

PAIEMENT MOBILE SANS CONTACT

LIBÉRER LES SMARTPHONES
ET LEURS UTILISATEURS

PAR **HOUSSEM ASSADI** (*DEJAMOBILE*)
LIONEL BARABAN (*FAMOCO*)
NICOLAS BRULEY (*ANTELOP SOLUTIONS*)
JEAN-MICHEL CHANAVAS (*MERCATEL*)
VINCENT DUVAL (*PAYLIB*)
MICHEL GANZIN (*GROUPEMENT DES CARTES BANCAIRES*)
RAPHAËL RICHARD (*PLAYFRANCE.DIGITAL*)

PAIEMENT MOBILE SANS CONTACT : LIBÉRER LES SMARTPHONES ET LEURS UTILISATEURS

PRÉAMBULE	5
INTRODUCTION	7
La sensibilité des données bancaires	7
Les big tech, garantes de nos données bancaires ?	8
Du libre-choix pour le consommateur !	8
Le paiement mobile, une solution nécessaire en contexte de crise sanitaire	9
CONCLUSION	10
ANNEXES	11
Proposition de loi française relative au paiement mobile sans contact	11
Proposition de règlement européen relatif au paiement mobile sans contact (en anglais uniquement)	14

PRÉAMBULE

Aujourd'hui, les plateformes numériques dominantes régissent l'ensemble des activités humaines, qu'elles soient personnelles ou professionnelles, individuelles ou collectives. Notre travail consiste, d'une part, à alerter et sensibiliser les représentants publics et privés s'agissant des processus de transformation numérique en cours, et du caractère parfois prédateur des entreprises qui dominent cet écosystème, et d'autre part, imaginer des solutions, juridiques, techniques ou économiques pour libérer les consommateurs et les entreprises du joug des plateformes. C'est bien là tout le sens de l'action de la Fondation Digital New Deal.

Quand Apple refuse au gouvernement français l'accès au bluetooth en arrière-plan dans le cadre du développement de l'application StopCovid, c'est bien la capacité de l'Etat à répondre à la crise sanitaire qui est mise à mal. En effet, la souveraineté des Etats est remise en cause par des entreprises aux services immatériels – les big tech – contestant le contrôle régalién classique dans des domaines aussi essentiels que l'imposition, la sécurité ou encore la création monétaire. L'obsolescence du droit positif se fait alors évidente : le droit d'auteur, le droit de la propriété intellectuelle, le droit des médias, le droit fiscal – la liste est non-exhaustive – se révèlent subitement inadapés à la réalité des usages alors que doivent émerger de nouveaux concepts juridiques comme, à titre d'exemples, les neutralités du net et des terminaux. Et bien d'autres encore.

Nous avons récemment contribué à la réflexion sur la future directive *Digital Services Act*, qui met notamment en lumière la question de la responsabilité des plateformes, dans une note intitulée *Réflexions dans la perspective du Digital Services Act européen*¹. Également, nous mettons en avant, dans nos travaux et nos prises de paroles, le rapport de force à sens unique entre les big tech et les consommateurs / entreprises utilisatrices, tous deux prisonniers d'écosystèmes fermés, matérialisés par des systèmes d'exploitation propriétaires. Les big tech, jouant de puissants effets de réseaux, disposent d'un avantage concurrentiel indéniable, leur permettant d'une part, de consolider leurs positions monopolistiques, et d'autre part, de rendre difficile – voire impossible – l'émergence de solutions concurrentes alternatives.

Le marché du paiement mobile instantané en constitue une probante illustration, avec la présence de *gatekeepers*², qui en abusant de leur position dominante, achèvent d'annihiler toute forme de concurrence. A titre d'exemple, Samsung réserve l'accès pratique et rapide à sa propre application paiement via un *swipe*³. Autre exemple : l'opérateur Apple n'autorisant pas les tiers à accéder à l'antenne NFC qui équipe ses téléphones (iPhones) et autres objets connectés portables (iWatches), les consommateurs ayant acquis ces produits ne peuvent effectuer des paiements sans contact en magasin via des applications ou solutions concurrentes d'Apple Pay. Apple se réserve ainsi le marché des solutions de paiement sans contact en magasin, restreignant la liberté de choix des consommateurs et la concurrence entre solutions de paiement, et freinant le développement du paiement par téléphone sans contact, alors que la pandémie en cours confirme la nécessité de faciliter ce mode de paiement.

Des initiatives législatives émergent sur ce thème en Europe. L'Allemagne a notamment adoptée début d'année une législation demandant aux big tech de permettre à des applications paiement européennes de pouvoir accéder à l'antenne NFC. En France, une proposition de loi visant à garantir le libre choix du consommateur dans le cyberspace, adoptée à l'unanimité par le Sénat, ambitionne également d'assurer le libre choix du consommateur sur les terminaux. Ces initiatives visent à faire d'internet un écosystème plus ouvert, favorable à l'innovation, où le consommateur récupère son pouvoir d'agir, autrement dit sa capacité à faire des choix comme il peut le faire dans d'autres marchés régulés.

