COLLECTION **LIVRE BLANC** **N°2**

QUAND LA CONFIANCE PAIE

Les moyens de paiement d'aujourd'hui et de demain au défi de la protection des données

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

COLLECTION **LIVRE BLANC - N°2**

QUAND LA CONFIANCE PAIE : Les moyens de paiement d'aujourd'hui et de demain au défi de la protection des données

SOMMAIRE

Septembre 2021

Directeur de la publication : Gwendal Le Grand

Rédacteur en chef : Thomas Dautieu

Rédacteurs de ce livre blanc : Aymeric Pontvianne (chef de projet), Antoine Courmont, Erevan Malroux, Gaston Gautreneau, Délia Rahal-Löfskog avec l'aide de Valérie Bourriquen, Clément Commerçon, Viktorija Elenski, Pauline Faget, Estelle Hary, Antoine Planchot, Flora Sanchez et Clémence Scottez.

Conception graphique : Agence Linéal - 03 20 41 40 76

Impression : Le Réveil de la Marne

Illustrations : Lakee MNP (Adobe Stock)

SOMMAIRE

ÉDITO

Des transformations significatives des moyens de paiement sont à l'œuvre, en particulier depuis le début de la pandémie : recours accru au paiement sans contact, recul de l'usage des espèces, essor des achats en ligne. Ces évolutions structurelles s'accompagnent d'un déclin du recours aux espèces, de l'usage croissant des nouveaux moyens de paiement purement numériques comme le paiement mobile, les transferts entre particuliers et le recours aux portefeuilles numériques. Elles accompagnent le développement des Fintechs avec la mise en œuvre de la deuxième directive sur les services de paiement ouvrant à ces dernières les données bancaires.

Les enjeux économiques sont considérables. Ainsi, le géant américain du paiement Square a-t-il annoncé qu'il allait racheter le spécialiste australien du paiement fractionné Afterpay pour 29 milliards de dollars, soit plus que ce que Microsoft a consacré au rachat de LinkedIn. À terme, le domaine des paiements connaîtra des transformations encore plus profondes avec de nouvelles évolutions techniques comme le développement du virement instantané, le projet d'euro numérique lancé le 14 juillet dernier par la Banque centrale européenne mais aussi le projet de réseau paneuropéen de carte bancaire European Payments Initiative (EPI), qui feront évoluer encore le positionnement des acteurs économiques.

Or les données de paiement sont des données à caractère personnel : données d'achat, données financières, données contextuelles, elles concernent bien des aspects de l'existence des individus. Elles peuvent permettre de « tracer » leurs activités personnelles, de cerner leurs comportements ; elles peuvent être utilisées pour commettre des fraudes. En outre, le recours à tel ou tel moyen de paiement et, en particulier, les possibilités de recourir aux espèces comportent également des enjeux importants d'anonymat et de protection de la vie privée. La CNIL se devait d'analyser les enjeux de vie privée relatifs aux données de paiement, à leur circulation et à leur protection.

Ce Livre blanc s'adresse à la fois au grand public et aux professionnels. Il pose de premiers jalons d'analyse économique et juridique. Il est adossé à une consultation publique sur des questions de conformité plus précises et définit une feuille de route d'accompagnement des différents acteurs pour les années à venir. Ce rapport n'est, en effet, qu'une première étape dans le dialogue que nous entamons avec les parties prenantes. L'objectif est de parvenir, à terme, à une entière conformité des traitements de données des différents acteurs concernés (banques et leurs prestataires mais aussi commerçants, e-commerçants, prestataires de service de paiement) pas seulement pour protéger les personnes mais aussi pour renforcer également l'égalité concurrentielle entre tous les acteurs du marché français. Nous avons encore beaucoup à apprendre les uns des autres.

Les données de paiement sont aujourd'hui devenues un enjeu de souveraineté avec l'intérêt affiché des grands acteurs du numérique pour les moyens de paiement qui soulève avec davantage d'acuité encore les enjeux de vie privée liés aux transferts internationaux de données. La CNIL entend contribuer à ce débat sur les plans national et européen. Mais parce que le sujet est complexe et peu transparent, nous avons aussi l'ambition d'éclairer autant que possible les personnes sur les risques et les enjeux liés aux données et aux moyens de paiement.

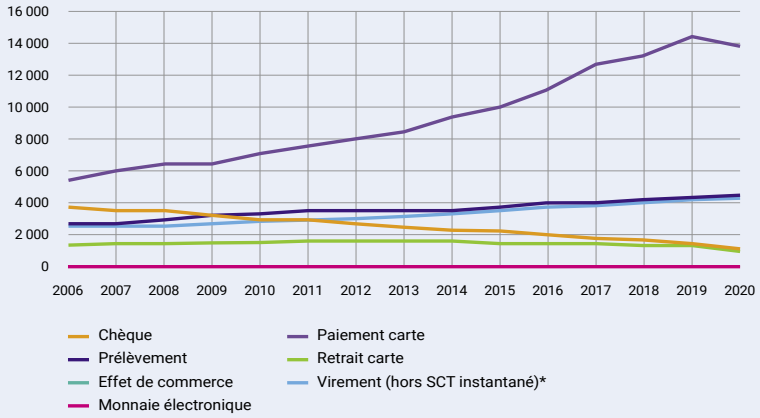
Enfin, l'économie numérique se nourrit de la confiance entre les personnes et les professionnels. Les nouveaux usages des données de paiement ne doivent pas déroger à cette réalité. Les enquêtes montrent que les clients sont parfois réticents à confier leurs données de paiement aux jeunes pousses européennes et autres Fintechs, nouveaux acteurs dans ce domaine. La CNIL aura atteint son objectif si elle contribue, à son échelle, à ce que la protection de la vie privée soit indissociable des mutations constatées en matière de services de paiements et d'une innovation responsable.

Marie-Laure Denis,
Présidente de la CNIL

CHIFFRES CLÉS

USAGE DES MOYENS DE PAIEMENT EN FRANCE DE 2006 À 2020

EN MILLIONS D'OPÉRATIONS



* SCT instantané (*SEPA instant credit transfert*) : virement instantané.

Source : Observatoire de la sécurité des moyens de paiement

59 %

DES PAIEMENTS EN POINT DE VENTE,

POUR 25 % DES MONTANTS PAYÉS, ÉTAIENT RÉALISÉS EN ESPÈCES EN FRANCE EN 2019

Selon l'enquête SPACE de la BCE, 2019

TENDANCE DES MOYENS DE PAIEMENT EN FRANCE

68 %

DES ADEPTES DES ACHATS EN LIGNE PENSENT QUE LA SÉCURITÉ DES DONNÉES ET DES TRANSACTIONS SUR UN SITE DE E-COMMERCE RESTE UN CRITÈRE DE SÉLECTION

Selon le Baromètre trimestriel de l'audience du e-commerce en France Fevad -Médiamétrie (4e trimestre 2020)

1 FRANÇAIS SUR 10

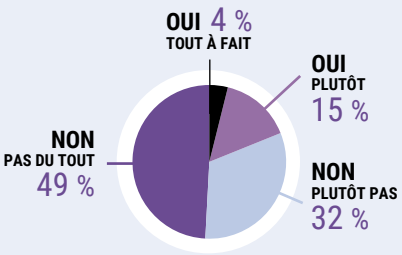
DÉCLARE UTILISER UN MODE DE PAIEMENT PAR ORDIPHONE

Selon la dernière étude du Global Consumer Survey menée à l'été 2020

81 %

DES PERSONNES INTERROGÉES NE SOUHAITENT PAS VOIR DISPARAÎTRE LE LIQUIDE AU PROFIT DE MOYENS DE PAIEMENT DÉMATÉRIALISÉS

Selon l'observatoire Ifop / Brink's 2019



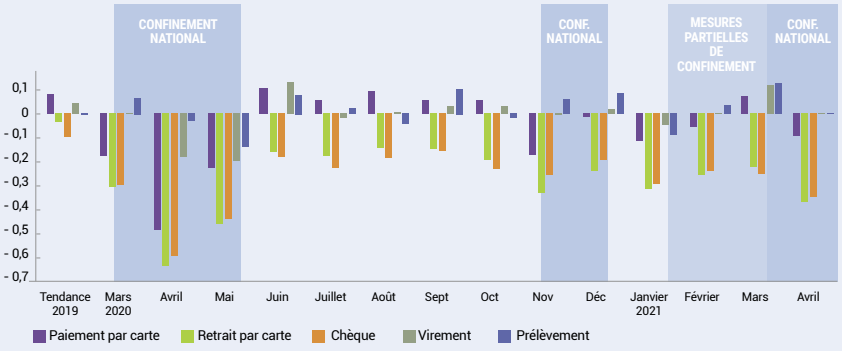
CHIFFRES CLÉS

CRISE LIÉE À LA COVID-19

Un recul très net, notamment pendant les périodes de confinement, des moyens de paiement impliquant un contact physique, une croissance du sans contact et des paiements en ligne (cartes, virements, prélèvements) traduisant une numérisation accrue des paiements.

