes les études de faisabilité nécessaires et nous savons comment mettre en œuvre Monnet. Mais nous ne pourrons mener à bien ce projet sans un modèle économique clair et durable de l'interchange en Europe. Nous aimerions, à travers un dialogue constructif avec la Commission européenne, avoir des réponses aux

---

[87] Extrait d'un rapport du Conseil Général de l'Economie de 2013

[88] http://www.fbf.fr/en/files/8HVAWC/Press_release_monnet_project_2011_EN.pdf

questions concrètes que nous nous posons. Si les banques n'ont pas de perspective claire sur la question des revenus, il sera impossible d'aller de l'avant ».

Mais malgré un intérêt de principe de la DG Marché intérieur, la DG Concurrence a répondu par une fin de non-recevoir à cette demande et a sonné le glas du projet, définitivement abandonné en mai 2012.

2.4.1.2 La création du scheme russe MIR

Après que plusieurs banques russes se sont vu refuser l'accès aux services des *schemes* américains VISA et MasterCard du fait des sanctions internationales prises à la suite de la crise ukrainienne (cf. ci-dessus, chapitre 1.1.3, p. 13), le président russe a déclaré le 27 mars 2014 que la Russie allait créer son propre système de paiement électronique. Ce service était destiné à constituer une alternative à l'offre des *schemes* américains qui contrôlaient alors 85 % des transactions par cartes de crédit et de débit effectuées en Russie.

MIR est un *scheme* de paiement national établi par la Banque centrale de Russie à la suite d'une loi adoptée le 1er mai 2017. MIR est principalement accepté par des sociétés basées en Russie, comme Aeroflot ou les chemins de fer russes, mais il commence à être également reconnu par des sociétés étrangères ayant des activités en Russie. Le système est exploité par une filiale de la Banque centrale de Russie.

Ce nouveau *scheme* de crédit a été conçu en 2016 pour pallier tout nouveau risque de blocage électronique des paiements. La Sberbank, première banque russe, a commencé à émettre des cartes en octobre 2016. À la fin de 2016, 1,76 million de cartes MIR avaient été émises par 64 banques, ce nombre atteint 69,8 millions en novembre 2019. MIR est promu par le gouvernement russe, la législation exigeant le paiement par ce moyen de l'aide sociale et des pensions[89].

2.4.2 Le projet EPI de nouveau *scheme* européen

En même temps que se tenaient les auditions qui ont conduit au présent rapport, et dans le contexte d'un marché mondial très évolutif (cf. notamment, parmi les transactions les plus récentes, le rachat du *third party provider* américain Plaid par Visa[90], l'investissement de Tencent dans la fintech Lydia[91] ou le rachat d'Ingénico par Worldline[92]), plusieurs grandes banques européennes mènent des discussions en vue de créer un nouveau système de paiement paneuropéen, alternatif à ceux proposés par les grands *schemes* américains (Visa, MasterCard) et chinois (China UnionPay, Alipay, WeChatPay). Plusieurs aspects du projet ont été éventés lors d'un colloque organisé le 5 novembre 2019 par la Revue Banque[93], donnant lieu par la suite à un communiqué de l'AFP et à des articles de presse[94].

---

[89] Source Wikipedia

[90] Cf. communiqué de presse de Visa : "*Visa To Acquire Plaid*", 13 January, 2020 https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.16856.html

[91] Cf. "*Lydia announces €40 million Series B funding led by Tencent, to create Europe's leading finance super-app*", 15 January, 2020 https://www.dropbox.com/s/h5agt8v1s98k7ur/Lydia%20PR%20fundraising%20January%2015%202020%20EN.pdf?dl=0

[92] Cf. "*Creation of a new world-class leader in payment services Worldline to acquire Ingenico*", February 3, 2020 https://worldline.com/en/home/investors/operation-disclaimer/operation/pr-2020_02_03-02.html

[93] Cf. « *Un projet de scheme européen est à l'étude* », Revue Banque n° 838, 25 novembre 2019 http://www.revue-banque.fr/management-fonctions-supports/breve/un-projet-scheme-europeen-est-etude

[94] Cf. par exemple « *Le projet des banques européennes pour contrer Visa et Mastercard* », les Echos 6 novembre 2019 https://www.lesechos.fr/finance-marches/banque-assurances/le-projet-des-banques-europeennes-pour-contrer-visa-et-mastercard-1145680

De source publique donc, une vingtaine de banques européennes ont engagé depuis plusieurs mois un projet de création d'un *scheme* paneuropéen des paiements, initialement dénommé PEPS-I (*pan-european payment system initiative*) et aujourd'hui baptisé EPI (*european payment initiative*). Les transactions de paiement se déboucleraient par virement instantané et seraient compensées via TIPS (*target instant payment settlement*), le service d'infrastructure de marché lancé par l'Eurosystème en novembre 2018. Le projet s'appuierait donc sur l'utilisation d'une infrastructure déjà existante, qui organise une interbancarité à l'échelle européenne.

EPI doit composer avec des difficultés techniques, tant il existe dans les pays européens une grande diversité d'habitudes de paiement. En particulier, une dizaine de pays européens possèdent leur propre *scheme* de paiement national, comme la France (avec le GIE Carte bancaire), l'Allemagne, l'Italie, l'Espagne ou les Pays-Bas. Si elles parviennent à s'unir, les banques devront aussi convaincre les autres acteurs, comme les commerçants et les utilisateurs. Les banques devront aussi se mettre d'accord sur un modèle économique viable, qui devra être également validé par les autres parties prenantes aux transactions de paiement, qu'il s'agisse des établissements bancaires ou des commerçants.

Ce projet rencontre directement les préoccupations de la Banque Centrale Européenne. Dans un discours récent[95], Benoît Cœuré, membre du directoire de la BCE, a salué certains progrès européens en matière de paiement (SEPA, TIPS), mais s'est inquiété de l'absence de solution européenne de paiement, tant sur le lieu de vente que pour le commerce en ligne, ainsi que de l'augmentation de la part de marché des cartes non européennes dans les paiements scripturaux.

Le Conseil des Gouverneurs de la BCE vise désormais à promouvoir les initiatives des marchés paneuropéens en matière de paiements de détail. L'initiative EPI est saluée ; ses promoteurs sont incités à collaborer étroitement avec la Commission européenne pour garantir la conformité de leur projet aux règles de concurrence de l'Union Européenne. Les cinq objectifs ci-dessous constituent le cœur de la stratégie de l'Eurosystème en matière de paiements de détail. Ils fournissent la vision abstraite d'une solution, EPI ou autre, à laquelle le secteur privé est invité à donner naissance :

2.4.2.1 Portée paneuropéenne et expérience client

Les consommateurs doivent pouvoir effectuer des paiements dans tous les commerces de l'Union européenne avec la même efficacité et la même sécurité que dans leur pays d'origine. Une large acceptation par les commerçants de toute l'Union européenne, ainsi qu'une gouvernance robuste et efficace, conditionnent l'atteinte de la masse critique et la pleine exploitation des avantages du marché unique.

2.4.2.2 Pratique et économique

Une solution de paiement de détail européenne, pour être largement acceptée, doit répondre aux besoins et aux attentes des utilisateurs. L'expérience de paiement doit être simple, flexible, sûre et commode, à la fois pour les consommateurs et les commerçants. Les paiements doivent pouvoir être effectués par des moyens variés tels que les cartes de paiement, les téléphones portables, les objets connectés et les paiements instantanés, et par des canaux tels que le sans contact (NFC). Le paiement instantané semble permettre des paiements plus efficaces et moins coûteux, au bénéfice des consommateurs.

---

[95] « *Vers les paiements de demain: une stratégie européenne* », Discours de Benoît Cœuré, à la conférence conjointe de la BCE et de la Banque nationale de Belgique sur le thème "*Franchir le gouffre des paiements de détail de demain*", Bruxelles, le 26 novembre 2019
https://www.bis.org/review/r191126e.htm

2.4.2.3 Sûreté et sécurité

Une nouvelle solution de paiement européenne doit respecter toutes les exigences légales et réglementaires. Elle doit assurer le meilleur niveau de prévention contre la fraude et offrir au consommateur des procédures efficaces de règlement des litiges et de remboursement.

2.4.2.4 Identité européenne et gouvernance

Une marque et un logo communs doivent renforcer l'identité européenne. Une structure de gouvernance européenne, dans laquelle les acteurs européens du paiement sont impliqués dans l'orientation stratégique et les modèles d'affaires, doit assurer la satisfaction des besoins des clients européens.

2.4.2.5 Acceptation globale

Une nouvelle solution européenne doit être ouverte aux commerçants basés en dehors de l'Union Européenne, afin de renforcer les économies d'échelle et l'adhésion européenne. Une acceptation mondiale doit donc être un objectif de long terme.

2.4.3 Quelques interrogations soulevées par l'élaboration d'un *scheme* européen de paiement

2.4.3.1 Veiller à associer toutes les parties prenantes (banques, commerçants, consommateurs, industriels…)

Un facteur essentiel de succès d'un *scheme* européen tiendrait à l'engouement, ou au moins à l'intérêt qu'il susciterait, au-delà de la communauté bancaire, auprès de l'ensemble des parties prenantes. Les utilisateurs des systèmes de paiement, commerçants en ligne, commerçants sur le lieu de vente et consommateurs, comme les industriels du paiement, doivent avoir leur mot à dire sur les orientations à retenir. Aucune solution concoctée en vase clos par les banques ne peut espérer rencontrer une large adhésion du public.

2.4.3.2 Attention à ne pas lâcher la proie pour l'ombre[96]

Les *schemes* nationaux jouent aujourd'hui un rôle important : ils représentent des parts de marché significatives, ils protègent efficacement les données personnelles, le service qu'ils offrent est robuste et bon marché, le taux de fraude est faible, ils contribuent à l'existence d'un marché compétitif et ils limitent les risques de souveraineté.

L'essor du marché unique européen et la justification d'un nouveau *scheme* reposent sur la croissance des transactions transfrontières, d'un pays à l'autre de l'Union européenne. Mais dans l'immédiat, ces transactions sont très minoritaires et ne suffiraient pas à amortir des coûts de développement importants. C'est pourquoi la tentation peut être forte pour les banques de chercher à majorer les volumes qui seraient confiés à un nouveau *scheme* au détriment de ceux traités par les actuels *schemes* nationaux. Mais il serait regrettable qu'une telle évolution se traduise par une dégradation des performances ou par des risques accrus.

Pour minimiser les risques d'exécution, un pilotage du projet de *scheme* européen doit associer toutes les parties concernées, par exemple sous l'égide de l'*euro retail payments board* (ERPB)[97].

---

[96] Cf. « *Le chien qui lâche sa proie pour l'ombre* », J. de La Fontaine, 1668

[97] L'*Euro Retail Payments Board* (ERPB) est un organe stratégique de haut niveau chargé de favoriser l'intégration, l'innovation et la compétitivité des paiements de détail en euros dans l'Union européenne. Il a été lancé le 19 décembre 2013 par la BCE

2.4.3.3 La question du modèle économique

La question de l'équation économique apparaît centrale. La construction d'un nouveau *scheme* et la promotion d'une nouvelle marque de paiement requièrent à l'évidence des moyens importants, alors que les consommateurs ne semblent pas spontanément ressentir la nécessité d'un *scheme* européen, que le commerce ne semble pas non plus disposé à accepter une hausse des frais bancaires et que les ressources des banques ne sont pas sans limite.

Cette question compliquée suggère deux réflexions :

> **Il ne serait pas complètement cohérent de vouloir lancer une marque de paiement européenne forte et de ne pas affronter la concurrence d'autres *schemes* internationaux hors des frontières européennes. Il serait paradoxal de croire au marché unique européen, mais de craindre que les consommateurs européens se détournent d'un instrument de paiement mieux accepté en Europe que dans le reste du monde. Il n'est pas exclu qu'un réseau d'acceptation hors des frontières européennes se développe et contribue à terme à la rentabilité du projet. Il serait dommage de renoncer d'emblée à l'ambition que le nouveau *scheme* européen prenne progressivement toute sa place dans les instances de gouvernance d'EMVCo et de PCI SSC. En d'autres termes, il paraît important de peser les avantages et les inconvénients d'un parti-pris de co-badgeage des nouvelles cartes.**

> **La logique du règlement 2015/751, consistant à proscrire la situation dans laquelle un *scheme* national bénéficie d'une exclusivité sur les transactions domestiques, si elle est confirmée lors de sa révision, n'a pas été poussé jusqu'à son terme par les banques ; il pourrait apparaître opportun d'engager une réflexion sur une évolution du statut juridique des *schemes* nationaux, leur transformation en sociétés de capitaux étant éventuellement susceptible de favoriser des rapprochements capitalistiques entre eux, ainsi que la valorisation par les banques de leurs investissements passés au profit de nouveaux projets.**

Par ailleurs, la question du modèle d'affaires semble très dépendante, comme cela avait été le cas avec le projet Monnet (cf. ci-dessus, chapitre 2.4.1.1, p. 54), d'une certaine visibilité sur le niveau des commissions d'interchange. A cet égard, la mission renvoie aux observations déjà faite (chapitre Recommandation n° 2, p. 42) sur la nécessité, quel que soit le niveau des commissions d'interchange, de conditions neutres de concurrence entre un paiement par carte traditionnel et d'autres formes de règlements qui se déboucleraient par un paiement instantané (tel que le Request to pay).

2.4.3.4 L'indépendance du nouveau scheme par rapport aux normes EMVCo

Si les transactions que le projet EPI envisage de traiter se débouclent par les nouvelles infrastructures de paiement instantané, les autres caractéristiques du projet n'ont pas été divulguées et sont peut-être encore en discussion.

---

et a remplacé le Conseil SEPA. L'ERPB est présidé par un représentant de la BCE ; il comprend des représentants des établissements financiers, des consommateurs et des entreprises. La Commission européenne assiste aux réunions en tant qu'observateur.

Une ligne de crête est probablement difficile à dessiner entre un projet qui se démarquerait des moyens de paiement existants par son caractère innovant et, au contraire, un projet auquel les consommateurs adhèreraient facilement parce qu'il ressemblerait à ce qu'ils connaissent.

Ces arbitrages portent aussi sur le choix de s'appuyer sur les standards mondiaux du paiement par carte (EMVCo, PCI SSC…) – à la détermination desquels les porteurs du nouveau projet auraient alors vocation à participer – ou de s'en émanciper, comme les applications de paiement chinoises Alipay et WeChatPay, pour tirer le meilleur parti de choix techniques innovants (s'agissant notamment du paiement instantané).

2.5 L'harmonisation des exigences de conformité au règlement général sur la protection des données personnelles (RGPD)

2.5.1 Quelques rappels sur le RGPD

2.5.1.1 Qu'est-ce qu'un traitement de données personnelles et quelles sont les entreprises soumises au RGPD ?

Pour le RGPD, une donnée à caractère personnel est une information se rapportant à une personne physique « *qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne…* »[98].

Il importe peu que celui qui détient la donnée soit lui-même capable d'identifier la personne physique concernée, il suffit que quelqu'un d'autre soit susceptible de le faire. Même en l'absence de nom ou d'un numéro d'identification, il suffit qu'un ou plusieurs éléments spécifiques propres à « *l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* » permette de rattacher par recoupement une donnée à une personne physique pour que cette donnée soit qualifiée de donnée personnelle : ce pourrait être par exemple le cas si un événement comportait des indications d'heure et de géolocalisation suffisamment précises pour qu'une personne soit identifiable.