¹ Rapport disponible [ici](#) en français et [ici](#) en anglais – mars 2020

³ « swipe » désigne le glissement latéral du doigt sur un écran tactile

² « gardien » en français

Paiement mobile sans contact

Adopter en droit interne une disposition législative sur le paiement mobile, ayant comme objectifs l'ouverture à la concurrence de l'accès à l'antenne NFC, l'équité ergonomique et la régulation des coûts d'accès, constitue selon nous un moyen juridique de corroborer la nécessité plus globale de réguler spécifiquement, au niveau national et européen, les big tech.

Cette note est une invitation à envisager différemment le marché du paiement mobile instantané ; certains opérateurs qui y évoluent ne semblent pas respecter les règles du jeu de la concurrence. Après la présentation d'un certain nombre de constats prouvant cette dérive, nous proposons un texte législatif pour le droit interne, et si tant est que la volonté d'agir s'étend à l'échelle du continent, une ébauche de réglementation européenne.

—
Arno Pons, délégué général de la Fondation Digital New Deal

INTRODUCTION

La place de l'argent liquide a-t-elle vocation à se réduire ? Serons-nous tous amenés à payer la plupart de nos achats dans les magasins avec notre smartphone ? Facebook réussira-t-il à diffuser sa propre cryptomonnaie Libra ? Ce futur, encore dystopique il y a quelques années, deviendra-t-il réalité ? Les big tech se substitueront-elles aux banques ? S'établiront-elles en véritable « *gatekeepers* » des mondes marchands de nos économies européennes ? Alors que des glissements structurants sont opérés par les big tech, dont nous percevons l'intérêt majeur pour les secteurs bancaires et marchands, des questions émergent. Plus que des questions, des doutes.

Si l'on s'intéresse aux récentes innovations du secteur bancaire, force est de constater que derrière des innovations en apparence invisibles ou accessoires – le NFC est un bon exemple tant il reproduit un geste auquel nous sommes désormais habitués, le paiement sans contact – se jouent des enjeux majeurs de souveraineté et de sécurité.

Apple, Google et Samsung ont respectivement lancé Apple Pay, Google Pay et Samsung Pay. Alors que l'usage d'Apple Pay s'est diffusé, la firme à la pomme a également travaillé de concert avec Goldman Sachs sur la création d'une carte bancaire, dont les limites⁴ ont déjà été mises en lumière. Google et Samsung adoptent la même stratégie en annonçant également faire de même⁵. L'intention de ces opérateurs numériques mondiaux de s'immiscer dans le secteur bancaire – voire monétaire – constitue un sujet politique majeur, un sujet de souveraineté prégnant.

En ce sens, pourquoi l'ambition des big tech de s'établir dans le secteur bancaire, et en particulier dans le marché du paiement mobile instantané, constitue-t-elle une menace pour notre souveraineté ?

La sensibilité des données bancaires

La collecte, le traitement et l'exploitation des données personnelles et non-personnelles constitue le cœur du modèle économique des big tech. Ces opérateurs disposent d'une qualité et d'une quantité de données immenses ; elles peuvent être relatives à un individu, provenir des réseaux sociaux, de nos habitudes d'achat ou encore des requêtes de recherche.

Ces opérateurs enrichissent considérablement leur connaissance client avec la pertinence des informations contenues dans les données de transaction bancaire. Au cœur de l'intérêt de ces opérateurs trans-sectoriels pour ces nouvelles données se trouve notamment la capacité, grâce à celles-ci, de tisser des réseaux d'interactions, qui permettent par exemple d'améliorer encore un peu plus l'efficacité de leur service de publicité ciblée, voire d'augmenter le prix des espaces disponibles. En effet, les données bancaires ne sont pas uniquement utiles pour en apprendre plus sur un individu ; leur valeur est concrétisante et structurante puisqu'elles rendent possible de lier des individus entre eux ou avec des entreprises.

Investir dans le marché de la banque et du paiement se révèle attractif pour les big tech : l'exploitation commerciale de ces nouvelles données stratégiques va constituer une nouvelle source de revenus, permettre de rendre leurs utilisateurs encore plus captifs et menacer la capacité des commerçants à se développer comme à préserver la valeur de leurs fonds de commerce.

⁴ <https://www.theverge.com/2019/11/12/20960409/apple-card-discriminatory-credit-limits-goldman-sachs-brand>

⁵ <https://www.theverge.com/2020/5/7/21251293/samsung-pay-debit-card-sofi-this-summer>

Les big tech, garantes de nos données bancaires ?