ÉVOLUTION DES FLUX DE PAIEMENT EN VOLUME PAR RAPPORT À LA PÉRIODE DE RÉFÉRENCE PRÉ-CRISE (MARS 2019/FÉVRIER 2020) EN %

Selon le rapport 2020 de l'Observatoire de la sécurité des moyens de paiement



PAR RAPPORT À 2019

+ 37 %

POUR LES PAIEMENTS SANS CONTACT

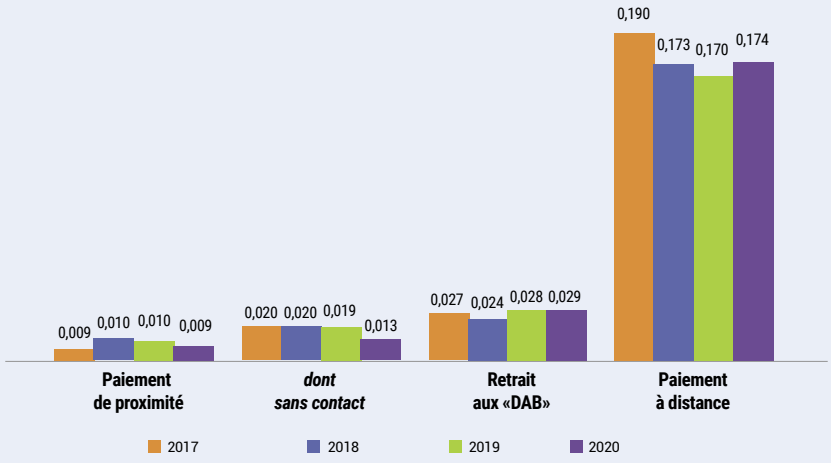
+ 13,2 %

POUR LES PAIEMENTS PAR CARTE EN LIGNE EN NOMBRE DE TRANSACTIONS

FRAUDE

COMPARAISON DES TAUX DE FRAUDE SUR LES TRANSACTIONS NATIONALES, PAR TYPE DE TRANSACTION (EN %)

Source : Observatoire de la sécurité des moyens de paiement



DAB : distributeurs automatiques de billets

2 825

NOTIFICATIONS DE VIOLATIONS DE DONNÉES REÇUES À LA CNIL EN 2020

DONT

311

POUR LES ACTIVITÉS FINANCIÈRES ET D'ASSURANCE

+ 5 %

EN 2020 PAR RAPPORT À 2019

Selon le rapport annuel 2020 de la CNIL

DONNÉES DE PAIEMENT : de quoi parle-t-on et pourquoi en parler ?

Les opérations de paiement, c'est-à-dire de versement d'une contrepartie monétaire à la mise à disposition d'un bien ou d'un service, sont d'une importance essentielle pour la vie économique et sociale.

La rapidité et la fiabilité du règlement des transactions, que ce soit entre professionnels (règlement-livraison des actifs sur les marchés financiers par exemple), entre professionnels et particuliers (achats de détail) voire entre particuliers (paiements de pair à pair) est un facteur clé de l'efficacité et du niveau de confiance dans l'économie.

La valeur ajoutée du secteur des paiements dans le monde était estimée en 2019 à quelque 1 500 milliards[1] de dollars, soit l'équivalent du PIB de l'Espagne, et en croissance de quelque 7 % par an avant la pandémie. Enfin, les opérations de paiement, qui emportent l'intégralité de la valeur des transactions dans l'économie, présentent un caractère systémique pouvant se révéler en cas de panne et de disruption des systèmes utilisés.

Une révolution des paiements est en marche : ce terme employé dès le rapport Pauget-Constans de 2012 sur l'avenir des moyens de paiement n'est plus aujourd'hui une métaphore. Le domaine des paiements se trouve en effet aujourd'hui au centre de trois bouleversements aux effets cumulatifs :

Un bouleversement technologique impliquant une mutation des usages

L'essor du commerce en ligne et corrélativement des paiements en ligne, l'usage de la monnaie électronique sur *wallet* et le paiement sur ordiphone ont modifié les comportements des consommateurs et renouvelé les conditions d'opération des paiements et de circulation des données correspondantes.

Un bouleversement concurrentiel et l'arrivée d'acteurs innovants

Face au couple traditionnel formé par les banques et les réseaux de cartes bancaires, se sont développés de nouveaux acteurs prestataires de service de paiement à la faveur du e-commerce ou rendant de nouveaux services en ligne aux consommateurs, mouvement qui s'est accompagné d'une irruption des grands acteurs du numérique dans ce domaine.

Un bouleversement réglementaire et dans l'accès aux données

La réglementation européenne a fait le choix de l'*« open banking »* avec la deuxième directive sur les services de paiement (DSP) de 2015 qui implique un accès encadré mais obligatoire aux données de compte bancaire par de nouveaux acteurs Fintechs.

L'enjeu pour l'économie française est important : les emplois dans la filière des moyens de paiement ont été estimés à **72 000 emplois directs et 18 000 indirects en 2014[2] avec une valeur ajoutée de 6 à 7 milliards d'euros,** dont la moitié en-dehors du système bancaire.

Aujourd'hui, comme le rappelle la récente stratégie en matière de paiements de détail de la Commission européenne, « autrefois relégués aux services de back office, les paiements ont acquis une importance stratégique »[3] et sont une question de « souveraineté économique et financière de l'Europe ». Enjeu économique, d'innovation et de souveraineté, risques pour la vie privée et les données personnelles : **nos données de paiement ne sont plus aujourd'hui dans l'ombre du secret bancaire. C'est pourquoi la CNIL a décidé de se saisir du sujet**. Les vues exprimées dans le cadre de ce Livre blanc lui permettront également de prendre toute sa part du débat européen sur ces questions.

> ***« Autrefois relégués aux services de back office, les paiements ont acquis une importance stratégique »***

1 - *Global Payments 2020, Fast forward into the future* [en anglais], octobre 2020, bcg.com
2 - Cartographie de la filière des moyens de paiement en France, avril 2014, finance-innovation.org
3 - Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions sur une stratégie en matière de paiements de détail pour l'UE, 24 septembre 2020, eur-lex.europa.eu

QU'EST-CE QU'UNE DONNÉE DE PAIEMENT ?

Les opérations de paiement[4] mettent en jeu de la monnaie, fiduciaire, scripturale ou électronique, des moyens de paiement (la technique permettant d'utiliser la monnaie pour réaliser la transaction), des systèmes de paiement (l'infrastructure utilisée par le transfert de fonds depuis l'initiateur pour atteindre son destinataire) et enfin des données de paiement.

Ces dernières peuvent être définies comme toutes les données collectées et traitées à l'occasion d'une opération de paiement, un champ potentiellement large et dont les liens avec d'autres types de données (historiques d'achat, données de connaissance client) sont de plus en plus forts avec l'essor du paiement en ligne.

Concrètement, les données qui nous intéressent ici tombent dans trois grandes catégories dont les frontières sont moins claires pour les paiements en ligne que pour les paiements physiques :

- **Données de paiement proprement dites :** entre autres identifiants du moyen de paiement utilisé, montant de la transaction, date et heure du paiement, identité du commerçant, identité du bénéficiaire, IBAN, score de lutte anti-fraude du client… Elles dépendent du moyen de paiement et du système de paiement utilisés et sont traditionnellement historicisées par les acteurs bancaires.

- **Données d'achat ou de caisse :** entre autres caractéristiques des produits achetés, date et lieu de l'achat, identifiants de la carte de fidélité le cas échéant… Elles sont observées lors de l'acte d'achat et traditionnellement collectées et historicisées par les commerçants (traditionnels ou en ligne).

- **Données contextuelles ou comportementales :** données de connaissance client, géolocalisation, caractéristiques du terminal utilisé pour un achat en ligne, caractéristiques des produits prospectés en amont de l'achat, temps passé à prospecter… Plus faciles à collecter lors d'un achat en ligne, elles sont aisément accessibles aux grands acteurs du numérique.