Le RGPD régit tous les traitements de telles données personnelles, et il faut comprendre le terme de traitement dans son acception la plus large puisqu'il s'agit de « *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction* ».

Le RGPD est un règlement de portée extraterritoriale : il s'applique au traitement des données à caractère personnel effectué **dans le cadre des activités d'un établissement ou d'un de ses sous-traitant sur le territoire de l'Union européenne**, que le traitement ait lieu ou non dans l'Union. Il s'applique également au traitement des données à caractère personnel **relatives à des personnes qui se trouvent sur le territoire de l'Union européenne** par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées à l'offre de biens ou de services à ces personnes concernées dans l'Union ; ou au suivi du comportement de ces personnes au sein de l'Union[99].

---

[98] Article 4, point 1) du règlement 2016/679 du 27 avril 2016

[99] Article 3, paragraphes 1. et 2. du règlement 2016/679 du 27 avril 2016

2.5.1.2 A quelles conditions un traitement de données est-il permis par le RGPD ?

Le traitement de données à caractère personnel doit être licite et loyal. L'information et la communication relative au traitement de ces données à caractère personnel doivent être aisément accessibles, faciles à comprendre, formulées en des termes clairs et simples. Ce principe vaut tout particulièrement pour les informations communiquées aux personnes concernées sur l'identité du responsable du traitement et sur les finalités du traitement, ainsi que pour les autres informations visant à assurer un traitement loyal et transparent à l'égard des personnes physiques concernées et leur droit d'obtenir la confirmation et la communication des données à caractère personnel les concernant qui font l'objet d'un traitement.

Les personnes physiques doivent être informées des risques, règles, garanties et droits liés au traitement des données à caractère personnel et des modalités d'exercice de leurs droits en ce qui concerne ce traitement. En particulier, les finalités spécifiques du traitement des données à caractère personnel doivent être explicites et légitimes, et déterminées lors de la collecte des données à caractère personnel.

Les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire pour les finalités pour lesquelles elles sont traitées. Cela exige, notamment, de garantir que **la durée de conservation des données soit limitée**. Les données à caractère personnel ne doivent être traitées que si la finalité du traitement ne peut être raisonnablement atteinte par d'autres moyens. Les données à caractère personnel doivent être traitées de manière à garantir une sécurité et une confidentialité appropriées.

Le traitement de données personnelles est soumis à **une condition de licéité**[100] : il n'est admis que si, et dans la mesure où, au moins une des conditions suivantes est remplie:

a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ;

b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;

c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;

d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;

e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;

f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers.

Antérieurement au RGPD, la directive 95/46/CE du 24 octobre 1995[101] instituait une protection des données à caractère personnel sur le fondement d'un régime d'autorisation des traitements de données personnelles. Désormais, les entreprises interprètent et appliquent les règles sous leur responsabilité, sous le contrôle a posteriori de la CNIL et des autres instances nationales de protection des données personnelles et sous la menace de sanctions pouvant atteindre 4 % de leur chiffre d'affaires.

---

[100] Article 6 du règlement 2016/679 du 27 avril 2016

[101] Directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

2.5.1.3 Si plusieurs entreprises concourent à la prestation d'un même service, quels sont les droits et les obligations de chacune ?

Le RGPD apporte une attention particulière à clarifier les responsabilités entre donneur d'ordre et **sous-traitant** lorsque leurs relations portent sur des données à caractère personnel. La réalisation d'un traitement de données personnelles par un sous-traitant doit être régie par un contrat définissant l'objet et la durée du traitement, la nature et les finalités du traitement, le type de données à caractère personnel et les catégories de personnes concernées, en tenant compte des tâches et des responsabilités spécifiques du sous-traitant dans le cadre du traitement à effectuer et du risque pour les droits et libertés de la personne concernée. Après la réalisation du traitement pour le compte du responsable du traitement, le sous-traitant doit, selon le choix du responsable du traitement, renvoyer ou supprimer les données à caractère personnel[102].

Les obligations du sous-traitant sont étroitement définies par le donneur d'ordre : le sous-traitant ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel le sous-traitant est soumis ; dans ce cas, le sous-traitant informe le responsable du traitement de cette obligation juridique avant le traitement[103].

Il peut advenir que plusieurs entreprises collaborent à la fourniture d'un service sans être l'une par rapport à l'autre dans un rapport d'étroite dépendance. Le RGPD admet une alternative au cadre de la sous-traitance, lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, en considérant qu'ils sont alors les **responsables conjoints du traitement**. Le coresponsable de traitement bénéficie d'une plus grande liberté d'initiative, au regard du RGPD, que le sous-traitant. Mais il supporte en contrepartie de plus fortes obligations.

Les responsables conjoints du traitement doivent en particulier définir leurs obligations respectives aux fins d'assurer le respect des exigences du RGPD, notamment en ce qui concerne l'exercice des droits de la personne concernée (droit d'accès, droit de rectification et d'effacement, droit à la limitation du traitement, droit à la portabilité des données, droit d'opposition…) et leurs obligations respectives quant à la communication des informations à fournir selon que les données à caractère personnel ont été ou non collectées auprès de la personne concernée[104].

2.5.1.4 Le rôle du Comité Européen de la Protection des Données

La directive 95/46/CE[105] n'avait pas permis d'éviter une certaine fragmentation des règles de protection des données à caractère personnel dans l'Union européenne, du fait de divergences de transposition et de mise en œuvre entre les Etats membres. L'un des enjeux de l'adoption du RGPD consistait à assurer une application cohérente et homogène des règles. A cet effet, et parce qu'il s'agit de rapprocher des règles de protection des données personnelles interprétées diversement depuis des décennies, une importante section du RGPD consiste à établir un mécanisme de contrôle de la cohérence[106].

Il est institué à cet effet un comité européen de la protection des données (CEPD), organe de l'Union doté de la personnalité juridique, auquel participe le chef de l'autorité de contrôle de chaque État membre. Le comité est notamment chargé d'examiner, de sa propre initiative, à la demande de l'un

---

[102] Cf. considérant (81) du RGPD

[103] Cf. articles 28 et 29 du RGPD

[104] Cf. article 26 du RGPD

[105] Directive 95/46/CE du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

[106] Articles 63 et suivants du RGPD

de ses membres ou à la demande de la Commission, toute question portant sur l'application du RGPD, et de publier des lignes directrices, des recommandations et des bonnes pratiques afin de favoriser l'application cohérente du règlement[107].

2.5.2 L'application de ces dispositions au contexte du paiement

2.5.2.1 Les données liées à des transactions de paiement de personnes physiques sont, sauf si elles sont anonymisées, soumises au RGPD

Il résulte de la définition des données à caractère personnel que **toute donnée associée à l'identifiant de compte ou au numéro de carte bancaire d'un ressortissant de l'Union européenne constitue une donnée à caractère personnel.** Il en va de même si l'identifiant de compte ou le numéro de carte bancaire est remplacé par un *token*[108] et qu'il est possible de reconstituer la donnée d'origine par *de-tokenisation* (c'est donc le cas des *tokens de sécurité* réversibles et des *tokens* de paiement). Il en va encore de même si l'auteur du paiement peut être identifié par recoupement. Dans tous ces cas, un traitement de données, au sens très large rappelé ci-dessus, doit respecter les principes relatifs à la protection des données personnelles.

A contrario, si une base de données ne comporte aucune donnée d'identification (nom, adresse…), si les données de sécurité personnalisées sont remplacées par un *token de sécurité* irréversible (c'est-à-dire que l'algorithme est tel que nul ne peut reconstituer la donnée d'origine) et si les autres données ne permettent pas par recoupement d'identifier la personne concernée, alors la base de donnée en question n'est pas une base de données à caractère personnel, elle n'est pas soumise au RGPD et son utilisation est libre.

C'est l'application de la notion d'anonymisation des données personnelles expliquée par le considérant 26 du règlement : « *Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage. Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci. Il n'y a dès lors pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable. Le présent règlement ne s'applique, par conséquent, pas au traitement de telles informations anonymes, y compris à des fins statistiques ou de recherche*. »

Cette notion d'anonymisation doit bien être distinguée de celle de pseudonymisation : « *les données à caractère personnel qui ont fait l'objet d'une pseudonymisation et qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires devraient être considérées comme des informations concernant une personne physique identifiable* » et donc soumises au RGPD. Sous certaines conditions toutefois, la pseudonymisation peut permettre d'utiliser des données personnelles à des fins autres que celles pour laquelle elles ont été collectées, sans nécessairement recueillir le consentement de la personne concernée.[109]

---

[107] Cf. articles 68 et suivants

[108] Cf. Tirer le meilleur parti des techniques de *tokenisation*, chapitre 2.3, p. 44

[109] Cf. article 6, paragraphe 4 du RGPD

Le Groupe de travail article 29 sur la protection des données (dit « G29 ») avait donné en 2014 une interprétation exigeante de la notion d'anonymisation.[110] Il ne s'agissait toutefois que d'une opinion (et non de lignes directrices), et elle a été élaborée avant l'entrée en vigueur du RGPD. Le Comité européen de la protection des données ne l'a d'ailleurs pas endossée ; mais il n'a pas non plus établi à ce sujet de lignes directrices.

L'opinion du G29 énonce notamment que, « *dans le cas où un responsable du traitement des données n'efface pas les données originales (identifiables) au niveau des événements individuels et transmet une partie de cet ensemble de données (par exemple après avoir supprimé ou masqué les données identifiables), l'ensemble de données résultant constitue encore des données à caractère personnel. Ce n'est que si les données sont agrégées par le responsable de leur traitement à un niveau où les événements individuels ne sont plus identifiables que l'ensemble de données résultant peut être qualifié d'anonyme.*

Une solution d'anonymisation efficace doit empêcher toutes les parties d'isoler un individu dans un ensemble de données, de relier entre eux deux enregistrements dans un ensemble de données (ou dans deux ensembles de données séparés) et de déduire des informations de cet ensemble de données. D'une manière générale, il ne suffit donc pas de supprimer directement des éléments qui sont, en eux-mêmes, identifiants pour garantir que toute identification de la personne n'est plus possible. »

2.5.2.2 Les difficultés propres à l'existence d'une chaîne d'intermédiaires

Les règles définies par le RGPD présentent un caractère général et leur application au cas des données de paiement ne comporte pas de particularité explicite. Il n'en reste pas moins, et ce n'est pas l'apanage des services de paiement, que des difficultés d'interprétation de certaines dispositions du RGPD se présentent. En particulier, la qualification et l'articulation des responsabilités définies par le RGPD ne vont pas de soi quand, dans un contexte de paiement, les données personnelles passent de main en main entre différents acteurs successifs d'une chaîne de traitement.

L'attention de la mission a été attirée sur le fait que les données constituées à l'occasion d'opérations de paiement ont des origines multiples : le payeur et sa banque, le bénéficiaire du paiement et sa banque… Les bases de données résultant de l'agrégation de ces données de différentes sources pourraient être protégées par le droit de la propriété intellectuelle, en tant qu'œuvres composites. Ainsi, une directive européenne du 11 mars 1996[111] accorde une double protection juridique aux bases de données : elles sont protégées d'une part comme œuvre de l'esprit, par le droit d'auteur, et d'autre part comme bien informationnel d'un genre nouveau, par le droit *sui generis* du producteur de la base de données. Mais l'existence éventuelle de droits patrimoniaux attachés à des bases de données de paiement ne saurait aux yeux de la mission limiter la portée du RGPD, ni retirer le caractère de données personnelles à l'ensemble des champs des bases de données de paiement constituées de plusieurs sources.

Les *schemes* de paiement (Visa, MasterCard, GIE CB) ont, en tant que gestionnaire de réseaux de carte, un positionnement ambigu. Les banques émettrices de cartes sont seules véritablement en contact et en relations contractuelles avec les porteurs de cartes. Le réseau de carte, qui assure le bon déroulement des paiements, peut apparaître comme un simple prestataire sous-traitant des banques ; les clients porteurs de cartes peuvent ne pas avoir conscience de l'existence de ces gestionnaires de réseau de carte et de leur rôle dans le traitement de leurs données.

Pourtant, de plus en plus, ils exploitent les données transitant dans leur système pour détecter la fraude à la carte bancaire et vendent cette prestation à des établissements financiers. Ils peuvent

---

[110] « *Opinion 05/2014 on Anonymisation Techniques* », Article 29 data protection working party, 10 April 2014 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

[111] Directive 96/9/CE du Parlement européen et du Conseil, du 11 mars 1996, concernant la protection juridique des bases de données

également être tentés d'exploiter des données de transaction à des fins commerciales, sous forme de valorisation des tendances d'achat inférées à partir de l'analyse des transactions[112]. Ces acteurs semblent devoir être qualifiés de responsable de traitement dès lors qu'ils utilisent les données de transaction pour une finalité autre que la gestion du réseau de carte (par exemple pour en déduire des modèles de fraude, pour analyser les habitudes de consommation, etc), au-delà du mandat donné par les banques émettrices.

Les *schemes* de paiement voient transiter par leurs systèmes des données toujours plus nombreuses et plus riches[113]. Les banques émettrices leurs communiquent des données personnelles d'identification des porteurs de cartes, tandis que les banques acquéreurs leurs communiquent les données personnelles correspondant aux paiements effectués par les porteurs de cartes chez les commerçants. Le *scheme* assure les traitements au sens du RGPD de ces données nécessaires au paiement (authentification, autorisation, compensation / règlement).

Ces traitements sont-ils exercés par l'entité qui assure le *processing* des transactions en tant que sous-traitant de la banque émettrice ou en tant que co-responsable de traitement ? Dans les deux alternatives, la réglementation est exigeante. Soit le processeur doit montrer qu'il agit strictement sur ordre de la banque émetteur, sans initiative et en rendant des comptes ; soit il se met en situation de garantir par lui-même les droits des personnes concernées.

Ces difficultés ne s'appliquent pas qu'aux *schemes*, mais aussi aux commerçants et à tous les acteurs de la chaîne de paiement qui interviennent dans l'acquisition des paiements entre le commerçant et la banque acquéreur. Beaucoup ont à leur disposition des données personnelles et sont fondés à les exploiter à des fins légitimes (telles que la mesure de la qualité du service rendu, la lutte contre la fraude ou le blanchiment…). Certains peuvent être tentés d'élargir ces finalités à d'autres, plus lucratives et moins légitimes : une valorisation commerciale des données de paiement peut en effet éveiller beaucoup de convoitises ou de suspicions.

La licéité d'un traitement peut être sujette à controverse. Dans certains cas, elle ne fait pas de doute : l'authentification de l'émetteur d'un paiement est justifiée par l'exécution d'un contrat, les diligences de lutte anti-blanchiment sont nécessaires au respect d'une obligation légale, la lutte contre la fraude ou la sécurité du réseau répondent à un intérêt légitime. Mais dans d'autres cas, la finalité d'un traitement est plus difficile à qualifier et la question suivante se pose : le responsable du traitement est-il fondé à considérer qu'il peut s'appuyer sur un intérêt légitime ou doit-il recueillir le consentement éclairé de la personne concernée ?

La question nous semble par exemple se poser dans le cas d'un acteur des paiements dont la politique de confidentialité comporte la mention suivante, assez ambigüe : « *Nous pouvons également traiter vos informations personnelles aux fins de nos propres intérêts légitimes ou des intérêts légitimes d'autrui, à condition que le traitement ne l'emporte pas sur vos droits et libertés. En particulier, nous traiterons vos informations personnelles au besoin pour […] comprendre et améliorer nos relations commerciales ou avec nos clients en général* ».