La sensibilité européenne concernant la protection des données est très forte, en témoigne l'adoption en mai 2018 du Règlement général sur la protection des données (RGPD). Son objectif, qui s'applique à toutes les organisations traitant des données personnelles, est double : protéger les citoyens concernant le traitement de leurs données à caractère personnel et responsabiliser les acteurs de ce traitement.

A l'inverse d'autres secteurs, l'utilisation d'informations personnelles est obligatoire dans le secteur bancaire : situation financière, patrimoine, revenus, profession, etc... sans oublier les informations sur l'état de santé s'agissant des assurances de prêt. En quelques années, le web et les équipements mobiles sont devenus les principales interfaces de connexion avec les banques, générant des données bancaires dites sensibles. A cet égard, les obligations du RGPD auxquelles les entreprises et les banques ont dû se conformer – collecte, stockage et analyse – et les droits auxquels les citoyens ont désormais accès – droit à l'accès, à la portabilité, à l'oubli et droit de rectification – ont permis de renforcer la relation de confiance entre les internautes et les établissements bancaires.

Depuis peu, la régulation du numérique, et tout particulièrement celle de ces acteurs dominants, les big tech, agitent les sphères publiques et privées. De l'enthousiasme des débuts – ces entreprises étaient l'incarnation du progrès et de l'innovation – aux dérives répétées d'un modèle prédateur – les exemples ne manquent pas – la nécessité de réguler s'impose peu à peu. A l'inverse, force est de constater que le marché bancaire est particulièrement régulé, notamment s'agissant de l'accès aux données. En effet, des contraintes juridiques fortes, et notamment les secrets statistique et professionnel, encadrent et protègent l'accès aux données⁶.

Les banques et les acteurs du paiement instantané s'imposent ainsi, face aux big tech, comme un véritable tiers de confiance s'agissant de l'utilisation de nos données bancaires. En outre, la question du traitement et de la conservation des données de paiement par les big tech mérite d'être abordée, notamment sur la question de la localisation des serveurs qui revêt une importance significative puisqu'elle détermine le droit applicable. En ce qui concerne les big tech, l'externalisation de la conservation des données vers des acteurs étrangers du cloud soulève des enjeux de sécurisation, de protection des données et de souveraineté.

Du libre-choix pour le consommateur !

Un rapport⁷ de M. Franck Montaugé et Mme Sylviane Noël, réalisé au nom de la commission des affaires économiques du Sénat sur la proposition de loi visant à garantir le libre choix du consommateur dans le cyberspace précise que « *Le système d'exploitation iOS offre aux applications tierces un accès très limité à la puce NFC des terminaux Apple, dans la mesure où Apple n'ouvre pas l'interface de programmation applicative (ou API) donnant accès à cette fonctionnalité. Or, cet accès étant nécessaire pour utiliser un terminal mobile pour effectuer un paiement sans contact, les applications concurrentes d'Apple Pay se retrouvent dans l'incapacité de proposer leurs services de paiement sans contact aux usagers des terminaux Apple de manière indépendante. Pour accéder à cette fonctionnalité à travers l'application Apple Pay, les services tiers doivent payer une commission à Apple. Cette absence d'accès aux puces NFC met aussi en jeu la fourniture de titres de transports dématérialisés. C'est le cas par exemple du pass Navigo dématérialisé, qui de ce fait, ne peut se déployer sur la plupart des terminaux des usagers des transports en commun franciliens.* ».

⁶ Page 41 - 42 : https://www.cnis.fr/wp-content/uploads/2017/10/RAP_2015_140_acces-aux-donnees-bancaires.pdf

⁷ <http://www.senat.fr/rap/l19-301/l19-3011.pdf>

Ce point soulève deux problèmes majeurs :

- Un sujet de protection de la liberté de choix du consommateur, dans la mesure où ce dernier ne dispose pas de moyens alternatifs de paiement mobile s'il utilise un terminal équipé d'un système d'exploitation iOS ou s'il est préférentiellement renvoyé vers les solutions Samsung Pay ou Google Pay sur Android.

- Et une question de protection de la libre-concurrence ; à cet égard, Margrethe Vestager, Vice-présidente exécutive de la Commission européenne et Commissaire à la concurrence, a abordé le dossier Apple Pay lors d'une conférence de presse en marge du Web Summit 2019 à Lisbonne en précisant : *"People see it becomes increasingly difficult to compete in the market for easy payments"*⁸.

A titre de rappel, les règles de concurrence permettent de créer les conditions d'une concurrence loyale sur un marché. Elles favorisent notamment, toujours dans l'intérêt du consommateur, la baisse significative des prix et l'amélioration de la qualité des biens et des services. A l'égard de la problématique du marché du paiement mobile instantané, il faut lutter contre les pratiques unilatérales abusives d'opérateurs qui, à l'instar d'Apple, mais aussi de Samsung, réservent l'usage d'équipements (antenne NFC d'Apple) ou de fonctionnalités facilitant l'accès pratique et rapide à une application (swipe de Samsung) au profit de leurs propres solutions de paiement.