Au final, il est raisonnable de définir les données de paiement comme l'ensemble des données personnelles utilisées lors de la délivrance d'un service de paiement pour une personne physique, y compris des données annexes telles que la géolocalisation, des données contextuelles voire, selon le cas de figure, le détail des achats. Cette définition est d'ailleurs celle retenue par le régulateur des paiements britannique[5] alors que la directive sur les services de paiement (DSP2) ne définit pas cette notion. Dans ce Livre blanc, la CNIL se concentre sur les données personnelles associées aux paiements impliquant des particuliers.

À ce stade, il est important de rappeler que certains paiements (en espèces, en-dessous d'un montant de 1 000 € en France pour les paiements à un professionnel) n'engendrent pas de données personnelles associées et constituent aujourd'hui une alternative offerte à tous, comme discuté dans la suite de ce Livre blanc.

> ***Il est raisonnable de définir les données de paiement comme l'ensemble des données personnelles utilisées lors de la délivrance d'un service de paiement pour une personne physique***

4 - Une opération de paiement est définie comme une « action, initiée par le payeur ou pour son compte ou par le bénéficiaire, consistant à verser, à transférer ou à retirer des fonds, indépendamment de toute obligation sous-jacente entre le payeur et le bénéficiaire » (article L. 133-1 du Code monétaire et financier).
5 - *« Discussion Paper: Data in the Payment Industry »* [en anglais], 13 juin 2018, psr.org.uk.

LES DONNÉES DE PAIEMENT PEUVENT COMPORTER DES ENJEUX PARTICULIERS

Ces données sont des données à caractère personnel, car relatives à une personne physique (le client) identifiée ou identifiable, directement ou indirectement. Certaines sont qualifiées de données personnelles lorsqu'elles sont prises individuellement, d'autres le sont du fait de leur collecte conjointe avec d'autres données à des fins d'identification (ex : les caractéristiques du navigateur) ou parce qu'elles sont recoupables avec d'autres à des fins d'inférence sur une personne (ex : le montant d'une transaction).

D'une manière générale, et compte tenu de leur nature et des conditions de leur collecte, on les considérera comme personnelles sauf si elles ont fait l'objet d'une anonymisation.

Les données de paiement peuvent concerner de nombreux aspects de l'existence des personnes. Elles sont historicisées et conservées sur des comptes bancaires ou des porte-monnaie électroniques[6], au-delà du caractère éphémère des transactions, y compris sur de longues périodes. Elles ne sont donc pas sans rappeler ce que la Cour de justice de l'Union européenne (CJUE) dit des données de surveillance à grande échelle : « Ces données, prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci. »[7]

Une autre spécificité des données de paiement est qu'elles peuvent dans certains cas concerner des tiers et pas seulement la personne qui a réalisé une transaction : c'est le cas d'un paiement dont le bénéficiaire est une autre personne physique par exemple. Ces tiers sont dits « silencieux » car des données les concernant se trouvent retracées sur le compte d'une autre personne sans que le tiers puisse y accéder, ce qui comporte dans certains cas de figure des enjeux particuliers en termes de protection des données personnelles[8].

En outre, l'article 9 du Règlement général sur la protection des données (RGPD) protège particulièrement les données dites « sensibles », c'est à dire révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, les données biométriques aux fins d'identifier une personne physique de manière unique, les données concernant la santé ou celles concernant la vie sexuelle ou l'orientation sexuelle d'une personne. Si un simple transfert de fonds n'a pas pour objet de révéler de telles caractéristiques, les opérations de paiement dans leur ensemble peuvent occasionner un traitement de données sensibles au sens du RGPD, par exemple si une méthode d'authentification biométrique est utilisée.

Le Comité européen de la protection des données qualifie enfin certaines d'entre elles de « données hautement personnelles »[9] lorsqu'elles révèlent une géolocalisation ou peuvent être utilisées pour commettre des fraudes au paiement : c'est le cas des numéros de carte bancaire et autres identifiants de paiement par exemple. Ces dernières données concentrent évidemment des enjeux très élevés en termes de sécurité.

6 - Appelés également portefeuilles numériques (« *e-wallets* ») voir la définition de ces termes dans le glossaire.
7 - Arrêt de la CJUE, Grande chambre, « Digital Rights Ireland Ltd » (aff. C 293/12), considérant 27, 8 avril 2014, eux-lex.europa.eu.
8 - « Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR » [en anglais] (PDF, 308 ko), pp. 16 et suivantes, 15 décembre 2020, edpb.europa.eu.
9 - *Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/67* (PDF, 1,4 Mo), 4 octobre 2017, page 11.

LE CHAMP DES TRAVAUX : LES CONTOURS DE LA CHAÎNE DES PAIEMENTS

Comme les opérations de paiement elles-mêmes, les données de paiement concernent des acteurs économiques à la fois importants et nombreux :

- D'abord, elles concernent l'ensemble de la population, qui réalise des transactions monétaires pour l'ensemble des aspects de son existence. La dépense de consommation des ménages a ainsi représenté 1 268 milliards d'euros en France en 2019[10] soit, pour 67 millions d'habitants, quelque 18 650 euros par an et par habitant.

- Ensuite, les données de paiement (hors données d'achat) sont reflétées par les banques et réseaux de cartes bancaires (CB, Visa, Mastercard, etc.) : en France, le taux de bancarisation atteint 99 % d'après la Fédération bancaire française et 25 milliards d'opérations de paiement ont été traitées par les banques françaises en 2019. De même, 75 millions de cartes de paiement circulent en France, selon la BCE.

- Les commerçants et e-commerçants : le secteur représentait quelque 10 % de la valeur ajoutée de l'économie française en 2019[11] et 3,4 millions d'emplois.

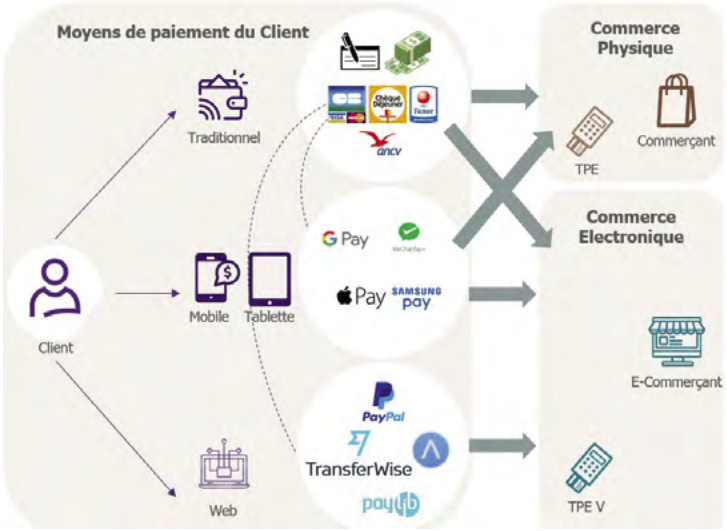
Au sein de ce secteur, la part du e-commerce est en croissance forte de plus de 10 % par an et représente désormais quelque 10 % du chiffre d'affaires du commerce de détail. En 2019, plus de 200 000 sites marchands étaient actifs en France selon la Fédération de la vente à distance (Fevad).

- Enfin, les prestataires de services de paiement, qu'ils soient physiques (prestataires monétiques en point de vente) ou numériques (permettant à un service d'accepter un paiement en ligne d'un client). Ainsi, au début de l'année 2021, 62 établissements de paiement étaient agréés en France, 8 prestataires de services d'information sur les comptes (PSIC), 15 prestataires de services d'initiation de paiement (PSIP) ainsi que 8 860 agents. Dans toute l'UE, on dénombre 715 établissements de paiement, 65 PSIC et 165 PSIP (source : sites web de l'Autorité de contrôle prudentiel et de résolution et de l'Autorité bancaire européenne).

Figure 1

Schéma simplifié de la chaîne des paiements selon le terminal utilisé.

Source : étude Wavestone pour la CNIL, décembre 2019



Les données de paiement circulent le long d'une chaîne assez longue et qui peut prendre deux grandes formes (Voir cartographie page 24). Lors d'une transaction physique, les données d'achat sont collectées par le parcours caisse et conservées par le commerçant, les données financières circulant le long de la chaîne monétique jusqu'au réseau de carte bancaire et aux banques où elles sont conservées. Lors d'une transaction en ligne, le parcours est moins normé : tous ces acteurs peuvent avoir accès aux données contextuelles voire certains d'entre eux aux données d'achat. La circulation des données financières soulève des questions de sécurisation avant de rejoindre l'acteur bancaire et le parcours des données via les prestataires de paiement en ligne relève de modèles et de pratiques hétérogènes.