Les mentions d'information quant au rôle et aux caractéristiques des traitements effectués par certains acteurs ne semblent pas toujours portées directement à la connaissance des personnes concernées. Elles peuvent figurer dans des conditions générales d'utilisation des cartes peu lisibles et sur lesquelles l'attention des clients n'est pas appelée. Les finalités de réutilisation des données ainsi que leur impact sur les personnes n'apparaissent pas toujours clairement, cette observation étant également vraie s'agissant des modalités d'exercice des droits.

Il n'est pas toujours évident de reconnaitre un intérêt légitime à l'exploitation des données personnelles par certains acteurs, l'équilibre entre leurs intérêts et la protection des droits des

[112] Par exemple, quel est le comportement des clients de l'enseigne X à l'égard de l'enseigne Y ?

[113] Cf. dans le cas du paiement en ligne le protocole d'authentification 3DS V2

personnes n'allant pas de soi. La conservation des données, tant en termes de finalité que de durée, n'est pas toujours expliquée avec une transparence suffisante.

Les informations recueillies par la mission auprès des différents acteurs sont dans quelques cas contradictoires et insatisfaisantes. D'indéniables difficultés d'analyse expliquent cette situation. Mais il importe de les lever et de définir une règle commune à tous, sans quoi on laisserait perdurer une situation où les acteurs, par méconnaissance de la norme plutôt que par un choix délibéré, appliqueraient avec un niveau d'exigence variable les mêmes principes de protection des données personnelles. Cette situation pourrait favoriser l'existence de passagers clandestins (*free riders*) et faire obstacle à une concurrence équitable (*level playing field*).

2.5.2.3 La durée de conservation des données de paiement

Selon l'article 5 du RGPD, les données à caractère personnel ne doivent pas être conservées sous une forme permettant l'identification des personnes concernées pendant une durée excédant « *celle nécessaire au regard des finalités pour lesquelles elles sont traitées* ». Cette règle d'application générale revêt une grande importance en matière de données de paiement, eu égard à la multiplicité des acteurs intervenant dans la réalisation d'une opération de paiement. Le choix de la durée de conservation des données de paiement par chaque acteur et le contrôle de l'effacement de ces données peuvent constituer des enjeux aussi importants que celui de la localisation des données de paiement.

Après la réalisation d'une opération de paiement, la conservation des données à caractère personnel ne se justifie, sans le consentement éclairé des personnes concernées, que par le droit de l'Union ou le droit national. La banque d'un consommateur est évidemment tenue de lui rendre des comptes et de satisfaire à des obligations comptables pendant plusieurs années ; il peut en être de même de la banque du commerçant ; mais il ne semble pas que les acteurs qui interviennent dans le *processing* du paiement soient fondés à conserver durablement des données personnelles.

Recommandation n° 5.	Le Comité Européen de la Protection des Données (CEPD) devrait se prononcer sur l'interprétation des règles du RGPD à retenir en matière de paiement, s'agissant notamment : - du statut des acteurs de la chaîne de paiement (sous-traitant ou co-responsable de traitement) et des conséquences de ce statut ; - des conditions de licéité d'une valorisation commerciale des données de paiement ; - de la durée de conservation des données de transaction par les intermédiaires de la chaîne du paiement.

2.5.3 L'obligation de localisation des données favorise le respect du RGPD

2.5.3.1 Le RGPD est une loi à caractère extra-territorial

Le champ d'application territorial du RGPD est défini à l'article 3 selon un double critère territorial :

- en premier lieu, ses dispositions s'appliquent « *dans le cadre des activités d'un établissement, d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union* », ce qui est assez naturel ;
- en second lieu, si le premier critère n'est pas satisfait, les dispositions du règlement s'appliquent également aux traitements de données à caractère personnel relatives à « *des*

personnes concernées qui se trouvent sur le territoire de l'Union », lorsque ces traitements sont liés soit à une offre de biens ou de services, soit au suivi du comportement de ces personnes.

On mesure bien l'étendue et le caractère innovant du champ d'application, qui peut conduire à rendre les dispositions du règlement applicables à la situation d'un traitement effectué pour le compte d'un responsable de traitement du pays A par un sous-traitant localisé dans le pays B et qui concerne un ressortissant du pays C de passage en Europe !

2.5.3.2 Le non-respect du RGPD peut être difficile à déceler

Les obligations énoncées par le RGPD sont de natures assez diverses. Certaines accordent des droits aux personnes physiques concernées par des traitements ou se traduisent par une communication à leur égard : droit d'accès aux données à caractère personnel, droit de rectification ou d'effacement de ces données, droit à la portabilité des données, droit d'opposition aux décisions fondées sur le profilage, communication d'une violation de données à caractère personnel, informations fournies lorsque des données à caractère personnel sont collectées, recueil du consentement…

D'autres obligations posées par le RGPD sont tout aussi importantes mais moins visibles : la tenue d'un registre de traitement des données à caractère personnel, l'obligation que les développements informatiques intègrent *by design* les enjeux de protection des données personnelles, la minimisation et le respect de la durée de conservation des données, la formalisation des relations avec les sous-traitants… Il apparaît bien difficile d'apprécier à distance la conformité d'une entreprise.

2.5.3.3 L'obligation de localisation des données de paiement pourrait faciliter l'identification et la sanction des manquements

Même si le RGPD est théoriquement applicable à tous, il existe sans doute de profonds écarts en ce qui concerne la possibilité d'apprécier la conformité d'un traitement, selon que celui-ci résulte de l'activité « *d'un établissement, d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union* » ou, dans le pire des cas, de l'activité d'acteurs sans implantation en Europe et de mauvaise volonté.

On est dans le premier cas sous le regard et à la portée d'une autorité de contrôle nationale. Dans le second cas, même si le responsable du traitement ou le sous-traitant est tenu de désigner par écrit un représentant dans l'Union européenne[114], maintes difficultés peuvent faire obstacle au contrôle : la langue, la culture, l'étendue du mandat du représentant… Aux difficultés du contrôle pourraient s'ajouter, le moment venu, celles du recouvrement de l'amende en cas de sanction.

La distinction entre ces deux situations d'application du RGPD renvoie à la différence rappelée par le rapport Gauvain[115] entre deux types de compétences selon lesquelles s'exerce la souveraineté des États : « *la compétence normative, qui est le pouvoir d'édicter des normes et de les appliquer à des situations données, au travers notamment de décisions administratives ou de jugements ; et la compétence opérationnelle, qui est le pouvoir de mettre en œuvre les normes (saisie de documents, arrestations)* ».

Si en matière de compétence normative, l'extraterritorialité est possible sous réserve qu'existent des critères de rattachement (rattachement territorial, rattachement personnel ou rattachement matériel), en matière de compétence opérationnelle, l'extraterritorialité est impossible, car elle viole les principes d'intégrité territoriale et d'indépendance des États énoncés par la Charte des Nations Unies.

---

[114] Cf. article 27 du RGPD : Représentants des responsables du traitement ou des sous-traitants qui ne sont pas établis dans l'Union

[115] Cf. chapitre 1.1.7 et note 33 p. 18 (p. 11 du rapport Gauvain)

L'obligation de localisation des données de paiement améliorerait, s'agissant de l'application des règles du RGPD, les chances de caractériser des manquements et de poursuivre une entreprise fautive. Elle conduirait aussi, par voie de conséquence, à un meilleur *level playing field*[116] entre toutes les entreprises traitant de données de paiement.

2.6 La protection des données de paiement stockées sur le cloud

2.6.1 Les enjeux liés à l'essor du stockage et du traitement des données sur le *cloud*

2.6.1.1 Le marché du cloud

La croissance très forte des données produites a conduit de nombreuses entreprises à externaliser tout ou parties de leurs données chez des sous-traitants, créant ainsi le *cloud*. Le marché mondial du *cloud computing* public (32,4 milliards de dollars en 2018 pour les activités dites *infrastructure as a service*) est actuellement dominé par Amazon Web Services (47,8 %), suivi par Microsoft Azure (15,5 %), Alibaba (7,7 %), Google (4 %) et IBM (1,8 %)[117].

Le fait de recourir à des prestataires étrangers est loin d'être anodin. Les autorités d'un pays étranger (le plus souvent les Etats Unis, au vu de la nationalité des principaux prestataires de *cloud*) peuvent accéder facilement à des données stockées dans des serveurs situés sur le territoire américain mais aussi en dehors de ce territoire en prétextant de la nationalité du prestataire.[118]

Dès lors, les entreprises françaises et européennes doivent être particulièrement vigilantes face à la confidentialité des données qu'elles externalisent. Ce constat avait conduit le Gouvernement à lancer en 2009 le projet Andromède d'un *cloud* souverain. Deux offres d'hébergement de données en ligne (Cloudwatt et Numergy) ont été financées par la Caisse des Dépôts et Consignations dans le cadre du Programme des Investissements d'Avenir (PIA) à hauteur de 75 millions d'euros chacun. Mais ces initiatives ont tourné court.

Cloudwatt, lancé en 2012 sous l'égide d'Orange, Thalès et la CDC, aujourd'hui exclusivement porté par Orange, cessera son activité le 1er février 2020[119]. Numergy, fondée en 2012 par SFR, Bull et la CDC, a été placée sous procédure de sauvegarde le 13 octobre 2015[120] et les parts des actionnaires

---

[116] Règles du jeu équitables, garantissant l'égalité des chances entre tous

[117] "*Gartner Says Worldwide IaaS Public Cloud Services Market Grew 31.3% in 2018*"., July 29, 2019 https://www.gartner.com/en/newsroom/press-releases/2019-07-29-gartner-says-worldwide-iaas-public-cloud-services-market-grew-31point3-percent-in-2018

[118] Extrait du « *Rapport étudiant la possibilité de créer un Commissariat à la souveraineté numérique* », Rapport du CGE au Ministre de l'Économie et des finances, J. Cueugniet et Ph. Louviau, mars 2017, annexé au rapport de la commission d'enquête sénatoriale sur la souveraineté numérique http://www.senat.fr/rap/r19-007-1/r19-007-11.pdf

[119] Cf. « *Une page se tourne pour le cloud souverain français* », les Echos, 1 août 2019 https://www.lesechos.fr/tech-medias/hightech/une-page-se-tourne-pour-le-cloud-souverain-francais-1118112

[120] « *Numergy sous procédure de sauvegarde* », les Echos, 21 oct. 2015 https://www.lesechos.fr/2015/10/numergy-sous-procedure-de-sauvegarde-278960

minoritaires ont été rachetées par SFR Group en janvier 2016. Selon l'Usine Nouvelle, le cloud souverain Numergy est définitivement enterré.[121]

Il faut toutefois signaler qu'un opérateur français, OVH, créé en 1999, est devenu un leader européen du *cloud* sans avoir bénéficié de subventions de ce type. De même, OUTSCALE, fondée en France en 2010 et majoritairement détenue par la société Dassault Systèmes depuis 2017, qualifié SecNumCloud par l'ANSSI le 2 décembre 2019 (cf. ci-dessous), est une entreprise française qui propose également des services d'*infrastructure as a service* (IaaS). Originellement créé pour répondre à la problématique de la souveraineté des données en France, OUTSCALE s'est étendu à l'international et implanté en Asie, en Europe et aux États-Unis.

Le ministère fédéral de l'Économie allemand a par ailleurs présenté le 29 octobre 2019 un projet baptisé GAIA-X d'infrastructure de données ouverte en réseau, qui offre aux entreprises et aux autorités européennes une alternative aux GAFAM. Le projet doit être mis en œuvre avant la fin de l'année 2020. La France, ainsi que d'autres pays européens, ont été invités à y prendre part.[122]

2.6.1.2 Le rôle de l'ANSSI

Face à une menace croissante et de plus en plus sophistiquée, le choix de solutions de sécurité représente un enjeu stratégique au sein des organisations aussi bien publiques que privées. Reposant sur l'expertise de centres d'évaluation privés agréés, le Visa de sécurité ANSSI a pour objectif de guider les utilisateurs dans leurs choix de solutions de sécurité, contribuant ainsi au renforcement des capacités de cyberdéfense de la France et de l'Europe. Le Visa de sécurité que délivre l'ANSSI permet d'identifier facilement les plus fiables d'entre elles, reconnues comme telles à l'issue d'une évaluation réalisée par des laboratoires agréés selon une méthodologie rigoureuse et éprouvée.

Dans le cadre de cette démarche, l'agence a élaboré le référentiel SecNumCloud en vue de permettre la qualification de prestataires de services d'informatique en nuage, dit *cloud*. L'objectif : promouvoir, enrichir et améliorer l'offre de prestataires de *cloud* à destination des entités publiques et privées souhaitant externaliser, auprès de prestataires de confiance, l'hébergement de leurs données, applications ou systèmes d'information. Sont concernés les prestataires d'informatique en nuage offrant des services de type SaaS (*software as a service*), PaaS (*platform as a service*) et IaaS (*infrastructure as a service*) et souhaitant obtenir un visa de sécurité ANSSI.

Le référentiel SecNumcloud conjugue des exigences relatives au prestataire de service d'informatique en nuage, à son personnel ainsi qu'à la localisation des données client au sein de l'Union européenne – échelle territoriale de référence – et le droit applicable à ces données. Lancé en 2016 avec deux niveaux de garantie, « SecNumCloud avancé » et « SecNumCloud essentiel », le référentiel a évolué et est devenu « SecNumCloud », dans un souci de simplification et de prise en compte des besoins exprimés par les utilisateurs potentiels. Depuis l'entrée en vigueur du RGPD, grâce à une coopération entre l'ANSSI et la CNIL, SecNumCloud inclut des exigences relatives à la protection des données, afin de répondre plus complètement aux attentes des besoins des entreprises, des administrations et des collectivités.[123]

---

[121] « *SFR se donne un nouveau départ dans le cloud… sans son cloud souverain Numergy* », l'Usine Nouvelle, 29 mars 2018 https://www.usinenouvelle.com/article/sfr-se-donne-un-nouveau-depart-dans-le-cloud-sans-son-cloud-souverain-numergy.N673834

[122] "*Germany's Digital Summit 2019: DIGITAL SME welcomes GAIA-X project*", European DIGITAL SME Alliance, 30 octobre 2019 https://www.digitalsme.eu/germanys-digital-summit-2019-digital-sme-welcomes-gaia-x-project/

[123] Cf. communiqué de l'ANSSI : « *SecNumCloud évolue et passe à l'heure du RGPD* », 22 juin 2018 https://www.ssi.gouv.fr/actualite/secnumcloud-evolue-et-passe-a-lheure-du-rgpd/

2.6.1.3 *L'hypothèse d'une obligation générale de localisation des données stockées sur le* cloud

Une commission d'enquête sur la souveraineté numérique[124], créée par le Sénat le 9 avril 2019, s'est attachée à identifier et à esquisser les moyens de reconquérir les champs fondamentaux de notre souveraineté numérique. S'agissant d'une obligation générale de localisation des données, sa position est nuancée :

« *Si promouvoir, voire dans certains cas imposer, une obligation de localisation des données sur un territoire précis (en France ou en Europe) est une idée qui peut paraître intéressante au premier abord, l'utilité réelle en termes de souveraineté numérique d'une telle démarche doit aujourd'hui être largement nuancée.*

Ces initiatives pourraient présenter un intérêt limité dans certains cas :

- *avant tout pour protéger certaines données particulièrement sensibles (traitements publics souverains, données privées financières ou commerciales stratégiques) ; à ce titre, lors de son audition, Mme Claire Landais, secrétaire générale du SGDSN, ne défend le recours à un* cloud *« interne » géographiquement localisé que pour les données les plus sensibles, dans une logique de cercles concentriques aux exigences de sûreté décroissante. Votre rapporteur considère également que l'on ne saurait imposer un mode de stockage particulier aux entreprises sans leur offrir des solutions industrielles performantes et accessibles répondant à leurs besoins. De telles solutions pourraient ainsi être imposées dans le cadre plus général des régimes des opérateurs d'importance vitale (OIV) ou des opérateurs de services essentiels (OSE) ;*
- *également pour garantir une accessibilité renforcée, soit du point de vue des entreprises dans une logique de gestion des risques (lorsque les données ne sont plus localisées en France ou en Europe, il est plus difficile en pratique de les contrôler et d'avoir une assurance de l'usage qui a été fait par des prestataires ou des partenaires localisés à l'étranger), soit du point de vue de la puissance publique (pour faciliter l'accès à ces données par la justice ou les régulateurs nationaux dans le cadre de l'exercice de leurs pouvoirs de contrôle sectoriel, comme l'a souligné la présidente de l'Autorité de la concurrence) ;*
- *et enfin, de façon générale, en stimulant la demande, pour soutenir l'écosystème industriel des acteurs du* cloud *et le développement des capacités de traitement des données.*

Le Sénat a ainsi pu, par le passé, soutenir des initiatives largement transpartisanes en ce sens : en 2016, lors des débats relatifs à la loi pour une République numérique, notre assemblée avait adopté, sans hélas être suivie par l'Assemblée nationale, un amendement de notre collègue Eliane Assassi et des membres du groupe communiste républicain et citoyen, avec un avis favorable de la commission des lois, visant à faire figurer dans la loi « Informatique et libertés » l'obligation de stockage des données personnelles des citoyens français sur le territoire européen.