Ces pratiques abusives réduisent et faussent la concurrence au profit de leaders déjà mondiaux, les big tech, au risque de faire perdre à l'industrie européenne des moyens de paiement la capacité à concurrencer ces leaders, et générer une perte de souveraineté des Etats en matière de paiements. Il convient de rappeler que la concurrence est considérée, au même titre que la liberté de circulation des marchandises, comme un élément moteur et fondamental de la construction du marché intérieur européen. A ces égards, il semble primordial que les différents opérateurs de solutions de paiement puissent être accessibles, sans distinction, via tous les systèmes d'exploitation existants.

Le paiement mobile, une solution nécessaire en contexte de crise sanitaire

La crise du Covid-19 a permis d'accélérer le projet de relever le plafond de paiement par carte sans contact ; désormais, nous pouvons utiliser la technologie sans contact de notre carte bancaire pour des transactions allant jusqu'à 50 euros. Le paiement sans-contact est désormais perçu comme un « geste barrière » pour les consommateurs et les autorités ; c'est un moyen d'envoyer un signal fort aux consommateurs – il semblerait par ailleurs que ce relèvement de plafond ait un impact positif et dynamique sur la consommation. Michel Ganzin, président du conseil de direction du Groupement des Cartes Bancaires, abonde en ce sens en précisant que *« l'absence de contact au moment du paiement apporte effectivement une protection supplémentaire »*⁹. A cela s'ajoute les apports confirmés de plusieurs études sur le paiement sans contact qui, *« par les facilités qu'il procure, dynamise l'activité et augmente le chiffre d'affaires des commerçants »*.

Ce raisonnement, qui prend en compte des considérations sanitaires, semble également être applicable au marché du paiement mobile. Dans un contexte de crise sanitaire, et particulièrement dans une situation épidémique, n'aurions-nous pas intérêt à largement diffuser les usages du paiement mobile ? En l'état, avec les barrières érigées par les opérateurs internationaux, qu'ils s'agissent d'Apple qui se réserve son antenne NFC pour son propre usage ou Samsung qui favorise sa solution de paiement mobile au détriment des autres, cela n'est pas envisageable.

⁸ <https://www.reuters.com/article/us-eu-antitrust-apple/eus-vesta-ger-says-apple-pay-has-prompted-many-concerns-idUSKBNIXHIYL>

Légiférer pour ouvrir l'accès au paiement mobile à la concurrence et ainsi permettre le libre-choix du consommateur conduira non seulement à encourager de nouveaux usages, mais revêt surtout un caractère nécessaire tant il s'inscrit dans le cadre des mesures sanitaires que le gouvernement essaye de faire appliquer partout sur notre territoire, et dont la nécessité n'est plus à démontrer.

CONCLUSION

Si le RGPD a permis d'affirmer une certaine vision du numérique, propre aux valeurs fondamentales européennes, il apparaît que ce règlement a été mis en place en réaction à l'hégémonie des big tech sur les données. S'agissant des problématiques de pratiques abusives de certains opérateurs sur le marché du paiement mobile, que cette note se propose d'étudier, il convient d'intervenir rapidement, c'est-à-dire avant que les géants du numérique n'aient consolidé des positions fortes ou attaqué des parts de marché trop importants.

Par ailleurs, comme le précise le Conseil de Stabilité Financière (FSB), « *ce n'est pas le rôle des autorités de protéger les établissements financiers de la concurrence, mais régulateurs et superviseurs devraient se montrer particulièrement vigilants à l'impact d'une telle concurrence sur la viabilité des modèles économiques existants et la nature de la réponse à apporter* »¹⁰.

Enfin, l'intervention rapide de la France, et certainement de l'Europe à terme, apparaissent d'autant plus nécessaire que, dans un contexte de crise économique inédite, toute éventuelle inertie risquerait de créer au profit des big tech un avantage pratiquement irréversible, au détriment des consommateurs et prestataires de paiement européens, et d'entraver l'essor du paiement sans contact dont les avantages sanitaires sont pourtant manifestes, tout particulièrement suite au contexte du Covid-19.

En outre, si nous sommes des spécialistes du paiement mobile sans contact, par les différentes fonctions que nous occupons, un sujet plus large, plus prégnant encore, nous interpelle en tant que citoyens. Le refus par Apple de donner accès au bluetooth en arrière-plan au gouvernement français, dans le cadre du développement et du déploiement de l'application StopCovid, nous semble symptomatique d'un glissement global malheureux. Des circonstances exceptionnelles n'ont pas empêché des entreprises privées de s'arroger une prérogative essentielle de la puissance publique, une fonction non-régaliennne mais tout aussi importante, la santé.