10 - INSEE, Comptes nationaux annuels, série 2.201 – Consommation finale effective des ménages, mai 2020, insee.fr
11 - INSEE, Valeur ajoutée par branche, données annuelles, juin 2021, insee.fr

CARTOGRAPHIE DES MOYENS DE PAIEMENT EN FRANCE

La circulation et le devenir des données de paiement varient sensiblement selon le moyen de paiement utilisé. C'est pourquoi la dynamique des différents moyens de paiement est d'une grande importance pour les travaux de la CNIL. En particulier, les transactions en espèces ne donnent pas lieu en elles-mêmes à un traitement de données personnelles : elles sont anonymes. Il s'agit donc du moyen de paiement le plus protecteur de la vie privée[12].

Si l'on se concentre sur les paiements de détail (concernant les particuliers), les statistiques disponibles montrent que les deux principaux moyens de paiement sont, en France comme en Europe, la carte bancaire et les espèces. En France, les transactions en espèces sont les plus nombreuses, mais de plus faible valeur moyenne, alors que les transactions par carte représentent la majorité des montants.

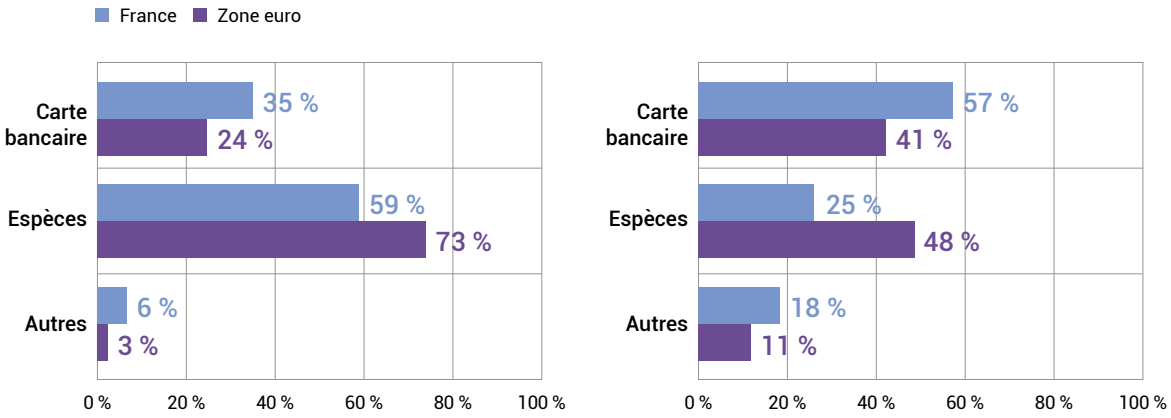
Hors des paiements en espèces (en monnaie dite Banque centrale ou fiduciaire) on parle de paiements scripturaux ou, comme le disent les économistes, réalisés en monnaie émise par les banques commerciales, sous le contrôle de ces dernières.

En France, **les paiements par carte**, dont les montants croissent année après année, ont atteint 578 milliards d'euros en 2020[13]. Son usage a légèrement baissé en 2020 (-4,3 % en volume par rapport à 2019) en raison du recul des paiements de proximité. **Le virement** de compte à compte, second moyen de paiement le plus utilisé et qui a été plutôt favorisé par la pandémie, concerne surtout les paiements à composante professionnelle (salaires, paiements interentreprises) et très peu les particuliers. **Les prélèvements** (hors chèques et cartes) sont le troisième moyen de paiement utilisé et peuvent l'être par les particuliers (mandat de prélèvement automatique par exemple)[14]. Ces moyens de paiement dématérialisés sont sécurisés par le système bancaire.

Figure 2

Part des différents moyens de paiement en point de vente et de pair à pair, en France et dans la zone euro (à gauche : en volume, à droite : en valeur).

Source : Enquête SPACE de la BCE (en anglais), données 2019, page 112



12 - On distingue la protection de la vie privée (article 7 de la Charte européenne des droits fondamentaux) et celle des données personnelles (article 8 de la Charte).
13 - Rapport 2020 de l'Observatoire de la sécurité des moyens de paiement (OSMP), juillet 2021, banque-france.fr, (PDF) page 19.
14 - Virement et prélèvement sont les deux grandes techniques de paiement via les comptes bancaires. À la différence du virement, effectué par le payeur, le prélèvement est effectué par le bénéficiaire, avec l'accord du payeur.

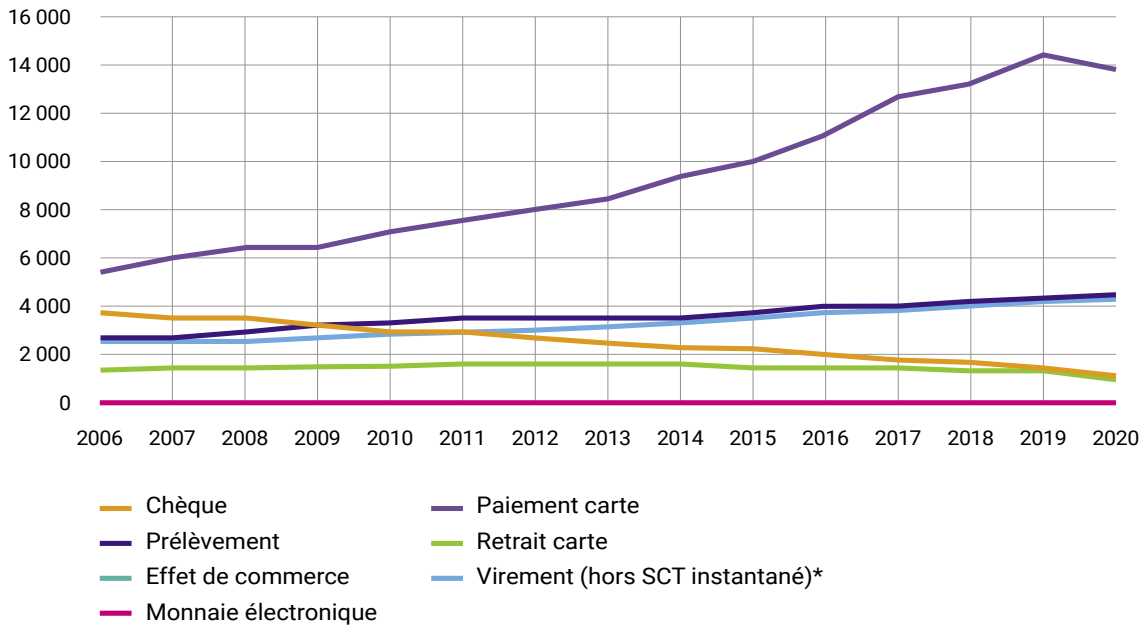
On remarque le déclin du **chèque**, qui reste ancré dans les habitudes des particuliers mais qui malgré la grande quantité de données personnelles qu'il comporte (nom, adresse, numéro de compte, signature…) est le moyen de paiement le plus fraudé : il ne nous intéressera pas ici car ne faisant pas partie des nouveaux moyens de paiement. **La monnaie électronique**, enfin, représente une part marginale des transactions scripturales (moins de 1 % tant en volume qu'en valeur) mais enregistre une hausse de son encours total qui s'établit à 688 millions d'euros (soit + 22,6 % par rapport à 2019).

À noter que lorsque le paiement est fait à distance, le choix du moyen de paiement est plus réduit : les principaux moyens de paiement utilisés (carte, virement, prélèvement) peuvent nécessiter une authentification potentiellement gourmande en données personnelles. Le champ de l'« anonymat » est également beaucoup plus limité (cartes prépayées sans compte bancaire, monnaie électronique peu répandue, avec des frais élevés et des plafonds d'utilisation très bas, qui handicapent ces solutions pourtant adaptées pour de faibles montants). Les banques en ligne les mettent d'ailleurs à disposition de leurs clients dans de meilleures conditions que les banques traditionnelles.

Figure 3

Usage des moyens de paiement en France de 2006 à 2020,en millions d'opérations.

Source : rapport 2020 de l'OSMP, juillet 2021, page 22



* SCT instantané (*SEPA instant credit transfert*) : virement instantané.