De telles initiatives doivent néanmoins prendre en compte l'évolution récente du droit européen et des systèmes juridiques étrangers, et il apparaît qu'une obligation de localisation des données ne répondrait pas au défi posé par certaines législations à vocation extraterritoriales. D'une part, s'agissant des données non personnelles, le droit européen limite drastiquement la possibilité d'imposer des exigences de localisation. Elles sont désormais interdites « sauf si elles sont justifiées par des motifs de sécurité publique dans le respect du principe de proportionnalité ».

D'autre part, et en tout état de cause, les clauses de localisation des données n'offrent pas de garanties face aux nouvelles législations ou pratiques étrangères à portée extraterritoriale (sanctions internationales, Cloud Act *adopté aux Etats-Unis en mars 2018, etc.) ni contre la porosité entre certains acteurs industriels et leur Gouvernement (certains équipementiers chinois, par exemple). Ainsi, quand*

---

[124] « *Rapport fait au nom de la commission d'enquête sur la souveraineté numérique* », 1er octobre 2019 http://www.senat.fr/rap/r19-007-1/r19-007-11.pdf

*bien même des données seraient physiquement localisées sur le territoire français ou européen, les entités qui contrôlent les centres de données (*datacenters*) continueront, en raison de leur nationalité, à être également soumises à des régimes juridiques les obligeant à coopérer avec des puissances étrangères*. »

2.6.2 Les entreprises financières recourent de plus en plus au *cloud*

2.6.2.1 Les exemples de Société Générale et d'HSBC

Une forte proportion de fintechs ont recours aux services *cloud*. Mais, alors que cette dépendance pouvait apparaître il y a quelques années comme un trait de faiblesse et d'immaturité des nouveaux entrants sur le marché des services financiers, et alors que les grandes banques, tout particulièrement en France, paraissaient très attachées à des systèmes informatiques propriétaires, certaines d'entre elles engagent un changement de stratégie, et un mouvement d'externalisation des traitements informatiques des banques sur le *cloud* public paraît irréversible. Cette situation est illustrée ci-dessous par un communiqué de la Société Générale et par le discours d'un dirigeant d'HSBC.

« *La stratégie* Cloud First *de Société Générale permet aux systèmes d'information du Groupe de gagner en agilité, en ouverture, en résilience et en efficacité afin d'offrir aux clients des services plus variés et plus rapidement. En lançant sa plateforme de services d'infrastructure basée sur le* cloud *hybride, Société Générale accélère pour atteindre l'objectif d'héberger 80 % de ses environnements dans le* cloud *(public ou privé) à horizon 2020.*

La transformation numérique s'inscrit au cœur du plan stratégique Transform to Grow *de Société Générale pour saisir les opportunités offertes par les nouvelles technologies, et notamment le* cloud*. En s'inspirant des géants du* Web*, Société Générale a initié dès 2014 une nouvelle approche pour ses infrastructures, pour permettre d'améliorer le* Time to Market *et l'innovation et ainsi mieux servir ses clients. D'abord basée sur un* cloud *privé créé en 2015, la stratégie* Cloud First *de Société Générale s'appuie désormais sur un dispositif de* cloud *hybride.*

La plateforme de services d'infrastructure de Société Générale intègre plusieurs fournisseurs de cloud *aussi bien privé que public. En effet, le* cloud *public est une opportunité majeure pour innover et passer à l'échelle. Les données des clients du Groupe sont hébergées sur son* cloud *privé et Société Générale collabore étroitement avec la BCE pour assurer la conformité réglementaire (audit, protection et localisation des données, réversibilité) de la plateforme et travaille sur un environnement spécifique défini pour assurer un usage conforme et sécurisé des services des principaux fournisseurs de* cloud*.*

Aujourd'hui, 60 % de l'infrastructure du Groupe est dans le cloud*. La plateforme de services* cloud *hybride est accessible depuis mai dernier. Construite et gérée en mode agile, elle offre un accès rapide et en* self-service *à une dizaine de services d'infrastructure et une centaine d'opérations sont réalisables via des APIs à travers un Portail commun aux métiers du Groupe.*

Des outils sont à disposition des développeurs du Groupe pour faciliter l'accès à la plateforme selon des normes et des principes d'architecture et de développement communs. En 2020, l'ensemble des services d'infrastructure de Société Générale seront entièrement automatisés et accessibles. La plateforme offrira une vue consolidée des services cloud *qu'ils soient public ou privé, pour garantir une maîtrise complète du* monitoring*, de la sécurité, de la conformité et de la facturation*. »[125]

[125] « *Société Générale accélère sa stratégie Cloud* », Communiqué du 18/10/2018 https://www.societegenerale.com/fr/newsroom/societe-generale-accelere-sa-strategie-cloud

Lors de la conférence Google Next '19 à San Francisco, le 9 avril 2019, Darryl West, *Group CIO* d'HSBC, a présenté la stratégie de son groupe à l'égard du *cloud*.[126] Le groupe HSBC, qui s'est constitué par croissance externe et repose sur une organisation décentralisée, s'appuie sur une infrastructure ancienne, à base de *mainframes*, qui, bien que fiable, ne dispose pas des structures de base de données propices au *machine learning* et à l'analyse des données. Après avoir laborieusement cherché à exploiter ses données par ses propres moyens, HSBC s'est résolu à adopter une stratégie axée sur le *cloud*.

La banque, qui compte 39 millions de clients dans le monde, est présente dans 66 pays et traite 1,5 trillions de dollars de paiements quotidiens. Certains besoins de calcul impliquent de grands ensembles de données et nécessitent des capacités de calcul brèves et très intenses :

- un exemple est celui de la lutte contre le blanchiment d'argent : « *nous effectuons des analyses sur un énorme ensemble de données avec une grande capacité de calcul pour identifier les schémas (*patterns*) qui révèlent une activité répréhensibles au sein de notre clientèle* ». Il s'agit d'une application qui nécessite des ensembles de données massifs, une grande capacité informatique, mais aussi une capacité de *machine learning* pour déceler un petit nombre d'opérations suspectes au sein d'un énorme gisement d'opérations ;
- un autre est l'analyse des risques de marché : le groupe doit être en mesure d'exécuter régulièrement des simulations complexes de Monte-Carlo portant sur des milliards de transactions pour mieux comprendre et mieux gérer son exposition aux risques de marché.

HSBC a engagé depuis 3 ans un partenariat avec Google. Elle recourt par ailleurs aux services d'AWS, au cloud public Azure de Microsoft et à Oracle. La banque travaille avec tous les grands fournisseurs de *cloud* et poursuit une stratégie hybride, identifiant les forces et les faiblesses de chaque fournisseur.

La première application opérationnelle de calcul sur le *cloud* est le calcul de la position de liquidité consolidée du groupe : avant le recours au *cloud*, le calcul prenait entre 9 et 14 heures chaque jour et environ 40 heures à la fin du mois. Désormais, le calcul ne prend plus que 2 à 3 heures, ce qui permet au groupe d'être plus réactif et de mieux maîtriser ses risques.

2.6.2.2 Les règles applicables aux établissements financiers

Le règlement n° 1093/2010 du 24 novembre 2010 instituant l'autorité bancaire européenne (EBA) charge celle-ci d'émettre des orientations et des recommandations, dans l'objectif d'établir des pratiques de surveillance cohérentes, efficientes et effectives au sein du système européen de surveillance financière (SESF) et d'assurer une application commune, uniforme et cohérente du droit de l'Union. Les autorités compétentes et les établissements financiers sont tenus de tout mettre en œuvre pour respecter ces orientations et recommandations[127].

C'est dans ce cadre que l'EBA a publié le 25 février 2019 des orientations relatives à l'externalisation, qui précisent les dispositifs en matière de gouvernance interne, y compris en termes de gestion saine des risques, que les établissements, les établissements de paiement et les établissements de monnaie électronique doivent mettre en œuvre lorsqu'ils externalisent des fonctions, en particulier en ce qui concerne l'externalisation de fonctions critiques ou importantes. Ces orientations sont applicables depuis le 30 septembre 2019 à tous les accords d'externalisation conclus, révisés ou modifiés à partir de cette date, et en principe au plus tard le 31 décembre 2021 à tous les accords existants. Les

[126] Conférence "Google Cloud Next '19", April 9-11, 2019, Moscone Center, San Francisco
https://cloud.withgoogle.com/next/19/sf/speakers?session=GENKEY05
https://www.youtube.com/watch?v=NS2mgBW_eS0&feature=youtu.be

[127] Cf. Règlement n° 1093/2010 du 24 novembre 2010 instituant l'autorité bancaire européenne (ABE), Article 16

recommandations de l'EBA du 28 mars 2018 sur l'externalisation vers des fournisseurs de services en nuage[128] sont abrogées à compter du 30 septembre 2019.[129]

Dans le cadre de leur dispositif de gestion des risques, les établissements financiers doivent tenir à jour un registre comprenant des informations sur tous leurs dispositifs d'externalisation, en faisant une distinction entre l'externalisation de fonctions critiques ou importantes et les externalisations portant sur d'autres fonctions. En cas d'externalisation vers un prestataire de services *cloud*, le registre doit indiquer les modèles de services et de déploiement (*cloud* public, privé, hybride ou communautaire), la nature spécifique des données conservées et les lieux (c.-à-d. les pays ou régions) où ces données seront stockées.

Dans le contexte de services *cloud*, les établissements financiers doivent définir les exigences de sécurité des données et des systèmes dans le cadre du dispositif d'externalisation et doivent contrôler en permanence le respect de ces exigences. Ils doivent adopter une approche par les risques en ce qui concerne les lieux de stockage et de traitement des données, ainsi que les considérations relatives à la sécurité informatique.

2.6.3 La localisation sur le territoire européen des données de paiement hébergées sur le *cloud*

2.6.3.1 *La localisation des données est déjà offerte par certains acteurs majeurs du* cloud *public*

Microsoft, rencontré par la mission, nous a dit ne pas redouter une obligation de localisation sur le territoire européen de certaines données[130]. Les utilisateurs du service *cloud* de Microsoft (Azure) auraient la possibilité de choisir que les données confiées dans le cadre de ce service soient exclusivement hébergées sur des serveurs situés sur une certaine zone géographique, France ou Europe.

Microsoft reconnaît être soumis au CLOUD Act et, à ce titre ou à d'autres, à de multiples demandes de communication d'informations par de nombreuses autorités nationales. Il publie deux fois par an le nombre des demandes qui lui sont faites et le sort de ces demandes[131]. Ainsi, au premier semestre 2019, au total, 24 175 demandes ont été reçues concernant 43 727 clients.

Après analyse par les services juridiques de Microsoft, 27 % de ces demandes ont été repoussées ; 14 % se sont avérées infructueuses ; 53 % ont donné lieu à la communication de données de contexte ; dans seulement 5 % des cas, le contenu des données demandées a été transmis aux autorités. La France, à elle seule, représentait d'ailleurs 3 656 demandes, soit 15 % du total (rejetées à 46 % et infructueuses dans 12 % des cas ; pour le solde, seules des données de contexte ont été transmises).

Au regard de ces volumes, il est intéressant de noter que le nombre des demandes émises par les autorités américaines et portant sur des données stockées hors des Etats-Unis n'a concerné au premier semestre 2019 que 126 personnes physiques et une seule entreprise.

---

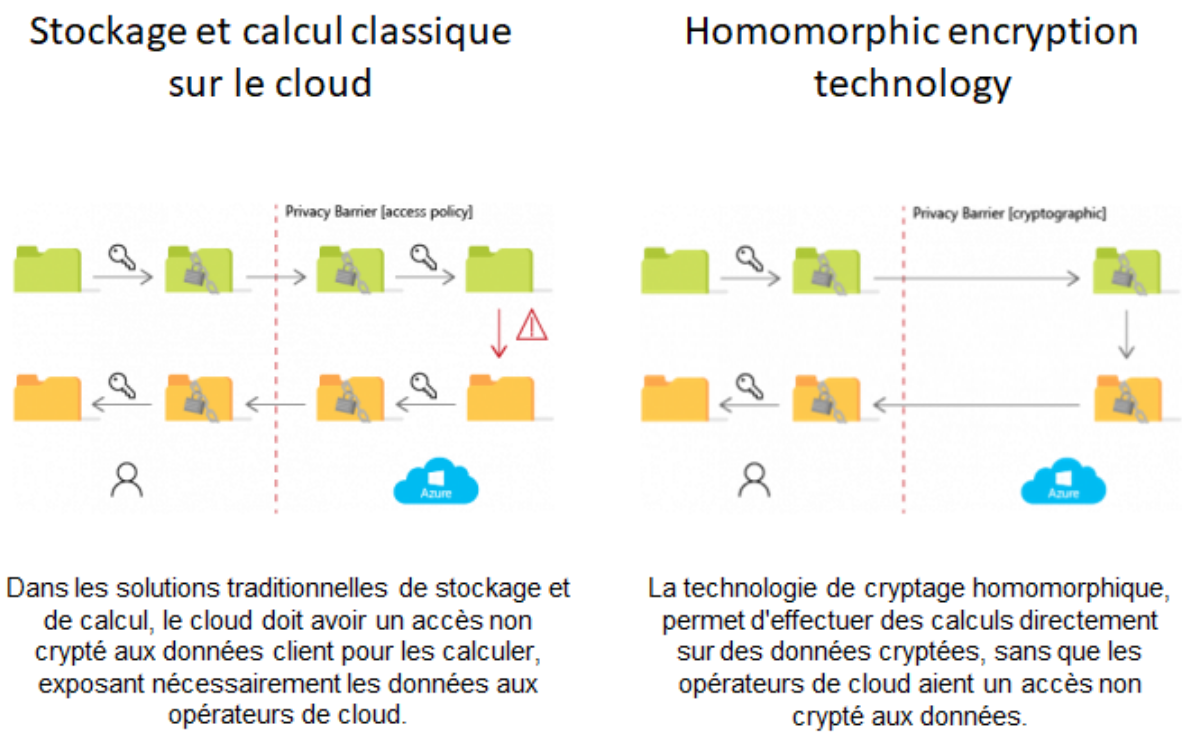
[128] « *Recommandations sur l'externalisation vers des fournisseurs de services en nuage* », EBA, 28 mars 2018 https://eba.europa.eu/sites/default/documents/files/documents/10180/2170125/de3571be-cdba-4c42-997e-98ec85eac7c2/Recommendations%20on%20Cloud%20Outsourcing%20(EBA-Rec-2017-03)_FR.pdf

[129] « *Orientations relatives à l'externalisation* », EBA, 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

[130] Cf. aussi le *code of conduct* élaboré par Cloud Infrastructure Services Providers in Europe (CISPE), association dont l'objectif est de développer la compréhension et la promotion de l'utilisation des services d'infrastructure cloud dans l'Espace économique européen (EEE) https://cispe.cloud/code-of-conduct/

[131] "*Law enforcement requests report*" https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report

A ses clients potentiels qui craignent le plus la divulgation de leurs données, Microsoft propose de crypter leurs données et de conserver la clé. Nul autre que le client n'a la capacité de décrypter les informations, et notamment pas Microsoft. Si ces données venaient à être visées par un mandat des autorités américaines, Microsoft serait dans l'incapacité de livrer à celles-ci autre chose que des données cryptées – et les autorités américaines ne sauraient elles-mêmes rien en tirer.