Liste des signataires :

- Houssein Assadi (*Dejamobile*)
- Lionel Baraban (*Famoco*)
- Nicolas Bruley (*Antelop Solutions*)
- Jean-Michel Chanavas (*Mercatel*)
- Vincent Duval (*Paylib*)
- Michel Ganzin (*Groupement des Cartes Bancaires*)
- Raphaël Richard (*PlayFrance.Digital*)

⁹ <https://www.franceinter.fr/economie/vers-moins-de-contact-y-compris-dans-vos-achats>

¹⁰ <https://www.lesechos.fr/finance-marches/banque-assurances/les-regulateurs-financiers-vigilants-face-a-loffensive-des-gafa-dans-la-banque-1154851>

MESURES VISANT À FACILITER LE PAIEMENT MOBILE SANS CONTACT EN PRÉSERVANT LA LIBERTÉ DE CHOIX DU CONSOMMATEUR ET LA LOYAUTÉ DE LA CONCURRENCE

Article 1

Est qualifiée de fournisseur de système d'exploitation toute personne qui, à titre professionnel, édite ou adapte le système d'exploitation d'un terminal mobile, ou qui est responsable de la première mise à disposition sur le marché de l'Espace Economique Européen d'un terminal mobile, dès lors que ce terminal permet aux consommateurs situés sur le territoire français d'effectuer un paiement mobile sans contact.

Article 2

Est considéré comme un service utile au paiement mobile sans contact tout service, système d'exploitation, logiciel, émulation, matériel, composant, antenne, élément sécurisé, ou autre élément contrôlant ou facilitant l'accès à une fonctionnalité, outil ou raccourci ergonomique d'un terminal mobile, dès lors qu'il permet, améliore ou facilite le paiement sans contact.

Article 3

I. Tout fournisseur de système d'exploitation s'assure que les produits et services qu'il offre permettent à tout consommateur situé sur le territoire français d'exercer librement et sans entrave sa liberté de choix entre tout prestataire de services permettant ou facilitant le paiement mobile sans contact.

II. Tout fournisseur de système d'exploitation garantit des conditions de concurrence équitables entre sa propre activité de services de paiement et les activités concurrentes exercées directement ou indirectement par les établissements de crédit, établissements de monnaie électronique, prestataires de services de paiement, établissements de paiement et agents au sens de la Directive (UE) 2015/2366. Le respect de cette obligation est apprécié au niveau de l'ensemble du groupe du fournisseur de système d'exploitation, en tenant compte de toutes les sociétés directement ou indirectement contrôlantes ou contrôlées au sens de l'article L. 430-1-III du code de commerce.

III. Le respect des obligations prévues à l'article 3 I° et II° du présent texte implique notamment que le fournisseur de système d'exploitation assure un égal accès ergonomique au consommateur, afin qu'il puisse exercer sa liberté de choix des applications liées au paiement, et s'assure que :

(i) tout outil ou raccourci ergonomique que le fournisseur de système d'exploitation propose ou met en place sur le terminal mobile pour faciliter l'utilisation d'une application concernant le paiement sans contact soit librement et gratuitement ouvert au consommateur, quelle que soit l'application de paiement qu'il aura choisie ;

(ii) tout consommateur soit libre d'installer sur son terminal mobile toute application tierce de son choix liée à un service de paiement ou une opération de paiement et de définir cette application comme l'application par défaut ou favorite.

Proposition de loi française

Article 4

Le fournisseur de système d'exploitation est tenu de mettre à disposition de tout prestataire de services de paiement, établissement de crédit, établissement de monnaie électronique, établissement de paiement ou agent au sens de la Directive (UE) 2015/2366 qui lui en fait la demande, tous les services utiles au paiement mobile sans contact dans des conditions équitables, raisonnables et non discriminatoires.

Article 5

L'accès visé à l'article 4 du présent texte est accordé, au choix du fournisseur de système d'exploitation, soit gratuitement, soit moyennant une redevance, dans le respect des conditions cumulatives suivantes :

1° la redevance n'excède pas les coûts marginaux, c'est-à-dire les coûts effectivement encourus liés au travail supplémentaire spécifiquement demandé par le tiers demandeur d'accès ;

2° il n'existe pas d'autre solution pratique et économiquement viable qui permettrait de traiter la demande d'accès de manière équivalente ou plus efficace à un coût égal ou inférieur ;

3° les coûts sont déterminés et ventilés avec précision, afin de permettre une vérification aisée.

Article 6

I. Par dérogation à l'obligation d'accès énoncée à l'article 4 du présent texte :

1° un fournisseur de système d'exploitation n'est pas soumis à l'obligation d'accès s'il établit que ce système compte moins de 2 millions d'utilisateurs enregistrés dans le marché intérieur de l'Espace Economique Européen au cours du dernier exercice financier. Ce seuil doit être évalué à la date de la demande d'accès.