DES ACTIVITÉS RÉGULÉES PAR DES RÉGLEMENTATIONS MULTIPLES

La circulation et l'usage des données de paiement sont bien sûr soumis au RGPD, mais cette réglementation coexiste avec diverses autres réglementations dont la portée et l'articulation sont objets de toute l'attention des services de conformité des acteurs concernés.

Le domaine des paiements a longtemps été bien décrit par le distinguo entre monnaie fiduciaire (les espèces) émise par la banque centrale et rendue disponible pour le grand public par les quelque 50 000 distributeurs automatiques de billets que compte la France métropolitaine et monnaie scripturale.

Alors que les espèces relèvent de quelques règles simples comme le pouvoir libératoire ou le cours légal, la monnaie scripturale et les opérations associées relèvent des opérations de banque et sont traditionnellement régies par le droit bancaire, en France, par le Code monétaire et financier (CMF). Parmi les règles importantes pour les paiements on peut citer :

- **les règles européennes** de lutte contre le blanchiment des capitaux et le financement du terrorisme du livre 5 du CMF[15], risque pour lequel les opérations de paiement sont particulièrement sensibles puisqu'elles sont présentes tant à l'entrée en relation avec tout professionnel qu'au stade de la vigilance sur les transactions réalisées ;

- **les règles nationales** régissant l'externalisation de certaines fonctions des banques et notamment l'arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des entreprises d'investissement ;

- **les règles du secret bancaire,** également nationales (article L. 511-33 du CMF, voir page suivante).

De cette matrice bancaire se sont progressivement autonomisés, sous l'influence du droit européen et au nom de la promotion de l'innovation et de la concurrence par l'*« open banking »*, à partir de 2007, un régime d'opérations de monnaie électronique[16] (ex : PayPal) et un régime spécifique aux opérations de paiement. Ce dernier régime visait à mettre en concurrence les banques et des acteurs non bancaires pour les services de paiement pour à avancer vers un espace unique de paiements en euros à l'époque très fragmenté en Europe. Cette première directive de 2009 sur les services de paiement, instaurant le statut d'établissement de paiement, a été révisée par la directive dite DSP2[17] de 2015 permettant à des acteurs tiers de type Fintechs d'avoir accès aux comptes bancaires de leurs clients pour la réalisation d'un certain nombre d'opérations réglementées (initiations de paiement[18] ou informations agrégées sur les comptes[19]) avec un agrément du superviseur national, en France l'Autorité de contrôle prudentiel et de résolution (ACPR) et dans des conditions très sécurisées (notamment une contrainte d'authentification forte via, pour simplifier, l'application de banque en ligne).

En outre, quelques normes nationales d'ordre consumériste sont venues au fil du temps réglementer le recours aux moyens de paiement et aux preuves d'achat de détail mais de manière relativement lacunaire, traduisant d'ailleurs la moindre réglementation des opérations de commerce de détail par rapport aux opérations bancaires (par exemple : article D. 112-3 du Code monétaire et financier sur le plafond des paiements en espèces, arrêté du 3 octobre 1983 relatif à la délivrance d'une note pour tout achat supérieur à 25 euros, etc). S'agissant plus spécifiquement des paiements en ligne, les consommateurs sont également protégés par la réglementation nationale et européenne régissant les ventes à distance et par le principe selon lequel le fournisseur des instruments de paiement reste responsable des fraudes en ligne (protégeant le client de bonne foi).

15 - Transposant notamment la 5e directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme et la 6e directive (UE) 2018/843 du 30 mai 2018 la modifiant. À voir également le règlement (UE) 2018/1672 du Parlement européen et du Conseil du 23 octobre 2018 relatif aux contrôles de l'argent liquide entrant dans l'Union ou sortant de l'Union.
16 - Directive 2000/46/CE du Parlement européen et du Conseil du 18 septembre 2000 concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements, révisée en 2005 et en 2009.
17 - Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur.
18 - Prestataires de services d'initiation de paiement ou PSIP.
19 - Prestataires de services d'information sur les comptes ou PSIC.

Ce panorama serait incomplet sans mentionner les textes européens régissant les systèmes de paiement eux-mêmes, qui relèvent de règlements de compétence propre de la Banque centrale européenne, organisant par exemple la surveillance des réseaux de carte bancaire et de leurs opérations en Europe par les banques centrales[20] ainsi que les importantes règles du règlement dit « interchanges », relevant de la procédure européenne ordinaire, réglementant les commissions de ces réseaux[21].

Enfin, les activités de paiement, notamment sur les points peu régulés par les États, font l'objet de normes internationales élaborées par le secteur privé, notamment les grands réseaux internationaux de carte bancaire : normes dites Europay Mastercard Visa ou EMV, norme de sécurité PCI-DSS protégeant notamment la transmission des numéros de carte bancaire dans les infrastructures monétiques, norme 3DSecure pour la lutte contre la fraude dans les paiements en ligne, notamment.

« Les consommateurs sont également protégés par la réglementation nationale et européenne régissant les ventes à distance et par le principe selon lequel le fournisseur des instruments de paiement reste responsable des fraudes en ligne »

ZOOM SUR...

Secret bancaire et vie privée

Prévu par la loi, le secret bancaire est une forme de secret professionnel relatif, comportant des exceptions et dont le professionnel assujetti peut être délié par la personne qui en bénéficie. Il s'impose, en vertu des articles L.511-33 et L.522-19 du code monétaire et financier, aux établissements de crédit, aux sociétés de financement mais aussi aux établissements de paiement. Il bénéficie aux personnes tant physiques que morales. Sa violation est pénalement sanctionnée (un an d'emprisonnement, peine complémentaire d'interdiction professionnelle).

Selon un récent rapport du Haut comité juridique de la place financière de Paris, « les contours de cette obligation, dont le périmètre est très large, demeurent complexes à appréhender du fait d'une multitude d'exceptions disséminées dans la réglementation et d'évolutions jurisprudentielles régulières. L'appréhension du périmètre précis d'application du secret bancaire demeure source d'insécurité juridique, tant pour les personnes protégées que pour les établissements assujettis (et les personnes physiques astreintes au secret) qui restent exposés à des sanctions pénales, certes peu prononcées, mais particulièrement lourdes.[22]»

Si secret bancaire et protection des données personnelles relèvent du même esprit, les contraintes juridiques liées au secret bancaire semblent, selon certains acteurs, en raison de son périmètre très large, supérieures à celles issues du RGPD d'un point de vue opérationnel.

20 - Règlement UE n°795/2014 de la Banque centrale européenne concernant les exigences de surveillance applicables aux systèmes de paiement d'importance systémique.
21 - Règlement (UE) 2015/751 du Parlement européen et du Conseil du 29 avril 2015 relatif aux commissions d'interchange pour les opérations de paiement liées à une carte.
22 - Haut comité juridique de la Place financière de Paris, Rapport sur le secret bancaire, 6 juillet 2020, banque-france.fr.

MOYENS ET DONNÉES DE PAIEMENT : ENJEUX SOCIÉTAUX ET DE LIBERTÉS PUBLIQUES

Traçabilité

L'enjeu, voire le risque le plus évident de la circulation des données de paiement est celui de la connaissance potentiellement détaillée des transactions par des entités privées, opérant à grande échelle et capables de réutiliser cette connaissance pour leur propre compte. Les données de paiement s'appuient sur un régime documentaire pour tenir les comptes, identifier les clients et mémoriser leurs dettes, que ce soit pour des raisons de tenue de compte (chez les banques) ou fiscales (caisse en point de vente). Cette historicisation des données accroît leur valeur et leur attractivité pour le développement de nouveaux services, majoritairement réalisés par des acteurs tiers, de tailles diverses, spécialisés sur un type d'analyse (lutte anti-fraude, paiement de pair à pair, vision patrimoniale consolidée…).

Ainsi, la longueur de la chaîne multiplie le nombre d'acteurs susceptibles de « capter » les données. La numérisation des paiements accroît les possibilités de circulation et de combinaison de ces données avec d'autres. Les données de paiement sont susceptibles de nourrir une « économie de la surveillance » à l'instar des données du géant de l'internet chinois Alibaba (via ses filiales de e-commerce AliExpress et bancaire Ant Financial, utilisant la solution de paiement Alipay) utilisées pour nourrir le système de crédit social chinois.[23] La question se pose aussi en Europe, même si la réglementation actuelle fait obstacle à un tel scénario.