Des nouvelles techniques de cryptage homomorphe[132] permettent en effet de stocker sur le *cloud* des données cryptées et d'effectuer certains calculs sur ces données sans avoir besoin de les décrypter – et donc sans que le prestataire de service *cloud* ait nécessité de savoir décrypter les données.

2.6.3.2 Localisation des données de paiement et service cloud

L'utilisation par de très nombreuses entreprises de services de *cloud* public ne semble pas faire obstacle à la mise en œuvre d'une décision de localisation des données de paiement sur le territoire européen. De nouvelles organisations permettent aux entreprise de ne plus dépendre d'un prestataire unique de *cloud* public : le *cloud* hybride (un client peut associer ses propres serveurs et ceux qu'il loue à des tiers) et le multi-*cloud* (un client utilise plusieurs prestataires de *cloud* public différents). S'agissant plus spécifiquement des données de paiement, et sous réserve d'un examen plus approfondi avec l'ensemble des acteurs concernés, la CNIL et l'ANSSI, plusieurs solutions semblent possibles.

La première consiste à privilégier l'offre de services *cloud* nativement européens (OVH, OUTSCALE, GAIA-X…). La deuxième repose sur un engagement contractuel des grands prestataires mondiaux de services *cloud* d'assurer le stockage et le traitement des données sur le territoire européen. Dans les deux cas, le cryptage homomorphe peut assurer une sécurité supplémentaire.

S'agissant des établissements financiers régulés, les orientations de l'EBA (cf. chapitre 2.6.2.2 p. 71) pourraient être renforcées :

---

[132] "*Homomorphic Encryption*", Microsoft, March 27, 2016
https://www.microsoft.com/en-us/research/project/homomorphic-encryption/

Recommandation n° 6.	Lorsque des établissements financiers européens externalisent le stockage ou le traitement de données de paiement sur le *cloud*, ils devraient être incités : - à recourir de préférence à un prestataire européen de services *cloud* ; - à défaut, à exiger que le prestataire *cloud* s'engage contractuellement à ce que les données soient détenues et traitées en Europe ; - à exiger que les données de paiement soient chiffrées dans des conditions telles que le prestataire de services *cloud* ne puisse lui-même les décrypter.

Le programme d'étude 2019-2020 de la CNIL prévoit qu'elle fera un état des lieux technique et précis sur les infrastructures et services cloud. Ces travaux devraient lui permettre d'actualiser ses recommandations et d'identifier de nouveaux leviers de régulation de ce secteur.

2.7 Les initiatives reposant sur la blockchain

La lettre du 19 juin 2019 du ministre de l'économie nous engageait à tenir compte des profondes évolutions du secteur d'activité des services de paiement, caractérisé par l'émergence de nouvelles solutions de paiement et par l'expérimentation de nouvelles technologies telles que la *blockchain*.

2.7.1 Le projet Libra de Facebook

L'annonce[133] quasi-concomitante par Facebook du lancement d'un projet de système de paiement, engagé alors depuis plus d'un an, reposant sur une crypto-monnaie dont la valeur est associée à un panier de monnaies[134], et fédérant de nombreux acteurs internationaux de premier plan (parmi lesquels Visa, MasterCard, Uber, Spotify, eBay et PayPal), ne pouvait manquer d'appeler l'attention de la mission.

L'initiative de Facebook était saluée comme un événement majeur : « *l'effort, s'il réussit, menace de bouleverser la plomberie traditionnelle et lucrative du commerce électronique et serait probablement l'application la plus courante à ce jour de la crypto-monnaie* »[135]. Mais le projet Libra a immédiatement suscité l'attention et les réserves des autorités, aux Etats-Unis et en Europe.

Le jour même de l'annonce du projet Libra, le 18 juin 2019, le ministre français de l'économie déclarait : « *Que Facebook créé un instrument de transaction, pourquoi pas. En revanche, que ça devienne une monnaie souveraine, il ne peut pas en être question* »[136]. Il annonçait également avoir demandé aux

---

[133] "Facebook Plans Global Financial System Based on Cryptocurrency", New-York Times, June 18, 2019 https://www.nytimes.com/2019/06/18/technology/facebook-cryptocurrency-libra.html?action=click&module=Top%20Stories&pgtype=Homepage

[134] D'où le terme de *stablecoin* élaboré pour différencier crypto-monnaies associées à ce type d'initiatives des crypto-monnaies dont la valeur est purement spéculative, telles que le bitcoin ou l'ethereum

[135] "*Facebook Building Cryptocurrency-Based Payments System – Social-media giant is recruiting financial firms, merchants to help launch payments platform*", Wall Street Journal, May 2, 2019 https://www.wsj.com/articles/facebook-building-cryptocurrency-based-payments-system-11556837547

[136] « *Facebook va créer sa monnaie : "Nous allons demander des garanties", prévient Bruno Le Maire* », interview sur Europe 1, 18 juin 2019 https://www.europe1.fr/economie/facebook-va-creer-sa-monnaie-nous-allons-demander-des-garanties-previent-bruno-le-maire-3905215

gouverneurs des banques centrales des sept pays membres du G7 un rapport sur les garanties qu'il faut fixer pour s'assurer qu'il n'y a pas de risque de financement illicite ou de risque pour le consommateur.

Les 17 et 18 juillet 2019, les Ministres des finances et les Gouverneurs de banque centrale du G7, réunis à Chantilly, ont reconnu que « *si l'innovation dans le secteur financier peut apporter des avantages substantiels, elle peut également comporter des risques. Ils sont convenus que les* stablecoins*, et les autres nouveaux produits en cours d'élaboration, y compris les projets ayant une empreinte mondiale et potentiellement systémique comme Libra, soulèvent de graves préoccupations tant réglementaires que systémiques, ainsi que des enjeux de politiques publiques, qui doivent tous être traités avant que ces projets ne puissent être mis en œuvre.*

En ce qui concerne les préoccupations réglementaires, les Ministres et les Gouverneurs sont convenus que les éventuelles initiatives de type stablecoins *et leurs opérateurs devraient en tout état de cause satisfaire aux normes les plus élevées de réglementation financière, en particulier en matière de lutte contre le blanchiment et de financement du terrorisme, afin de garantir qu'elles n'affectent ni la stabilité du système financier, ni la protection des consommateurs. Les éventuelles lacunes réglementaires devraient également être comblées.*

En ce qui concerne les préoccupations systémiques, les Ministres et les Gouverneurs sont convenus que des projets comme le Libra peuvent affecter la souveraineté monétaire et le fonctionnement du système monétaire international. Les Ministres et les Gouverneurs sont pour autant convenus que ces projets soulignaient la nécessité d'améliorer sensiblement les systèmes de paiements transfrontaliers et de les rendre moins coûteux pour les consommateurs. Les Ministres et les Gouverneurs ont salué les conclusions préliminaires du groupe de travail du G7 sur les stablecoins*, coordonné par Benoît Cœuré, président du Comité des paiements et des infrastructures de marché, et ont appelé à approfondir les questions précitées*. »

Le rapport final du groupe de travail[137], publié en octobre 2019, relève que les systèmes de paiement actuels, malgré l'accomplissement de progrès importants, présentent deux lacunes majeures : une grande partie de la population mondiale n'y a pas accès et les paiements de détail transfrontaliers restent inefficaces. À l'échelle mondiale, 1,7 milliard d'adultes n'ont pas accès à un compte de transaction, même si 1,1 milliard d'entre eux ont un téléphone mobile[138]. De surcroît, la disposition d'un compte de transaction étant un préalable pour accéder à des services financiers supplémentaires, tels que le crédit, l'épargne et l'assurance, le manque d'accès à des comptes de transaction entrave l'inclusion financière[139].

Les utilisateurs de la première vague de crypto-actifs, tels que le bitcoin, ont pâti de prix très volatils, d'interfaces utilisateur compliquées, de carences de gouvernance et de conformité à la réglementation. Ces crypto-actifs ont pu être utilisés pour leur caractère spéculatif ou en tant que moyen de se livrer à des activités illicites, mais ils n'ont pas permis de répondre aux lacunes des systèmes de paiement existants. Il existe donc un espace de progrès pour de nouvelles initiatives, qu'elles reposent sur des crypto-actifs plus stables (*stablecoins*) ou sur d'autres technologies émergentes.

---

[137] "*Investigating the impact of global stablecoins*", Committee on Payments and Market Infrastructures (CPMI), G7 Working Group on Stablecoins, october 2019
https://www.bis.org/cpmi/publ/d187.pdf

[138] "*The Global Findex Database 2017: measuring financial inclusion and the fintech revolution*", the World Bank, April 2018
http://documents.worldbank.org/curated/en/332881525873182837/pdf/126033-PUB-PUBLIC-pubdate-4-19-2018.pdf

[139] « *Fintech for the people* », Keynote speech by Benoît Cœuré, Chair of the CPMI and Member of the Executive Board of the ECB, at the 14th BCBS-FSI high-level meeting for Africa on strengthening financial sector supervision and current regulatory priorities, Cape Town, 31 January 2019,
https://www.ecb.europa.eu/press/key/date/2019/html/ecb.sp190131~24b8e3fb49.en.html

Toutefois, les avantages éventuels de ces nouvelles initiatives à base de *stablecoins* ne pourraient être exploitées si sur les plans juridique, de régulation et de supervision elles soulevaient par ailleurs des risques importants, détaillés dans le rapport Cœuré et liés :

- à la sécurité juridique,
- à l'existence d'une gouvernance robuste (notamment en ce qui concerne les règles d'investissement et le mécanisme de stabilité de la valeur du crypto-actif),
- au blanchiment d'argent, au financement du terrorisme ou à toute autres formes d'activité financière illicite,
- à la sécurité, à l'efficacité et à l'intégrité des systèmes de paiement,
- à la cyber-sécurité et à la résilience opérationnelle,
- à l'intégrité du marché,
- à la confidentialité, à la protection et à la portabilité des données,
- à la protection des consommateurs et des investisseurs,
- à la conformité à la législation fiscale.

En outre, si ces initiatives étaient appelées à prendre une dimension mondiale (*global stablecoins*), il conviendrait également d'apporter des réponses aux défis qu'elles pourraient représenter pour la conduite de la politique monétaire et pour la stabilité financière, ainsi qu'aux menaces qu'elles pourraient faire naître sur le système monétaire international et sur la libre concurrence.

A la lumière des réactions internationales, Facebook a annoncé le 15 juillet 2019[140] qu'il renonçait à la mise en œuvre de son projet tant que les questions réglementaires ne seraient pas réglées et que le Libra n'aurait pas reçu les approbations nécessaires. Parmi les 28 institutions qui avaient soutenu le projet Libra, PayPal a annoncé son retrait le 4 octobre 2019[141], et eBay, Mastercard, Stripe et Visa[142] le 11 octobre 2019.

Le 27 décembre 2019, le président et ministre des Finances de la Suisse, pays où le projet cherche à obtenir un agrément, a déclaré dans une interview qu'il ne pensait pas que le Libra avait une chance dans sa forme actuelle, estimant que les banques centrales n'accepteraient pas le panier de devises qui sous-tend la crypto-monnaie. Selon lui, le projet, sous cette forme, a donc échoué[143].

2.7.2 Les projets de monnaie digitale de banque centrale

Le projet Libra a relancé l'intérêt pour les projets de monnaie digitale de banque centrale (*central bank digital currencies* ou CBDC), définie comme une « *nouvelle forme numérique de monnaie de banque centrale qui diffère des comptes de réserve ou de règlement traditionnels inscrits au nom des banques*

---

[140] "*Facebook Says Libra Won't Launch Until Regulators Satisfied*", Bloomberg, 15 juillet 2019 https://www.bloomberg.com/news/articles/2019-07-15/facebook-says-libra-won-t-launch-until-regulators-satisfied

[141] "*PayPal withdraws from Facebook's libra cryptocurrency*", CNBC, October 4, 2019 https://www.cnbc.com/2019/10/04/paypal-withdraws-from-facebooks-libra-cryptocurrency.html

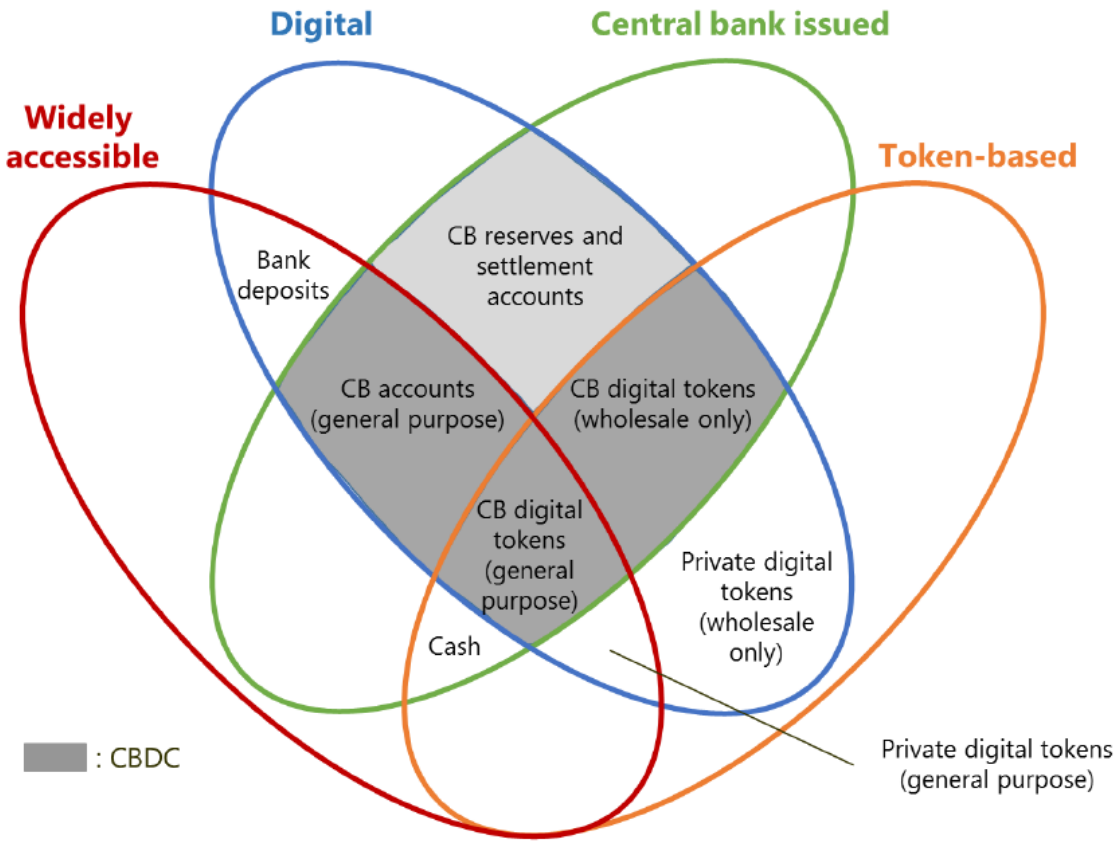
[142] "*Facebook's libra cryptocurrency coalition is falling apart as eBay, Visa, Mastercard and Stripe jump ship*", CNBC, October 11, 2019 https://www.cnbc.com/2019/10/11/ebay-drops-out-of-facebook-libra-cryptocurrency-one-week-after-paypal.html