2° le fournisseur de système d'exploitation peut refuser d'accorder l'accès prévu à l'article 4 s'il démontre que cet accès menace de façon concrète, documentée et substantielle la sécurité des paiements au préjudice des consommateurs.

II. Le fournisseur de système d'exploitation ne peut se prévaloir d'une menace sécuritaire et bénéficier de la dérogation prévue à l'article 6 I 2° du présent texte que s'il démontre avoir fait ses meilleurs efforts pour l'éviter et pour offrir aux tiers demandeurs d'accès des options alternatives sécurisées, pratiques et économiquement viables, afin de préserver une concurrence libre et loyale entre les prestataires de services de paiement et la liberté de choix des consommateurs.

III. Le fournisseur de système d'exploitation ne peut en tout état de cause refuser une demande d'accès conforme à l'article 4 si le requérant ou l'établissement de paiement, de crédit ou de monnaie électronique dont il est l'agent consent à le garantir par écrit par avance contre toute éventuelle réclamation d'un consommateur, en ce qu'elle serait due à cet accès. Une telle garantie ne pourra pas porter préjudice au consommateur et n'exonèrera pas le fournisseur du système d'exploitation de son obligation de respecter les dispositions des articles 3 et 6 II° du présent texte.

Article 7

Tout manquement aux obligations prévues par le présent texte peut donner lieu à une action devant la juridiction compétente, y compris devant le juge des référés, et aux sanctions dans les conditions définies à l'article L. 442-4 du Code de commerce, à l'initiative du ministère public, du ministre en charge de la consommation, du président de l'Autorité de régulation des communications électroniques et des Postes, du président de l'Autorité de contrôle prudentiel et de résolution ou du président de l'Autorité de la concurrence ou de toute autre personne justifiant d'un intérêt à agir.

**OBLIGATIONS APPLICABLE TO PROVIDERS OF TECHNOLOGY
INFRASTRUCTURES SERVICES ENSURING A LEVEL PLAYING FIELD
AND CONSUMERS' FREEDOM OF CHOICE AS REGARDS
PAYMENT SERVICES**

Whereas:

1. Directive (EU) 2015/2366 of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) n°1093/2010, and repealing Directive 2007/64/EC Directive (EU) 2015/2366 (Payment Service Directive 2 – PSD 2) provides the legal foundation for a better integrated internal market for safe electronic payments within the EU. Given that the retail payments market has experienced significant technical innovation and the emergence of electronic and mobile payment, the PSD 2 established a new framework for payment services, with the goal of making international payments within the EU as easy, efficient and secure as payments within a single country. It also seeks to open up payment markets to new entrants to ensure that consumers, merchants and companies enjoy choice and transparency of payment services to benefit fully from the internal market.
2. Payment services are essential for the proper functioning of vital economic and social activities.
3. In recent years, payments with mobile phones, digital tablet or other personal digital devices became increasingly popular in Europe and an increasing number of European citizens make use of a mobile device on a day-to-day basis for their financial services, including payments.
4. Since the adoption of the PSD2, and as recently underlined by the German Parliament and the French Senate, the consumer's liberty of choice in the field of payment transactions appear however to be more and more dependent upon access to technology, hardware, component, know-how or software enabling, facilitating or preventing the use of a third-party application in relation to a payment transaction or a payment service. This may include, for example access to a hardware or secure element, a Near Field Communication antenna, a manual for developing the software under the OS or applications, or a card emulation which displays the card information on the mobile device that is required in order to enable a payment transaction or the use of a payment application or service.
5. New rules should be established to close the regulatory gaps within the Union regarding access to such technology, tool or component while at the same time providing more legal clarity and ensuring consistent application of the legislative framework across the Union. This should generate efficiencies in the payment system as a whole and lead to fair competition, more choice and better prices for consumers and strengthening their trust in a harmonised payments market.
6. New rules shall also prevent distortions of competition to the detriment of consumers. Thus, each provider of technology services that may contribute to the provision of payment services or to e-money activities, including tool facilitating the use of any application relating to payment service, payment transaction or e-money (e.g. ergonomic or fast access tools) shall ensure a level playing field between its own payment services business (at group level), and other payment service providers, payment institutions, credit institutions, payment systems, agents and e-money issuers.

7. These new rules shall be defined and applicable without prejudice to EU competition law rules and to EU regulations or national laws protecting consumers.

8. Member States should lay down rules on the penalties applicable to infringements of this Regulation and should ensure that those penalties are effective, proportionate and dissuasive and that interim measures and compensation are applicable in due time.

Article 1

Definitions

The following definitions shall apply:

(1) 'agent' means a natural or legal person who acts on behalf of any payment institution and/or credit institution.