Anonymat

Un autre enjeu important concerne l'anonymat des transactions, permis par l'usage des espèces et qui est au cœur des transformations actuelles des moyens de paiement. Le choix d'un moyen de paiement est en effet déterminé principalement par les caractéristiques des transactions et la facilité d'utilisation. Si l'usage des espèces est plus fréquent pour les populations aux revenus plus faibles, le critère principal de choix du moyen de paiement est le montant de la transaction. En 2019, 92 % des transactions de moins de 5 euros étaient réalisées en espèces dans la zone euro[24], même si la situation a évolué depuis lors avec la pandémie. Les espèces sont également privilégiées pour les paiements en magasin, utilisées en France avant la pandémie pour plus de 50 % des paiements de moins de 20 euros.

Les espèces présentent des avantages qui rendent peu probable leur totale disparition. L'argent liquide est à ce stade le seul moyen de paiement universellement accepté partout sur le territoire pour toute forme de paiement. Outre le pouvoir libératoire, l'accès aux espèces est aisé et leur usage garantit l'anonymat de la transaction, d'où leur popularité auprès du grand public. Toutefois, le risque est de voir apparaître, selon le mot de Tim Wu, une forme de « tyrannie de la commodité »[25]: en rendant les alternatives aux espèces suffisamment pratiques dans la vie quotidienne, la part des espèces pourrait inexorablement se réduire. L'usage des espèces a ainsi le potentiel de devenir assez marginal, ce qui aurait des conséquences en termes d'inclusion sociale et de protection de la vie privée (voir aussi la contribution de Marc Schwartz, page 19).

Plusieurs économies nationales sont déjà converties au « *cashless* ». En Suède par exemple, l'application Swish, introduite en 2012 par six banques scandinaves, est aujourd'hui utilisée par plus de 50 % de la population pour régler les petites transactions. En Chine, sous l'impulsion d'Alipay et de WeChat, 80 % des paiements s'effectuent via mobile en 2018 contre moins de 20 % en 2013. De 2010 à 2016, la Suède est passée de 40 à 15 % de transactions en espèces dans les commerces. Les promoteurs du « *cashless* » mettent en avant l'efficacité, le gain de temps et d'argent, la sécurité de ce moyen de paiement pour les clients et les commerçants, la lutte contre la fraude et le terrorisme. Pour les banques françaises, la diminution de la part des espèces et des chèques, des moyens de paiement très coûteux à entretenir (10 à 15 000 € par an pour un distributeur de billets), représente un enjeu de profitabilité majeur.

La disparition de la monnaie fiduciaire présenterait aussi des enjeux importants pour la vie privée et les libertés. Avec les espèces, les transactions entre deux personnes peuvent être effectuées sans qu'aucun tiers ne soit au courant. Les entreprises ne peuvent proposer de la publicité à partir des habitudes de transaction ou des sources

23 - Voir par exemple « Le système de crédit social · Comment la Chine évalue, récompense et punit sa population », juillet 2019, institut-thomas-more.org.
24 - Étude SPACE de la BCE, déjà citée, tableau 11 page 31, décembre 2020, ecb.europa.eu.
25 - « La tyrannie de la commodité », 24 mars 2018, lemonde.fr.

de revenus, ou attribuer un score de crédit, les gouvernements ne peuvent tracer ces dépenses et le conjoint qui a accès au compte joint ne peut pas savoir quel cadeau lui est préparé. La fin des espèces marquerait la fin de l'anonymat des transactions. Il deviendrait possible de tracer systématiquement les paiements : de savoir ce qu'une personne a acheté, à qui, à quelle fréquence et à quel prix. Cette traçabilité faciliterait certes, sous nos longitudes, le travail des administrations publiques pour identifier les fraudes fiscales, mais le prix à payer en termes de vie privée serait peut-être disproportionné.

Au-delà des paiements, l'anonymat apparaît comme une condition essentielle du fonctionnement des sociétés démocratiques : c'est par la défense de l'anonymat que peuvent s'exercer plusieurs libertés fondamentales essentielles (vote secret, liberté de publication anonyme, anonymat de la prise en charge hospitalière, secret professionnel, secret des correspondances, liberté d'aller et venir anonymement…). Et s'il n'existe pas de droit à payer anonymement, cette possibilité n'est-elle pas au soutien de nombre d'autres droits et libertés, vu les liens existant entre données de paiement et données de localisation, de santé, d'achat ou d'informations qu'elles comportent sur les liens entre les personnes ? De ce point de vue, les atteintes à l'anonymat dans les paiements devraient s'accompagner d'une réflexion sur leur proportionnalité et leur nécessité dans une société démocratique, pour reprendre les termes adoptés par la jurisprudence de la CJUE.

La parole à...
MARC SCHWARTZ

Marc Schwartz *est PDG de la Monnaie de Paris depuis décembre 2018 et enseigne l'économie des médias et des industries culturelles à l'École des affaires publiques de Sciences Po Paris. Issu de la Cour des comptes, passé par la direction du Trésor, France Télévisions et le cabinet Mazars, il a également été directeur du cabinet de la Ministre de la culture (Françoise Nyssen) en 2017. Il est diplômé de Sciences Po Paris, ancien élève de l'ENA et titulaire d'un master de finance d'entreprise et d'un Executive MBA.*

À l'occasion de la crise sanitaire de la COVID-19, le paiement sans contact a connu un essor significatif. L'idée que nos sociétés allaient progressivement et inéluctablement vers un avenir sans cash a été relayée par de nombreux médias. À tort, selon Marc Schwatz, PDG de la Monnaie de Paris.

Dans votre étude "*Le grand paradoxe* – ou pourquoi le règne du cash est loin de s'achever" parue chez Terra Nova[26] , vous vous inscrivez en faux contre cette prétendue évidence. Quels éléments sous-tendent votre analyse ?

Tout d'abord, la réalité des chiffres. Le montant des espèces en circulation n'a jamais été aussi élevé, dans le monde entier, et n'a d'ailleurs jamais cessé de croître ! Le volume de dollars et d'euros en circulation a augmenté annuellement de 6 % à 8 % au cours des vingt dernières années. À la fin de l'année dernière, on comptait plus de 1 400 milliards d'euros de pièces et de billets qui circulaient. Et en 2020, en pleine crise sanitaire, l'augmentation s'est même accélérée : + 11 % pour l'euro et + 15 % pour le dollar. Si le cash devait disparaître, c'est l'inverse que l'on constaterait.

Je rappelle par ailleurs que l'argent liquide est la seule forme de monnaie émise par les banques centrales qui soit accessible au grand public et qu'il constitue ainsi un des piliers de la confiance dans la monnaie. Ce n'est pas un hasard si les citoyens refusent d'abandonner le cash. Lorsqu'on les interroge, ils se déclarent très majoritairement en faveur du maintien des espèces, preuve d'un réel attachement à la monnaie physique. Huit ménages sur dix en France et sept ménages sur dix aux États-Unis se déclarent opposés à la disparition de l'argent liquide ; et 74 % des Britanniques pensent qu'un monde sans cash les priverait de leur liberté de choix.

> ***« Ce n'est pas un hasard si les citoyens refusent d'abandonner le cash »***

Enfin, l'argent liquide reste un mode de paiement apprécié des particuliers. La dernière étude publiée par la Banque centrale européenne (BCE) établit que, en 2019, près des trois-quarts des paiements effectués aux points de vente

26 - « Le grand paradoxe – ou pourquoi le règne du cash est loin de s'achever », 8 janvier 2021, tnova.fr.

dans la zone euro ont été réglés en espèces, représentant 48 % de la valeur totale des paiements. Contrairement aux idées reçues, et même si leur usage diminue, les espèces restent donc un mode de paiement apprécié des consommateurs européens.

Quels sont les atouts dont peut se prévaloir l'argent liquide pour garantir son maintien à terme ?

L'argent liquide est un moyen de paiement universel, sûr et entièrement gratuit, que les particuliers peuvent utiliser pour régler instantanément leurs dépenses. C'est la seule forme de monnaie dotée d'un cours légal et d'un pouvoir libératoire immédiat, fût-il encadré par la réglementation. Les cartes bancaires ou les applications de paiement ne disposent pas d'un tel privilège et sont loin d'être universellement acceptées – sans même parler du Bitcoin !

L'argent liquide permet à ceux qui n'ont pas de compte ou de carte bancaire, ou qui n'ont pas une maîtrise suffisante des outils numériques, d'accéder à un moyen de paiement. Sans cash, des millions d'individus seraient incapables d'acheter des biens essentiels et se trouveraient encore plus en marge de la société. En France, où le taux de bancarisation approche de la saturation, 3 millions de personnes sont néanmoins en situation d'exclusion financière.