[143] "*Facebook's Libra has failed in current form: Swiss president*", Reuters, December 27, 2019 https://www.reuters.com/article/us-facebook-cryptocurrency/facebooks-libra-has-failed-in-current-form-swiss-president-idUSKBN1YV1G8

commerciales par les banques centrales »[144]. Selon Agustín Carstens, General Manager à la Banque des règlements internationaux, « *les tentatives pour créer de nouvelles formes d'argent ou pour concevoir de nouvelles façons de payer apparaissent presque chaque semaine* » ; et à leur tour, environ 70 % des banques centrales explorent ou expérimentent les CBDC.[145]

Une CBDC peut reposer sur des choix de conception très variés, selon notamment que l'accès à cette monnaie est limité ou très large (une CBDC de gros serait limité à un groupe limité d'utilisateurs et utilisé pour les paiements interbancaires et d'autres transactions de règlement ; une CBDC de détail serait accessible au grand public), que l'anonymat des transactions est assuré ou non (dans le premier cas, par un dispositif reposant sur des *tokens*[146] ; dans le second, par l'ouverture de comptes traditionnels) ; que les opérations sont admises aux seules heures de bureau ou au contraire 24 heures sur 24, 7 jours sur 7 ; et selon que les dépôts procurent ou non des intérêts.

Le diagramme ci-dessous, extrait de *Central bank digital currencies* (cf. note 144), expose selon ces différents critères les différentes formes de monnaie possible, qu'elle soit émise par une banque centrale ou non. *Private digital tokens (general purpose)* désigne les crypto-actifs tels que le bitcoin, l'ethereum et, le cas échéant, les *stablecoins*.



[144] "*Central bank digital currencies*", Committee on Payments and Market Infrastructures and Markets Committee, CPMI Papers, no 174, March 2018
https://www.bis.org/cpmi/publ/d174.pdf

[145] "*The future of money and payments*", Speech by Mr Agustín Carstens, General Manager of the BIS, at the Central Bank of Ireland, 2019 Whitaker Lecture, Dublin, 22 March 2019
https://www.bis.org/speeches/sp190322.htm

[146] Le mot *token* est employé dans le contexte de la monnaie digitale de banque centrale ou des crypto-actifs dans un sens différent de celui qu'il revêt au chapitre 2.3 (*tokenisation* d'un numéro de carte bancaire ou d'une autre donnée sensible, afin de l'occulter). Une monnaie digitale de banque centrale anonyme, bien qu'on parle alors de *tokens*, ne reposerait pas nécessairement sur la *blockchain* ; elle pourrait plutôt s'apparenter à la monnaie électronique (disponible par exemple sous la forme de cartes pré-payées)

L'alternative publique aux *stablecoins*, qui se rattachent sur le schéma aux *Private digital tokens (general purpose)*, pourrait être une CBDC de détail reposant sur l'émission de *tokens* – sur le schéma : *CB digital tokens (general purpose)*. Mais les CBDC de détail ne sont pas une panacée. Elles présentent elles-aussi des risques mal évalués à ce stade sur le plan de la stabilité monétaire et financière[147] :

- elles peuvent engendrer une certaine instabilité des dépôts des banques commerciales et une déstabilisation du financement de l'économie par les banques commerciales ;
- en période de crise, des mouvements brutaux et à grande échelle de conversion des dépôts des banques commerciales vers la monnaie digitale de banque centrale (*flight to quality*) pourraient se produire ;
- un rôle plus important pour la banque centrale dans l'allocation des ressources économiques pourrait provoquer des risques politiques et s'avérer inefficace pour l'économie.

Au même titre que les *stablecoins*, les CDBC de détail soulèvent des risques qui doivent aussi être circonscrits : blanchiment d'argent sale, financement du terrorisme, développement de l'économie souterraine… Enfin, le lancement d'une CBDC de détail induirait d'importantes conséquences opérationnelles pour les banques centrales dans la mise en œuvre de la politique monétaire et pourrait avoir des répercussions sur la stabilité du système financier.

Dans un discours récent, le Gouverneur de la Banque de France a fait part de son intérêt et de sa perception des enjeux[148], en estimant que « *nous, banques centrales, devons et voulons saisir cette injonction à l'innovation alors que les initiatives privées – notamment dans les paiements entre acteurs financiers – et la technologie accélèrent, et que la demande publique et politique s'amplifie* », et que la mise en place d'une CDBC nous permettrait de disposer d'un puissant levier d'affirmation de notre souveraineté face aux initiatives privées du type Libra.

A côté d'une CDBC de gros, utilisant la *blockchain* et toutes ses possibilités, notamment la disponibilité de *smart contracts*, et sur laquelle il est plus facile d'avancer rapidement, il souhaite poursuivre la réflexion sur la possibilité d'une CDBC de détail, à même de traiter des opérations de masse. Il semble estimer que, lorsque les difficultés soulevées auront été maîtrisées, la distribution de la CBDC s'effectuerait plutôt sous forme de comptes que de *tokens* (ce qui exclurait donc le recours à la *blockchain*), des seuils étant éventuellement fixés sur les montants de transactions anonymes.

2.7.3 Les enjeux de données propres à la *blockchain*

Les *blockchains* sont des technologies de stockage et de transmission d'informations, utilisant des réseaux décentralisés pair à pair, sans organe central de contrôle, sécurisés grâce à la cryptographie. Ce sont les technologies sous-jacentes aux crypto-monnaies, comme le bitcoin, mais elles ont aussi d'autres applications potentielles (l'état civil, le cadastre, les contrats de type notarié, la protection de la propriété intellectuelle…). Cette technologie repose sur un registre public réputé infalsifiable appelé *blockchain*. Il s'agit d'une base de données distribuée, c'est-à-dire qu'elle est enregistrée sur chacun des nœuds d'un réseau d'ordinateurs interconnectés. Toutes les transactions sont vérifiées par les nœuds du réseau.

Dans la version d'origine de la *blockchain*, apparue en 2008 comme partie intégrante du bitcoin[149], certains nœuds du réseau, qualifiés de « mineurs », disposant de puissants moyens de calcul, vérifient,

---

[147] "*The future of central bank money*", Speech by Benoît Cœuré, Member of the Executive Board of the ECB, at the International Center for Monetary and Banking Studies, Geneva, 14 May 2018 https://www.ecb.europa.eu/press/key/date/2018/html/ecb.sp180514_4.en.html

[148] « *Monnaie digitale de banque centrale et paiements innovants* », Discours de François Villeroy de Galhau, 04/12/2019 https://www.banque-france.fr/intervention/monnaie-digitale-de-banque-centrale-et-paiements-innovants

[149] "*Bitcoin: A Peer-to-Peer Electronic Cash System*", Satoshi Nakamoto, 2008 https://bitcoin.org/bitcoin.pdf

enregistrent et sécurisent les transactions. Celles-ci sont groupées dans des blocs, qui seront ensuite « enchaînés » les uns à la suite des autres pour former la *blockchain*. Le dernier bloc en date est ajouté au précédent (celui-ci étant dit « miné ») par le premier « mineur » qui réussit à résoudre un problème cryptographique difficile appelé « preuve de travail ». Ce mineur reçoit alors une certaine somme de bitcoins en récompense de sa réussite, et le nouveau bloc se propage à l'ensemble des nœuds du réseau.[150]

Par extension, la *blockchain* est une base de données distribuée, capable de gérer une liste d'enregistrements protégés contre la falsification ou la modification par les nœuds de stockage ; c'est donc un registre distribué et sécurisé de toutes les transactions effectuées depuis le démarrage du système réparti. Dans une acception large du concept de blockchain, celle-ci peut être gérée de manière plus ou moins décentralisée :

- une *blockchain* publique (c'est-à-dire un registre ouvert à tous) se caractérise par son ouverture totale et décentralisée : tout le monde peut y accéder et effectuer des transactions et tout le monde peut participer au processus de consensus. Il n'y a donc pas de tiers de confiance. C'est le modèle le plus connu, qui est à l'origine du bitcoin, et qui répond à une approche libertaire ;
- dans une *blockchain* à permission, ou « de consortium », le processus de consensus est contrôlé par un ensemble présélectionné de nœuds ; par exemple, on pourrait imaginer un consortium de 15 institutions financières, dont chacune opère un nœud et dont 10 doivent signer chaque bloc pour que le bloc soit valide. L'accès à cette *blockchain* peut être public ou restreint aux participants selon un processus de cooptation ;
- certaines *blockchains* sont totalement privées : l'accès d'écriture est délivré par une organisation centralisée, les autorisations de lecture peuvent être publiques ou restreintes. Il s'agit typiquement de l'utilisation à laquelle travaillent certains organismes de règlement-livraison de titres ou certaines banques centrales pour les opérations de règlement de devises en monnaie banque centrale[151].

> **L'utilisation d'une *blockchain* publique pour gérer des transactions de paiement entre personnes physiques apparaît, par nature, difficilement conciliable avec la mise en œuvre d'une obligation de localisation des données de paiement – et peut-être même avec le RGPD. La CNIL constate toutefois[152] que « *les* blockchains *sont des objets protéiformes et que les choix opérés par le responsable de traitement (entre une* blockchain *à permission ou une* blockchain *publique, entre différents formats pour l'inscription de la donnée dans les blocs, etc.) peuvent impacter significativement, à la hausse ou à la baisse, les risques sur les droits et les libertés des personnes* ». A ce stade, les projets de *stablecoins* comme ceux de monnaie**

[150] « *La blockchain – Les défis de son implémentation* », Ilarion Pavel, les Annales des mines, Réalités industrielles, août 2017
http://www.annales.org/ri/2017/ri-aout-2017/RI-AOUT-2017-Article-PAVEL.pdf

[151] Extrait de l'article : « *La blockchain et la loi* », Hubert de Vauplane, Revue banque, 26/02/2016
http://www.revue-banque.fr/risques-reglementations/chronique/blockchain-loi

[152] « *Blockchain et RGPD : quelles solutions pour un usage responsable en présence de données personnelles ?* », CNIL, 24 septembre 2018
https://www.cnil.fr/fr/blockchain-et-rgpd-quelles-solutions-pour-un-usage-responsable-en-presence-de-donnees-personnelles

digitale de banque centrale de détail apparaissent trop peu avancés pour une analyse plus approfondie des enjeux de la localisation des données.

À Paris, le 4 février 2020,

L'ingénieure générale des mines,

Sandrine Lemery

L'ingénieur général des mines,

Rémi Steiner

ANNEXES

Annexe 1 : Lettre de mission

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Paris, le 19 JUIN 2019

Le Ministre de l'Economie et des Finances

à

Monsieur le Vice-Président du Conseil général de l'Economie

Objet : Mission d'étude sur la mise en œuvre d'une politique de localisation des données critiques de paiement en Europe

Le Comité National des Paiements Scripturaux a entériné le 18 février 2019 une mise à jour de la stratégie nationale sur les moyens de paiement scripturaux, couvrant les années 2019 à 2024. Il y figure un sujet de préoccupation croissante, qui consiste à mieux assurer l'indépendance du marché et des acteurs européens dans le domaine des paiements, en favorisant le traitement au sein de l'Union européenne des données critiques relatives aux transactions de paiement.

Ces données critiques de paiement s'entendent naturellement des données de paiement sensibles[1], susceptibles d'être utilisées pour commettre une fraude (telles que les données personnalisées d'authentification d'un client auprès de son prestataire de services de paiement) ; mais également des données liées au contexte des transactions de paiement et qui ont trait, par exemple, aux habitudes des consommateurs ou à leur géolocalisation.

Dans toute la mesure du possible, il convient de tenir compte des profondes évolutions de ce secteur d'activité, caractérisées par l'émergence de nouvelles solutions de paiement (reposant notamment sur le paiement instantané), par l'expérimentation de nouvelles technologies (parmi lesquelles la *blockchain*, l'intelligence artificielle et l'identification biométrique), ainsi que par l'essor continu des paiements à distance.

Il convient également de prendre en considération les effets induits par le règlement général sur la protection des données personnelles[2] (RGPD), par la deuxième directive sur

[1] Définies à l'article 4 de la directive 2015/2366 du 25 novembre 2015 concernant les services de paiement dans le marché intérieur (DSP2)

[2] Règlement 2016/679 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

MINISTÈRE DE L'ÉCONOMIE ET DES FINANCES

services de paiement (DSP2) et par le règlement délégué pris pour son application, qui définit de nouvelles normes d'authentification forte et de communication[3].

Le risque d'atteintes à des données critiques de paiement concerne *a priori* l'ensemble des acteurs de la chaîne des paiements :

- les établissements financiers régulés soumis aux dispositions de la DSP2 et de son règlement délégué (établissements de crédit, établissements de paiement, agrégateurs de comptes ; acteurs anciens ou nouveaux entrants ; agréés par l'ACPR ou intervenant en libre prestation de services) ;
- les entreprises non régulées qui peuvent intervenir aux côtés d'un établissement financier, soit en tant qu'agent de celui-ci, soit en tant que sous-traitant d'une fonction opérationnelle importante (par exemple, l'hébergement de données ou de programmes sur le *cloud*) ; des dispositions particulières de la DSP2 et du RGPD encadrent de telles situations de sous-traitance ;
- les commerçants en ligne, notamment lorsqu'ils s'organisent pour limiter le recours à l'authentification forte de leurs clients à l'aide de systèmes d'analyse du risque[4] de chaque opération de paiement spécifique.

En appui du Comité national des paiements scripturaux, je souhaite que le Conseil général de l'économie conduise une analyse visant à apprécier l'importance et la sensibilité des traitements extra-européens portant sur des données critiques de paiement, ainsi que les enjeux de souveraineté qui pourraient en résulter pour les ressortissants européens. Il devra exposer toutes les recommandations qui lui paraîtront utiles, que ces recommandations s'adressent aux pouvoirs publics, aux établissements financiers, à leurs agents et à leurs sous-traitants, ou aux commerçants en ligne.