(2) 'credit institution' means an undertaking the business of which is to take deposits or other repayable funds from the public and to grant credits for its own account, as defined in point (1) of Article 4(1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council, including branches thereof, within the meaning of Article 1(1)(a) of the PSD2 Directive.

(3) 'e-money' means electronic money as defined in point (2) of Article 2 of Directive 2009/110/EC.

(4) 'group' means the undertaking concerned and all other undertakings belonging to the same group, i.e. all other undertakings mentioned in Article 5.4 (b), (c), (d) and (e) of the Regulation (EC) N° 139/2004 of 20 January 2004 on the control of concentrations between undertakings.

(5) 'personal digital device' means mobile phone, laptop, digital tablet personal computer or other mobile personal device enabling a consumer to make a payment transaction.

(6) 'payer' means a natural or legal person who holds a payment account and allows a payment order from that payment account or, where there is no payer's payment account, a natural or legal person who makes a payment order to a payee's payment account.

(7) 'payment institution' means a legal person that has been granted authorisation in accordance with Article 11 of PSD2 Directive¹² to provide and execute payment services throughout the European Union.

(8) 'payment service' means any business activity set out in Annex I of PSD2 Directive.

(9) 'payment system' means a funds transfer system with formal and standardised arrangements and common rules for the processing, clearing and/or settlement of payment transactions.

(10) 'payment transaction' means any payment transaction act, as defined in Article 4 (5) of PSD2 Directive.

(11) 'PSD2 Directive' shall mean Directive (EU) 2015/2366 of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

(12) 'technology infrastructures services' means the operating system (OS) and any other

Proposition de réglementation européenne

technology on mobile personal digital devices (including any component, tool, function, information, know-how or software) enabling, facilitating or preventing the use of a third-party application in relation to a payment transaction or a payment service, such as, for example a hardware component or secure element, a NFC antenna, a manual for developing the software under the OS or applications, or a card emulation which displays the card information on the personal digital device.

Article 2

Right of access to all technology infrastructure services

2.1. Any provider of technology infrastructures services that may contribute to or hinder the provision of payment services or to e-money activities in the internal market shall be obliged, upon written request from a payment service provider, a payment institution, a credit institution, a payment system, an agent or an e-money issuer, to make all technology infrastructure services available without undue delay under fair, reasonable and non-discriminatory conditions, in a way that the requesting undertaking can provide or operate its payment services or e-money transactions without hindrance.

2.2. The access set forth in Article 2.1 above shall be granted either for a fee complying with the following cumulative conditions:

- (a) the fee does not exceed the incremental costs, i.e. the efficiently incurred costs related to the additional work requested by the seeking access third party;
- (b) there is no practical and economically viable alternative to the arrangement which would lead to an equally or more efficient handling of the request for access at equal or lower cost;
- (c) the costs shall be precisely determined. The breakdown of the amount of the costs, including separate identification of each of its components, shall be part of the arrangement to allow for easy verification and monitoring.

2.3 As exceptions to the access requirement set forth in Article 2 above:

- (i) a provider of technology infrastructures services is not subject to the obligation if it has less than 2 million registered users in the European Union during the last fiscal year. This threshold is to be assessed at group level and on the day of the request for access.
- (ii) the provider of technology infrastructures services may refuse to grant access only if there are objective reasons to deny that access, such as for example a concrete, documented and substantial threat to the safety and integrity of its technology infrastructure services. The provider of technology infrastructures services bears the burden of proof of:
 - (a) the existence of such concrete threat;
 - (b) that it has complied with the guidelines enacted by the European Banking Authority, if any;
 - (c) that it has made its best efforts to minimize such threat and to offer access notwithstanding such threat; and

¹¹ <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015L2366&from=FR>

(d) that it has also made its best and prompt efforts to offer third-party access seekers practical and economically viable alternative options preserving competition among payment services providers and consumers' freedom of choice.

2.4 Subject to Article 2.3, no refusal to grant access may be opposed by the provider of technology infrastructures services should the credit institution or the payment institution acting for the payer accept to hold such provider of technology infrastructures services, subject to its full compliance with this regulation, harmless from any third party claim relating to a fully disclosed threat to the safety and integrity of the technology infrastructure services resulting from the access granted in accordance with Article 2.1 above.

Article 3

Level Playing Field

3.1 Any provider of technology infrastructures services that may contribute to the provision of payment services or to e-money activities shall ensure a level playing field between its own payment services business (at group level), and other payment service providers, payment institutions, credit institutions, payment systems, agents and e-money issuers. This shall notably imply that the provider of technology infrastructures services opens its operating system in order to grant the access set forth in Article 2 above, but also that it ensures a consistent customer experience for third-party services compared to its own services.

3.2 Any tool, feature or component facilitating the use of any application on a personal digital device relating to payment service, payment transaction or e-money (e.g. ergonomic or fast access tools)¹² shall be open to third-party applications on a free and open-source software licence basis.