L'accès aux services numériques est tout aussi discriminant : l'INSEE considère qu'un Français sur six souffre « d'illectronisme », ou « illettrisme numérique ». L'inclusion financière constitue donc un motif majeur du maintien de l'accès aux espèces. La BCE considère d'ailleurs que la possibilité de payer en espèces « est importante pour certains groupes qui, pour de nombreuses raisons légitimes, préfèrent le cash à d'autres modes de paiement, ou ceux qui ne sont pas en mesure d'utiliser la technologie digitale ».

Par ailleurs, l'argent liquide est résilient : il n'a pas besoin d'un branchement électrique ou d'une liaison internet. Enfin, c'est également un support d'épargne, vers lequel les ménages, notamment les plus modestes, se tournent en temps de crise. Comme l'or pour les ménages les plus aisés, le cash est une valeur refuge, surtout quand les taux d'intérêt sont bas, voire négatifs. C'est ainsi que l'on peut expliquer le rebond de la demande d'espèces dans le monde en 2020 : par ce rôle de thésaurisation.

Au-delà du rôle essentiel que joue le cash dans l'inclusion financière des ménages les moins favorisés, comment expliquez-vous l'attachement de tous à son maintien ?

Cet attachement aux espèces s'explique par des raisons de nature rationnelle, mais aussi par des raisons psychologiques ou symboliques.

Tout d'abord, le maintien de l'argent liquide ressort de la protection des libertés individuelles. La disponibilité d'une variété de moyens de paiement permet de choisir entre eux, selon ses préférences et selon les circonstances. Cette liberté de choix est le plus sûr garant de la confiance dans la monnaie.

De plus, les espèces permettent de régler une transaction de manière immédiate et anonyme, et donc de protéger les données individuelles. Et cet anonymat n'est pas, pour l'immense majorité des ménages, le paravent d'activités illégales !

Les paiements par carte ou en ligne laissent derrière eux un historique de paiement accessible par des entreprises privées, qui peuvent les utiliser à des fins publicitaires : c'est ce que font les géants du Net, et c'est ce qui explique leur attrait récent pour le marché des paiements. Les données pourraient aussi être utilisées par des gouvernements peu soucieux des libertés publiques. Des avertissements sur les possibles utilisations néfastes de données de paiement émergent de Chine, où certains pourraient être tentés d'utiliser les réseaux sociaux par exemple pour humilier publiquement les individus en retard sur le règlement de leurs dettes.

Par ailleurs, et s'il va de soi que l'argent liquide peut être utilisé à des fins illégales, son usage est plus sévèrement contrôlé aujourd'hui : limites de paiement en liquide dans les magasins ou pour régler ses impôts, enquêtes bancaires en cas de mouvements importants, etc. Et l'on constate que les manœuvres frauduleuses sur les moyens de paiement électroniques se développent, par exemple en Afrique avec les téléphones mobiles ou via les cryptomonnaies.

Enfin, la monnaie ne constitue pas seulement un moyen de paiement désincarné, mais aussi une institution qui crée du sens et signale l'appartenance à une communauté. Comme le disait récemment l'économiste Jacques Mistral : « la monnaie n'est pas une chose, elle est une relation sociale ».

Suridentification

À ces enjeux d'anonymat des paiements se combine la question de l'identification. L'usage des moyens de paiements scripturaux nécessite que la banque connaisse l'identité du débiteur et du créditeur mais cette identité est de plus en plus souvent requise par d'autres services utilisant des données de paiement, pour éviter les fraudes par exemple. L'évolution des paiements, notamment la part de plus en plus importante des paiements à distance, génère donc un risque de « suridentification » des personnes, de divulgation de leurs attributs d'identité allant au-delà de ce qui est nécessaire pour rendre le service demandé, qui peut la plupart du temps être rendu sur la base d'un identifiant déclaratif, voire d'un pseudonyme.

Au nom de la lutte contre la criminalité financière, de toutes les formes de fraude (aux paiements, fiscale), et à terme d'un élargissement des points sur lesquels une surveillance est requise, « le danger est que le paiement ne se moralise », pour reprendre la formule d'un avocat, et que le traditionnel principe selon lequel l'opération de paiement est indépendante de la transaction sous-jacente et n'a pas à en connaître, soit peu à peu perdu de vue à la faveur de la numérisation des opérations. Le grand public ne le souhaite pas, et s'avère plutôt réticent à l'utilisation d'une identité numérique officielle (dite « régalienne ») pour des usages financiers (paiement sur internet, opérations de banque en ligne, demande de crédit…) alors que l'usage d'une identité numérique régalienne est mieux accepté pour des démarches administratives, quoique non majoritairement (voir figure 4). Au final, le public apparaît assez conscient de la balance bénéfices/risques de l'identification pour chacun des cas d'usage.

Figure 4

Le besoin d'une identité numérique régalienne pour les Français selon les cas d'usage.

Source : sondage Ifop pour Acteurs Publics / EY, mars 2021

Inclusion

Un quatrième enjeu a trait à l'inclusion financière et sociale. L'évolution des moyens de paiement vers des solutions de plus en plus numériques a des effets contrastés. D'un côté, la dématérialisation des paiements pose la question de la « fracture numérique » et de l'accessibilité des solutions correspondantes, notamment en France où, selon l'INSEE, une personne sur six n'utilise pas Internet (plus d'une personne de plus de 75 ans sur 2 n'a pas accès à Internet) et plus d'un usager sur trois manque de compétences numériques de base[27]. Un quart des Français ne dispose pas d'un ordiphone (smartphone), car si presque 100 % de la tranche d'âge 18-40 ans en possède un, ce n'est pas le cas de plus d'un Français sur deux de plus de 70 ans, et un quart également de la population ne dispose pas d'un ordinateur, selon le Crédoc[28].

L'accès à des services de paiement universels pour la population est donc un enjeu, surtout lorsque l'authentification est requise pour utiliser le service. Ainsi, la généralisation de l'authentification forte par le recours à l'application de banque en ligne à la suite de la pleine entrée en vigueur de la directive DSP2 comporte-t-elle des enjeux d'inclusion pour les personnes qui n'ont pas d'ordiphone. C'est pourquoi, les pouvoirs publics demandent aux établissements bancaires de proposer des alternatives dont au moins une gratuite.

D'un autre côté, le développement de moyens et de solutions de paiement alternatifs peut favoriser l'inclusion financière, en abaissant par exemple le coût des transferts d'argent ou en fournissant de nouveaux services d'encaissement ou de vente en ligne à des très petites entreprises jusqu'ici privées de ces possibilités. Selon le Fonds monétaire international, ces bénéfices s'observent notamment dans les pays en développement[29], moins dans un pays comme la France.

Surveillance étatique

Conséquence de leur richesse pour appréhender la portée des actes des individus et de leur haute traçabilité dans les systèmes de paiement, les données de paiement sont d'un intérêt particulier pour la détection des crimes et des infractions. La surveillance des transactions est ainsi l'une des composantes des obligations des entités financières au titre de la lutte anti-blanchiment, et on sait que les transactions anonymes en espèces comportent plus de risques à ce titre, de même qu'au titre de la lutte contre la fraude fiscale.

Le sujet de la lutte contre le blanchiment et le financement du terrorisme (LCB-FT), dont un des enjeux est la bonne articulation avec le RGPD et qui relève d'autres travaux en cours de la CNIL et du Comité européen de la protection des données[30] n'est pas spécifique aux paiements et ne sera donc pas développé plus avant dans ce Livre blanc. Certes, les nouvelles technologies numériques peuvent susciter des risques nouveaux en la matière tout comme des possibilités de traçage plus étroit des transactions pour y faire face. Ces enjeux concernent toutefois les crypto-actifs en général, qui sont plus des réserves de valeur utilisées à des fins spéculatives que, à ce jour, des moyens de paiement à proprement parler (voir encadré sur le paiement crypto page 43). Le même débat est en cours s'agissant du projet d'euro numérique, qui devrait présenter les mêmes caractéristiques que le cash (voir page 45 et suivantes).