Vous mènerez cette mission en vous appuyant sur les travaux de l'Observatoire de la sécurité des moyens de paiement, en étroite relation avec les services compétents de la Banque de France, de l'ACPR, de la CNIL et de l'ANSSI. Vous bénéficierez de l'appui des services du ministère, notamment de la Direction générale du Trésor et de ses services économiques régionaux, ainsi que de la Direction générale des entreprises. Vous me remettrez votre rapport dans un délai de six mois.

Bruno LE MAIRE

[3] Règlement délégué 2018/389 de la Commission du 27 novembre 2017 complétant la directive 2015/2366 par des normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication

[4] cf. article 18 du règlement délégué du 27 novembre 2017

Annexe 2 : Liste des acronymes et expressions étrangères utilisés

ACPR	Autorité de contrôle prudentiel et de résolution, chargée de la supervision des établissements financiers (banques, assurances, établissements de paiement…)
amicus curiae	Du latin « ami de la cour », celui qui assiste la cour en fournissant des informations ou des conseils sur des questions de droit ou de fait
ANSSI	Agence nationale pour la sécurité des systèmes d'information
back-up	Dans les technologies de l'information, copie de données informatiques prises et stockées ailleurs afin de pouvoir être utilisées pour restaurer l'original après un événement de perte de données.
BCE	Banque centrale européenne
BIN	*Bank identification number*, ou numéro d'identification bancaire : ce sont les premiers chiffres d'un numéro de carte qui permettent d'identifier l'émetteur. Les numéros restants sur la carte, à l'exception du dernier chiffre, qui est une clé de vérification de la cohérence du numéro, sont le numéro d'identification de compte individuel.
blockchain	Technologie de stockage et de transmission d'informations, utilisant des réseaux décentralisés pair à pair, sans organe central de contrôle, et sécurisés grâce à la cryptographie (cf. chapitre 2.7.3 p. 78)
by design	Par construction, prévu dès la conception
card-on-file	Collecte et de stockage des informations de paiement pour une utilisation future (paiements récurrents, paiement en 1 click…)
CBDC	*Central bank digital currency* (monnaie digitale de banque centrale)
CGE	Conseil général de l'Economie
CIA	Central Intelligence Agency, service civil de renseignement étranger du gouvernement fédéral des États-Unis, chargé de recueillir, de traiter et d'analyser les informations de sécurité nationale
CLOUD Act	*Clarifying Lawful Overseas Use of Data Act*, loi fédérale des États-Unis promulguée en 2018 pour permettre aux forces de l'ordre fédérales d'obliger sous certaines conditions les sociétés technologiques basées aux États-Unis à fournir les données stockées sur leurs serveurs, qu'elles soient stockées aux États-Unis ou sur un sol étranger (cf. chapitre 1.1.5 p. 15)
cloud public	Ensemble de services informatiques proposés par des fournisseurs tiers sur l'internet public, facturés selon le temps de calcul, le volume de données ou la bande passante qu'ils consomment
CMI	Commission multilatérale d'interchange
CNIL	Commission nationale informatique et liberté
CNPS	Comité national des paiements scripturaux
datacenter	Espace dédié dans un bâtiment ou un groupe de bâtiments utilisé pour abriter des systèmes informatiques et des composants associés, tels que les télécommunications et les systèmes de stockage
de-tokenisation	Reconstitution par le calcul d'une donnée sensible à laquelle on avait substitué un token (cf. ce mot)

digital wallet	Porte-monnaie électronique
discovery	Dans les juridictions de common law, procédure préalable au procès dans laquelle chaque partie, par le biais du droit de la procédure civile, peut obtenir des preuves de l'autre partie ou des autres parties au moyen d'interrogatoires, de demandes de production de documents…
DoJ	*Department of Justice* (ministère américain de la justice)
DSP2	2ème directive sur les services de paiement (Directive 2015/2366 du 25 novembre 2015 concernant les services de paiement dans le marché intérieur)
EBA	*European banking authority* (autorité bancaire européenne)
EMVCo	Organisme international de standardisation du paiement par carte, promu à l'origine par Eurocard, MasterCard et Visa, pour faciliter l'interopérabilité et l'acceptation des transactions de paiement
EPI	*European payment initiative* : projet d'harmonisation des paiements, mené par de grandes banques européennes
ERPB	L'Euro Retail Payments Board (ERPB) est un organe de gouvernance de l'Union européenne, chargé de favoriser l'intégration, l'innovation et la compétitivité des paiements de détail en euros.
G10	Groupe de banques centrales (cf. chapitre 1.1.1)
G29	Groupe de travail européen qui rassemblant des représentants de chaque autorité nationale de protection des données personnelles avant le RGPD
G7	Groupe de discussion et de partenariat économique constitué entre l'Allemagne, le Canada, les États-Unis, la France, l'Italie, le Japon et le Royaume-Uni
GAFAM	Acronyme désignant Google, Amazon, Facebook, Apple et Microsoft
global stablecoin	*Stablecoin* (cf. ce mot) à vocation mondiale, telle que le projet Libra
guidelines	Lignes directrices
IaaS	*Infrastructure as a service* est l'une des principales composantes du *cloud computing*, qui permet de bénéficier de ressources informatiques virtualisées
IBAN	Système internationalement reconnu d'identification des comptes bancaires au-delà des frontières nationales, conçu pour faciliter la communication et le traitement des transactions transfrontalières
instant payment	Paiement instantané
level playing field	Règles du jeu équitables, garantissant l'égalité des chances entre tous
MLAT	*Mutual legal assistance treaty*, ou traité traité d'entraide judiciaire : accord entre deux États visant à faciliter la coopération policière et judiciaire, notamment en termes d'échanges de renseignements et de données personnelles
NFC	*Near field communication* (protocole de communication utilisé par le paiement sans contact)

NSA	*National Security Agency*, organisme gouvernemental du département de la Défense des États-Unis, responsable du renseignement d'origine électromagnétique et de la sécurité des systèmes d'information du gouvernement américain
OFAC	*Office of Foreign Assets Control*, agence de renseignement financier et d'application des lois rattaché au Département du Trésor des États-Unis ; il administre et applique des sanctions économiques et commerciales à l'appui des objectifs de sécurité nationale et de politique étrangère des États-Unis
on-us	Transaction de paiement dans laquelle la banque émettrice et la banque acquéreur sont identiques ; il n'est alors pas nécessaire de faire intervenir le *scheme* pour l'autorisation et la compensation
P2P	*Peer-to-peer* (de personne à personne)
PaaS	*Platform as a service,* forme de cloud computing, permettant à l'utilisateur de développer des applications
PAN	*Primary account number*, ou numéro de compte principal, ou encore numéro de carte : c'est l'identifiant de carte trouvé sur les cartes bancaires
pattern	Motif régulier, susceptible de se répéter de manière prévisible
PCI DSS	*Payment Card Industry Data Security Standard*, norme de sécurité des données de l'industrie des cartes de paiement
PCI SSC	*Payment Card Industry Security Standards Council*, organisme qui administer le référentiel PCI DSS
PEPS-I	*Pan European Payment System Initiative* : cf. EPI
premium	Une offre premium désigne une version améliorée d'un service donné, vendue plus cher que le service de base, ou la version payante d'un service gratuit
privacy officer	responsable de la protection de la vie privée
processing	traitement
RGPD	Règlement général sur la protection des données à caractère personnel (Règlement 2016/679 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)
SaaS	*Software as a service* est un modèle de distribution de logiciels dans lequel un fournisseur tiers héberge des applications et les met à la disposition des clients sur Internet
scheme	Ensemble des règles de fonctionnement, de responsabilité, de résolution des litiges, etc… instituées par des acteurs du paiement tels que Visa ou MasterCard afin d'assurer le traitement des transactions de paiement
SCT^{inst}	*Scheme* de virement instantané en euros, développé par le Conseil européen des paiements sur la zone SEPA
SDN	*Specially Designated Nationals And Blocked Persons List* (SDN) : liste d'individus, de groupes et d'entités, suspectés de terrorisme ou de trafic de stupéfiants
SEPA	*Single euro payment area* (zone de paiement en euro)

SESF	Système européen de surveillance financière, réseau d'autorités européennes qui comprend le Comité européen du risque systémique, les trois autorités européennes de surveillance (EBA, EIOPA, ESMA) et les autorités nationales de surveillance
smartphone	Téléphone mobile polyvalent permettant la navigation sur internet et des fonctionnalités multimédias, en plus des fonctions téléphoniques de base
soft power	Concept utilisé en relations internationales pour décrire la capacité d'un acteur politique — État, firme multinationale, ONG, institution internationale— d'influencer indirectement le comportement d'un autre acteur à travers des moyens non coercitifs (structurels, culturels ou idéologiques)
stablecoin	Crypto-monnaies conçues pour minimiser la volatilité du prix du Stablecoin, par rapport à un actif ou un panier d'actifs "stable"
SWIFT	*Society for Worldwide Interbank Financial Telecommunications,* coopérative de banques créée en 1973 qui garantit la sécurité des transactions financières. SWIFTNet est le réseau mondial privé de communication bancaire créé par les banques et géré par SWIFT
third party provider	Cette expression désigne deux nouvelles catégories d'établissements de paiement, définies par la DSP2 (cf. ce mot) : les agrégateurs de comptes et les initiateurs de paiement
time to market	Durée de développement et de construction d'une offre commerciale ou d'un produit, capacité à prendre position sur un marché au moment le plus pertinent
TIPS	*TARGET Instant Payment Settlement* (TIPS) est un service d'infrastructure de marché lancé par l'Eurosystème en novembre 2018. Il permet aux prestataires de services de paiement d'offrir des virements de fonds à leurs clients en temps réel, 24h / 24, tous les jours de l'année
token	Pseudonyme destiné à se substituer à une donnée de paiement de paiement sensible ; l'expression est aussi utilisée pour désigner un actif numérique émis et échangeable sur une *blockchain*
tokenisation	Transformation d'une donnée sensible en un *token*
TSP	*Token service provider* (fournisseur de service de *tokens*)
US Department of the Treasury	Département du Trésor des États-Unis

Annexe 3 : Liste des personnes rencontrées ou interrogées

Organismes publics et parapublics

Cabinet du ministre de l'Economie et des finances

- M. Emmanuel Monnet, Conseiller financement de l'économie

Cabinet du secrétaire d'Etat chargé du Numérique

- Mme Carole Vachet, Conseillère régulations et transformations numériques

Assemblée nationale

- M. Raphaël Gauvain, Député

Direction générale du Trésor

- M. Arnaud Delaunay, Chef du bureau services bancaires et moyens de paiement
- M. Clément Robert, Adjoint au chef du bureau services bancaires et moyens de paiement

Direction générale des entreprises

- M. Joffrey Célestin-Urbain, Chef du service de l'information stratégique et de la sécurité économiques
- M. Adrien Bresson, Chef du bureau réseaux et sécurité, service de l'économie numérique
- M. Mickaël Reffay, Head of data economy and software industries projects

Conseil national du numérique

- M. Charles-Pierre Astolfi, Secrétaire général

Banque de France

- M. Julien Lasalle, Chef du service de la surveillance des moyens de paiement scripturaux
- M. Pierre Bienvenu, Service de la surveillance des moyens de paiement scripturaux
- M. Guillaume Bruneau, Service de la surveillance des moyens de paiement scripturaux

Commission nationale informatique et liberté (CNIL)

- M. Paul Hebert, Directeur adjoint de la conformité
- Mme Clémence Scottez, Chef du secteur des affaires économiques
- M. Gaston Gautreneau, Ingénieur expert

Agence nationale de la sécurité des systèmes d'information (ANSSI)

- M. Grégoire Lundi, Coordinateur sectoriel

Autorité de contrôle prudentiel et de résolution (ACPR)

- M. Olivier Fliche, Directeur du pôle fintech innovation
- M. Geoffroy Goffinet, Adjoint au directeur des autorisations
- M. Su Yang, Pôle FinTech Innovation

Organisation professionnelles

Fédération bancaire française (FBF)
- Mme Solenne Lepage, Directrice générale adjointe
- M. Jérôme Raguénès, Directeur du département numérique, systèmes et moyens de paiement

Office de coordination bancaire et financière (OCBF)
- Mme Carole Delorme d'Armaille, Directrice générale
- Mme Anne-Marie Moulin, Directeur pôle juridique, réglementaire et conformité
- M. Olivier Durand, Directeur en charge des sujets de place

FEVAD
- M. Bertrand Pineau, Responsable veille, innovation & développement

Mercatel
- M. Jean-Michel Chavanas, Délégué général

France Fintech
- M. Alain Clot, Président
- M. Benoît Bazzocchi
- Mme Céline Brezin, Project Manager

Consultants et personnalités qualifiées

Edgar, Dunn & Company
- M. Pascal Burg, Director

European Institute of Financial Regulation (EIFR)
- M. Edouard de Lencquesaing, Président

JMG Consulting
- M. Jean-Michel Godeffroy

MS2ii
- Mme Sophia Briouel, CEO

NEXO Standards
- M. Claude Brun, Chairman

Pemance
- M. Régis Bouyala, Partner

PW consultants
- M. Thierry Leblond, Directeur du pôle monétique et moyens de paiement

Université Panthéon Assas (Paris II)
- Mme Bénédicte Fauvarque-Cosson, Conseillère d'Etat

Schemes de paiement et organismes de place

Visa

- M. Romain Boisson, Country manager France
- Mme Pia Sorvillo, Director european regulatory affairs & government relations
- M. Rabah Ghezali, Head of regulatory & government relations France, Monaco, Belgium & Lux.
- M. Jean-François Roche, Deputy director processing, services & support France
- M. Laurent Bailly, Head of digital solutions France, Belgium & Luxemburg

MasterCard

- Mme Solveig Honoré-Hatton, Country manager France
- M. Vincent Richir, Director public policy
- M. Bruno Baugnies, Senior vice president operations & technology
- Mme Delphine Charlot, Senior counsel privacy & data protection

Alipay

- M. Jean-Cyrille Girardin, Director strategic partnerships Europe
- M. Justin Barry, Director of legal & compliance EMEA

Groupement Carte Bancaire

- M. Philippe Laulanie, Administrateur
- Mme Karine Boubel, Secrétaire générale
- M. Loÿs Moulin, Directeur du développement

STET

- M. Jean-Marie Vallée, Directeur général

Fintechs

Bankin

- M. Joan Burkovic, CEO & co-founder

Lydia

- M. Cyril Chiche, CEO

Pumpkin

- M. Constantin Wolfrom, Co Fondateur et CEO

Slimpay

- M. Jérôme Traisnel, CEO

Banques

Groupe BPCE

- M. Jean-Yves Forel, Directeur général
- M. Fabrice Denèle, SVP, Strategy & Partnerships, Natixis Payment Solutions

Crédit Agricole Payment Services

- Mme Narinda You, Directeur de la stratégie et des relations de place

Groupe Société Générale

- M. Philippe Marquetty, Directeur des paiements
- Mme Françoise Mercadel-Delasalle, Directrice Générale Crédit du Nord
- Mme Aurore Gaspar, Directrice générale adjointe Boursorama
- M. Antoine Pichot, Délégué à la Protection des Données

Banque Postale

- M. Régis Folbaum, Directeur des paiements
- Mme Delphine de Chaisemartin, Directrice des affaires publiques et de la communication financière et institutionnelle
- M. François-Régis Benois, Directeur adjoint affaires publiques
- M. Alain Courouble, Directeur des risques opérationnels groupe
- M. Marc Hoffmann, Directeur de la donnée groupe