3.3 Payers shall be free to install any third-party application relating to payment service, payment transaction or e-money of their choice on mobile phones, laptops, digital tablet personal computer or wearables and to set such application as the default or favourite application.

Article 4

Payment data

Any provider of technology infrastructures services shall enable payment service providers, payment institutions, credit institutions, payment systems, agents and e-money issuers to guarantee consumers and end-users that their payment data are not collected, processed, shared or used for any commercial purpose. The general terms and conditions of use of the technology infrastructures may not lead consumers or end-users to waive such guarantee.

Article 5

Liability

Without prejudice to the provisions of EU regulations or national laws protecting consumers, the provider of technology infrastructures services shall not reduce or exclude any liability in relation to a payment transaction unless it proves full compliance with all Articles of this regulation.

Article 6
Compensation and penalties

6.1 Any provider of technology infrastructures services that does not comply with the obligations mentioned in articles 2, 3, 4 and/or 5 above is bound to compensate competitors and consumers for the harm in full, and the injured party has the right to require full compensation. Such compensation shall be promptly granted, without prejudice to and in addition with fines or remedies that may be applicable under competition law rules and/or Article 6(2) above.

6.2 Member States shall, by [...], lay down rules on interim measures and on the penalties applicable to providers of technology infrastructures services that do not comply with of this [Regulation] and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive. Member States shall notify the Commission of those rules and measures by [...] and shall notify it without delay of any subsequent amendment affecting them.

¹² e.g. Samsung Pay vertical swipe or Apple Pay double-click.

DIGITAL NEW DEAL

LE THINK – TANK DE LA NOUVELLE DONNE

Le think tank Digital New Deal a pour vocation d'éclairer de la manière la plus complète possible les évolutions à l'œuvre au sein du phénomène de «digitalisation», dans l'acception la plus large du mot, et d'élaborer des pistes d'actions concrètes à destination des entreprises et des décideurs publics français et européens. Portés par l'expertise de leurs rédacteurs et leur insertion dans le débat public, les travaux du think tank pourront participer à l'élaboration d'une pensée française et européenne de la régulation digitale au service de la mise en place d'un cadre équilibré et durable.

Le Conseil d'administration

Les membres du Conseil d'administration de Digital New Deal sont tous membres fondateurs. Ils sont issus d'horizons divers tout en étant en prise directe avec la transformation digitale des entreprises et des organisations. Forts de leur intérêt commun pour les questions numériques, ils ont décidé d'approfondir leurs débats en formalisant un cadre de production et de publication au sein duquel la complémentarité de leurs expériences pourra être mise au service du débat public et politique. Ils s'impliquent personnellement dans la vie de Digital New Deal.

Un délégué général (Arno Pons) pilote avec le président fondateur (Olivier Sichel) les orientations stratégiques de la fondation, et supervise un chargé de mission (Louis Magnes), qui assure la coordination, au quotidien, de l'ensemble des activités du think tank.

CONTACT: contact@thedigitalnewdeal.org | **WEBSITE:** www.thedigitalnewdeal.org

Olivier Sichel

Président Digital New Deal
DGA Caisse des Dépôts



Judith Rochfeld

Professeure agrégée de Droit,
Panthéon Sorbonne



Sébastien Bazin

PDG AccorHotels



Denis Olivennes

Président groupe CMI France



Robert Zarader

PDG Equancy



Alain Minc

Président AM Conseil



Yves Poilane

DG Ionis Education Group



Nicolas Dufourcq

DG de Bpifrance



NOS PUBLICATIONS

Réflexions dans la perspective du Digital Services Act européen
Reflections in the perspective of the European Digital Services Act

Liza Bellulo - mars 2020

Préserver notre souveraineté éducative : soutenir l'EdTech française

Marie-Christine Levet - novembre 2019

Briser le monopole des Big Tech : réguler pour libérer la multitude
Big Tech Regulation: Empowering the Many by Regulating A Few

Sébastien Soriano - septembre 2019

Sortir du syndrome de Stockholm numérique

Jean-Romain Lhomme - octobre 2018

Le Service Public Citoyen

Paul Duan - juin 2018

L'âge du web décentralisé

Clément Jeanneau - avril 2018

Et si le CAC 40 ubérisait...sa R&D

Paul-François Fournier - novembre 2017

Fiscalité réelle pour un monde virtuel

Vincent Renoux - septembre 2017

Réguler le « numérique »

Joëlle Toledano - mai 2017

Appel aux candidats à l'élection présidentielle pour un #PacteNumérique

janvier 2017

La santé face au tsunami des NBIC et aux platformistes

Laurent Alexandre - juin 2016

Quelle politique en matière de données personnelles ?

Judith Rochfeld - septembre 2015

Etat des lieux du numérique eu Europe

Olivier Sichel - juillet 2015