Groupe Crédit Mutuel

- M. Marc Rainteau, responsable des systèmes bancaires et moyens de paiement
- M. Elbachir Guemouri, Euro information

Crédit Mutuel Arkéa

- M. Ronan le Moal, CEO

ING Bank

- M. Frédéric Niel, Head of retail
- Mme Sarah Soul, Head of payments & cards

HSBC

- M. Arnaud Grass, Head of Payments and GLCM IT, HOST Information Technology

Acteurs techniques du paiement

Adyen
- M. Edouard de Raulin, Head of Sales France

Apple
- M. Gary Davis, Global Director of Privacy & Law Enforcement Requests
- M. Mikael Berrebi, International expansion, strategic partnerships & business development
- M. Prince Zhandire, Counsel
- M. Sébastien Gros, Head of government affairs

Hipay
- M. Grégoire Bourdin, CEO
- M. Mickael Ferraz, Head of legal et data protection officer
- M. Damien Fleuriot, Responsable de l'infrastructure IT et des réseaux, responsable de la sécurité des systèmes d'information

Ingenico
- Mme Odile Caillot, Head of global payment and innovations acceptance

Lyra
- M. Yves Sicouri, Directeur retail

Monext
- M. Frédéric Diverrez, Chairman

Thalès
- M. Alain Martin, Head of consulting & industry relations, banking & payment services
- M. François Chaffard, digital transformation for banking & payment

Transaction Network Services (TNS)
- M. Roger Mechri, Regional Manager France Benelux & DACH
- M. Germain Arilla, Sales executive

Worldline
- Mme Claude France, Directrice générale des opérations France
- M. Pascal Dehaussy, Finance services and equensWorldline France manager
- Mme Sylvie Calsacy, Head of Payment Strategy
- Mme Catherine Lafitte, business development (tokenisation)

Entreprises du commerce

Groupe Carrefour

- M. Frédéric Collardeau, Directeur General Carrefour banque & assurances
- Mme Isabelle Clairac, CEO Market Pay
- M. Carlos Martin, Directeur de la sécurité d'information

Decathlon

- M. Michel Yvon, Pôle trésorerie et financement groupe
- M. Xavier Fouré, e-commerce treasury manager
- M. Geoffrey Thery, IT engineer

SNCF Mobilités

- Mme Anne-Valérie Bouvier, Directeur paiements et flux financiers
- Mme Cécile de Saporta, Chef de projet paiements & flux financiers

Prestataires de services cloud

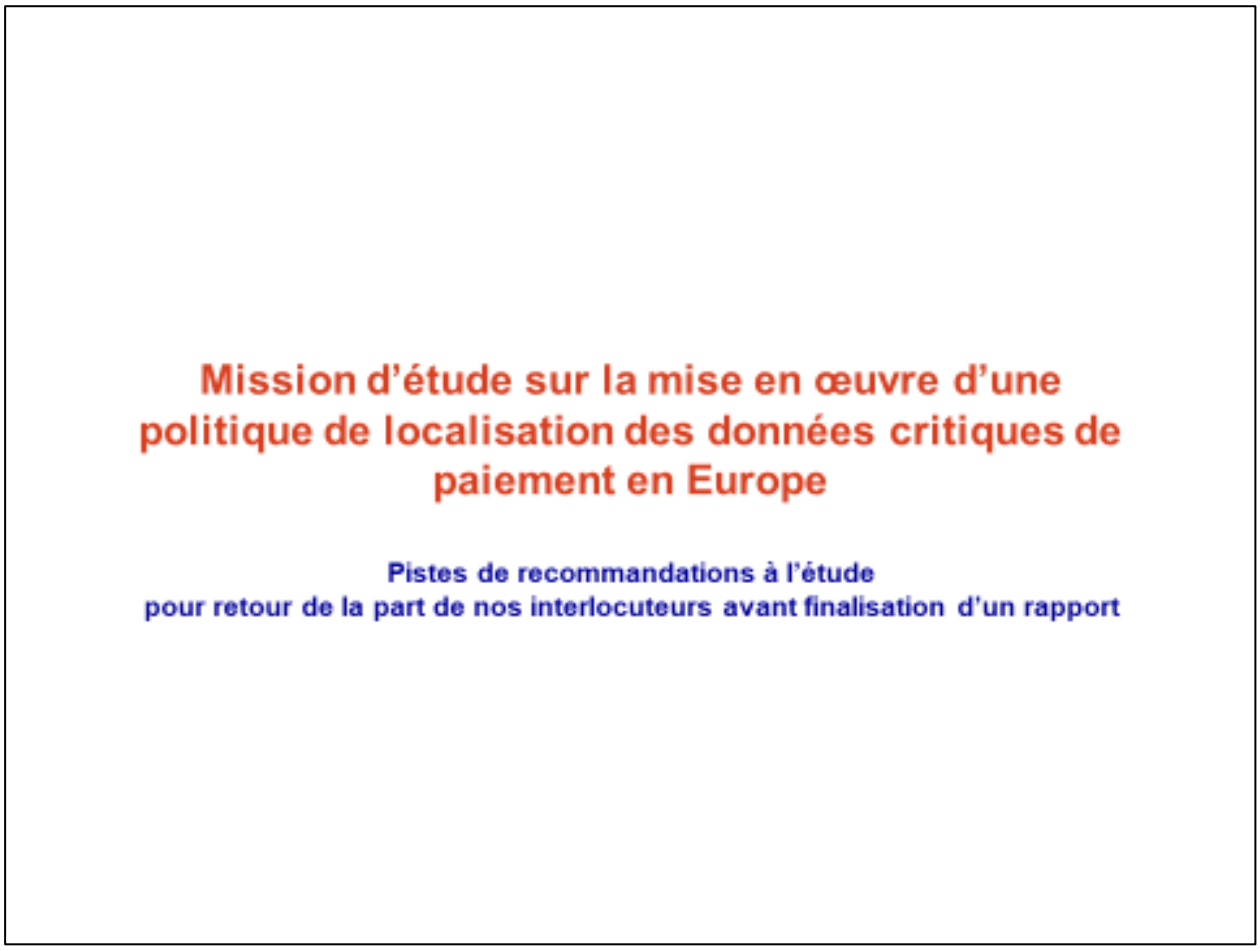
Microsoft

- M. Alfonso Castro, Directeur de la stratégie cloud
- M. Laurent Verdier, CTO - industry technology strategist

OVH

- M. Michel Paulin, Chief executif officer
- M. Grégoire Kopp, Special advisor

Annexe 4 : Pistes de recommandations soumises le 20 novembre 2019 aux interlocuteurs de la mission pour commentaires



Pistes de recommandations

1. Imposer la localisation en Europe des données de paiement ?
2. Imposer que le processing interbancaire des transactions par carte soit effectué en Europe
3. Favoriser l'émergence d'un système européen de paiement
4. Renforcer les normes européennes en matière de paiement
5. Assurer le respect des règles de protection des données personnelles
6. Protéger les données stockées dans le Cloud
7. Surveiller les conditions de mise en œuvre de la tokenisation
8. Soutenir et encadrer l'innovation avec une approche agnostique

3

Différents risques d'atteinte à la souveraineté européenne

- Risque politique : paralysie possible des services de paiement en cas de recours d'une forte proportion des acteurs du paiement à un même prestataire de service extra-européen et suspension des services de celui-ci pour raisons politiques
- Risque juridique : accorder des droits à la justice d'un pays tiers sur des données critiques de paiement appartenant à des ressortissants européens, en-dehors des règles d'entraide judiciaire
- Risque d'espionnage : ne pas assurer une protection adéquate des données critiques de paiement des clients européens vis-à-vis d'acteurs tiers
- Risque d'utilisation des données personnelles à des fins commerciales : moindre exigence de conformité à l'égard des règles du RGPD de la part de certains acteurs extra-européens et plus grande difficulté à assurer le contrôle et la sanction d'éventuels manquements
- Risque d'atteinte au level playing-field par de moindres contraintes réglementaires envers les acteurs extra-européens

2

1. Imposer la localisation en Europe des données de paiement ?

- **Des exemples étrangers (Inde, Indonésie, Turquie…) plus ou moins probants, des objections sérieuses mais pas d'inconvénient insurmontable**
- **Différentes modalités possibles :**
  - *Distinguer les transactions domestiques européennes (UE vs zone euro ou EEE?) et les transactions transfrontière européenne*
  - *Exiger seulement une copie en Europe des données de transactions ou interdire la copie hors d'Europe de données de transactions ?*
  - *Application à tous les acteurs du paiement ou seulement à ceux qui excèdent un certain seuil de part de marché ?*
  - *Quelles données « critiques » de paiement ?*
- **La localisation des données en Europe, une réponse à quel problème ?**
  - *Faciliter l'action de la justice (réquisition judiciaire…) ou de Tracfin*
  - *Faciliter le contrôle et la sanction de manquements aux règles de protection des données personnelles (RGPD)*
  - *Pas suffisant pour faire obstacle au Cloud Act, ni pour garantir la continuité des services de paiement*

4

2. Imposer que le processing interbancaire des transactions par carte soit effectué en Europe

L'article 7 du règlement interchange (2015/751) institue d'ores et déjà une séparation entre l'entité qui gère le scheme de cartes de paiement et les entités de processing interbancaire :

1. Les schémas de cartes de paiement et les entités de traitement :
   a) sont des entités indépendantes du point de vue de la comptabilité, de l'organisation et des processus décisionnels ;
   b) ne présentent pas les prix de manière groupée pour les activités liées au schéma de cartes de paiement et au traitement et n'octroient pas de subventions croisées à ces activités ;
   c) ne pratiquent aucune discrimination entre leurs filiales ou leurs actionnaires, d'une part, et les utilisateurs des schémas de cartes de paiement et d'autres partenaires contractuels, d'autre part, et notamment ne subordonnent aucunement la prestation de services à l'acceptation, par l'autre partenaire contractuel, d'un autre service qu'ils proposent, quel qu'il soit.

Recommandation : imposer que le processing interbancaire des transactions par carte entre un consommateur européen et un commerçant européen soit effectué en Union européenne, en demandant aux acteurs du processing interbancaire la localisation de leurs datacenters (stockage, lieu de traitement, back-up) en Europe ou le recours à un prestataire européen.

5

3. Favoriser l'émergence d'un système européen de paiement

- **Principales interrogations :**
  - *Veiller à associer toutes les parties prenantes (banques, commerçants, consommateurs…)*
  - *S'appuyer sur le virement instantané (SCT^{inst}) plutôt que sur les process cartes ?*
  - *Attention à ne pas diminuer la contribution à la souveraineté européenne qui tient à l'existence et à l'importance actuelles des schemes nationaux*
  - *Quel modèle économique ?*

6

4. Renforcer les normes européennes en matière de paiement

Une multitude d'instances de représentation des parties prenantes, des initiatives de normalisation prometteuses (Nexo), mais des progrès très modestes en termes d'interopérabilité européenne

EBA EUROPEAN BANKING AUTHORITY

Euro Retail Payments Board

Recommandations :

- **Besoin d'une politique européenne de convergence vers des standards communs**
  - *Faisant obstacle à la fragmentation du marché européen*
  - *Définissant à brève échéance etavec une gouvernance adaptée des objectifs ambitieux*
  - *Neutre technologiquement (carte, QR-code, paiement instantané…)*

Payment Service Providers / Processors / Retailers / Schemes / Vendors → ECSG

ECPC

nexo STANDARDS

European Payments Council

- **Envisager la création d'une agence européenne de lutte contre la fraude**
  - *Avec préalablement, observation européenne de la fraude selon des standards communs*

PAYMENTS EUROPE

ECPA

7

5. Assurer le respect des règles de protection des données personnelles

- Pour le RGPD, une « *donnée à caractère personnel* » est une information se rapportant à une personne physique « *qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne…* »
- Certains acteurs de la chaîne des paiements estiment qu'ils peuvent exploiter des données issues de transactions de paiement et commercialiser des données agrégées, sans le consentement des consommateurs

Recommandation : faire appliquer à l'ensemble des acteurs de la chaîne des paiements les mêmes règles de protection des données. Le Comité Européen de la Protection des Données devrait prendre position :

- *sur l'interdiction de l'utilisation des données de paiement à des fins commerciales sans accord explicite des consommateurs (opt-in)*
- *sur une durée de conservation limitée des données de transaction par les intermédiaires de la chaîne du paiement*

8

6. Protéger les données stockées dans le Cloud

Recommandations :

Lorsque des établissements financiers européens externalisent le stockage ou le traitement de données critiques de paiement sur le Cloud :

- **les inciter à recourir de préférence aux services de prestataires européens de services Cloud pour assurer une meilleure protection juridique extra-territoriale**
- **exiger que les données de paiement soient détenues et traitées dans des datacenters localisés en Europe (c'est une proposition offerte aujourd'hui par plusieurs acteurs majeurs du Cloud),**
- **exiger que les données de paiement soient chiffrées dans des conditions telles que le prestataire de services Cloud ne puisse lui-même déchiffrer ces données.**

Le programme d'étude 2019-2020 de la CNIL prévoit qu'elle fera un état des lieux technique et précis sur les infrastructures et services cloud. Ces travaux devraient lui permettre d'actualiser ses recommandations et d'identifier de nouveaux leviers de régulation de ce secteur.

9

7. Surveiller les conditions de mise en œuvre de la tokenisation

- La tokenisation consiste à substituer à un numéro de carte bancaire un alias exclusivement utilisable dans un certain contexte (paiement par mobile, e-commerce chez un commerçant donné…). Cette technique apporte une double sécurité : le numéro de carte ne circule pas ailleurs que chez le prestataire de token et le token est invalide hors de ce contexte.
- Le règlement 2015/751 relatif aux commissions d'interchange proscrit dans le cas de cartes cobadgées (article 8) toute mesure discriminatoire de routage des transactions, ainsi que tout mécanisme automatique, logiciel ou dispositif limitant le choix de la marque de paiement et/ou de l'application de paiement

Recommandations :

- *Veiller à ce que la mise en œuvre de la tokenisation ne conduise pas à « décobadger » une carte de paiement, mais donne lieu à la création de plusieurs tokens*
- *Si nécessaire, préciser à cet égard le règlement 2015/751 lors de sa prochaine révision*
- **Existe-t-il un enjeu de souveraineté qui conduirait à imposer que le token service provider soit localisé sur le sol européen ?*

| 10

8. Soutenir et encadrer l'innovation avec une approche agnostique

Recommandations :

- Privilégier les normes ouvertes (ISO 20022, NEXO…) au détriment des protocoles propriétaires (CB2A…)
- Veiller à la neutralité technologique des règles applicables (par ex. QR Code / paiement sans contact)
- Assurer des conditions neutres de concurrence entre le paiement instantané et les schemes de paiement par carte, par exemple en instituant un plafond autorisé de commission d'interchange pour le paiement instantané identique à celui autorisé par le paiement par carte de crédit, pour permettre le développement de schemes européens
- Global stablecoins : assurer le respect des principes édictés par le Committee on Payments and Market Infrastructures d'octobre 2019 ("Investigating the impact of global stablecoins")
- Promouvoir un dispositif paneuropéen public d'identification des consommateurs, en évitant la privatisation de cette fonction, essentielle à la fluidité et à l'efficacité des systèmes de paiement

| 11