Pour les mêmes raisons, les données de paiement sont par ailleurs devenues, depuis les attentats du 11 septembre 2001, un enjeu pour les services de renseignement. En 2006, les autorités de protection des données européennes ont été saisies de plaintes concernant le système de règlement interbancaire SWIFT, qui fournissait des données aux autorités américaines à l'insu des personnes concernées. En 2013, l'affaire Snowden a révélé que les analystes de la National Security Agency américaine suivaient une approche dite « *follow the money* » (« suivez l'argent ») utilisant des données financières et en particulier, des données de carte bancaire. Selon l'hebdomadaire allemand Der Spiegel, cette surveillance s'exerçait principalement aux États-Unis mais s'étendait en Europe, en Afrique et au Moyen-Orient, des théâtres d'opérations prioritaires pour tous les services de renseignement.

Dans cette optique, il ne fait pas de doute que les données, les moyens et les systèmes de paiement font l'objet d'enjeux de souveraineté tant pour les citoyens européens que pour les États européens, qui ont édicté des règles pour la protection des données personnelles de leurs citoyens (voir page 70 et suivantes).

27 - « Les compétences des Français dans la moyenne de l'UE ». Une personne sur six n'utilise pas Internet, plus d'un usager sur trois manque de compétences numériques de base », 30 octobre 2019, insee.fr.
28 - « Baromètre du numérique 2019 », novembre 2019, credoc.fr.
29 - « L'inclusion financière numérique au temps de la COVID », 1er juillet 2020, imf.org.
30 - « Déclaration relative à la protection des données à caractère personnel traitées dans le cadre de la prévention du blanchiment de capitaux et du financement du terrorisme » (PDF, 70 ko), adoptée le 15 décembre 2020, edpb.europa.eu.

ZOOM SUR...

LCB-FT et protection des données personnelles

Dans le cadre de la révision en cours des textes européens régissant ce domaine, les principes de protection des données personnelles peuvent concourir à renforcer l'efficacité du cadre LCB-FT dans la mesure où les données utilisées par ce dernier, que ce soit du fait des entités assujetties ou de leurs sources tierces, sont exactes, pertinentes et à jour, à l'appui d'une évaluation ciblée et proportionnée des risques.

C'est pourquoi, le Comité européen de la protection des données (CEPD) a publié, en mai 2021, une lettre de position aux autres institutions européennes[31] rappelant l'importance d'une articulation équilibrée entre la prévention des risques LCB-FT et la protection des données personnelles, tant dans l'intérêt des libertés publiques que pour la sécurité juridique des opérations des responsables de traitement assujettis à la lutte anti-blanchiment.

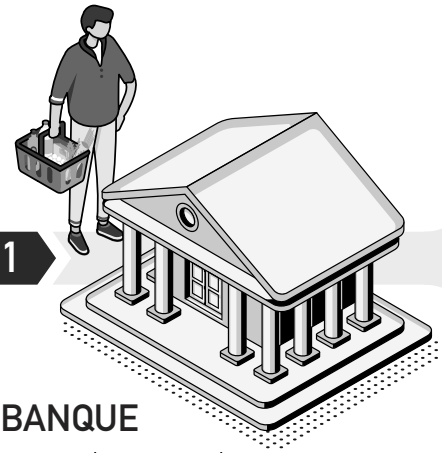
Dans cette lettre, le CEPD recommande notamment l'adoption d'un cadre spécifique de licéité s'agissant des données personnelles fournies par les sources externes, la définition de standards de proportionnalité dans le cadre de l'approche par les risques, des précisions s'agissant de la minimisation des données collectées. Il recommande que les données utilisées, tant par les assujettis que par leurs sources externes, soient exactes, fiables et à jour, et que les périodes de conservation de ces données ne soient pas excessives. Il souligne la nécessité d'adopter un cadre légal spécifique, avec des garanties appropriées, pour pouvoir traiter des données sensibles ou des données relatives aux condamnations pénales et aux infractions. Il appelle enfin à une coopération entre autorités de supervision lors de l'édiction de lignes directrices, tant au plan européen que national.

D'une manière générale, l'articulation entre les règles LCB-FT et le RGPD doit être guidée par les principes de nécessité dans une société démocratique et de proportionnalité des atteintes aux droits à la vie privée et à la protection des données consacrée par les articles 7 et 8 de la Charte européenne des droits fondamentaux.

31 - Lettre du CEPD aux institutions européennes sur l'articulation entre la prévention des risques LCB-FT et la protection des données personnelles (PDF, 235 ko) [en anglais], 19 mai 2021, edpb.europa.eu

DE COMPTE À COMPTE

Une cartographie simplifiée des moyens de paiement et des principaux acteurs associés.

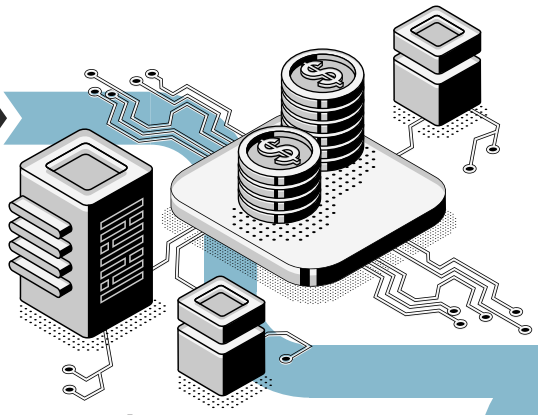


1

BANQUE

Fournit des services bancaires, comme par exemple un compte bancaire ou une application de banque en ligne.

HSBC



3

MONNAIE ÉLECTRONIQUE

Monnaie stockée sur des mémoires électroniques, indépendamment d'un compte bancaire. Peut être gérée par un porte-monnaie numérique.

Skrill PayPal

payLib

Lutte contre la fraude, initiation, cashback

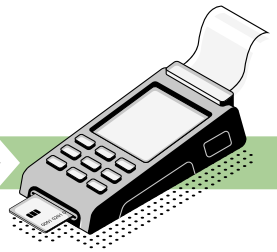
RÉSEAU DE CARTE DE PAIEMENT

4

Définit les règles leur interopérabilité entre banques, y compris à l'étranger.

VISA

mastercard



7

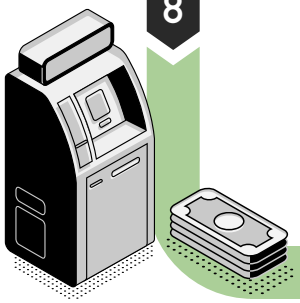
TERMINAL DE PAIEMENT ELECTRONIQUE

Lit les données d'une carte bancaire pour authentifier et lancer une transaction auprès d'un commerçant.

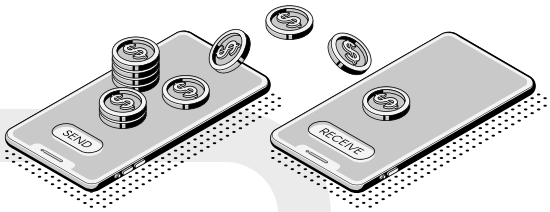
ESPÈCES

8

Moyen le plus anonyme pour réaliser ses achats, les espèces se retirent à un distributeur automatique de billets.



Opérations en ligne
Opérations en point de vente



2

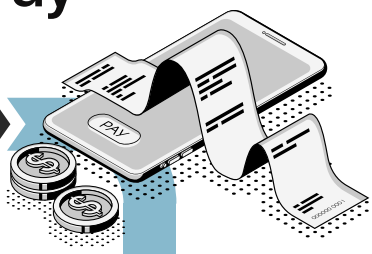
VIREMENTS

Transfert de sommes directement de compte à compte.

HUAWEI pay

Pay

SAMSUNG pay



5

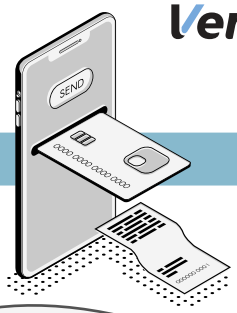
PAIEMENT MOBILE

Permet d'effectuer des paiements avec son téléphone. Généralement associé à un porte-monnaie numérique.

stripe

Square

verifone

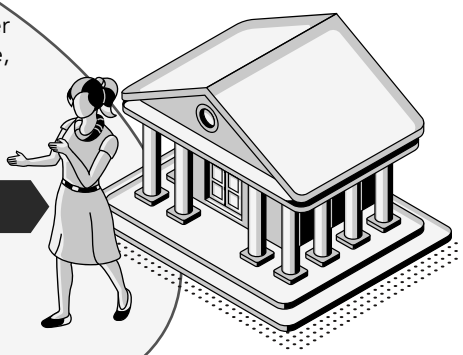


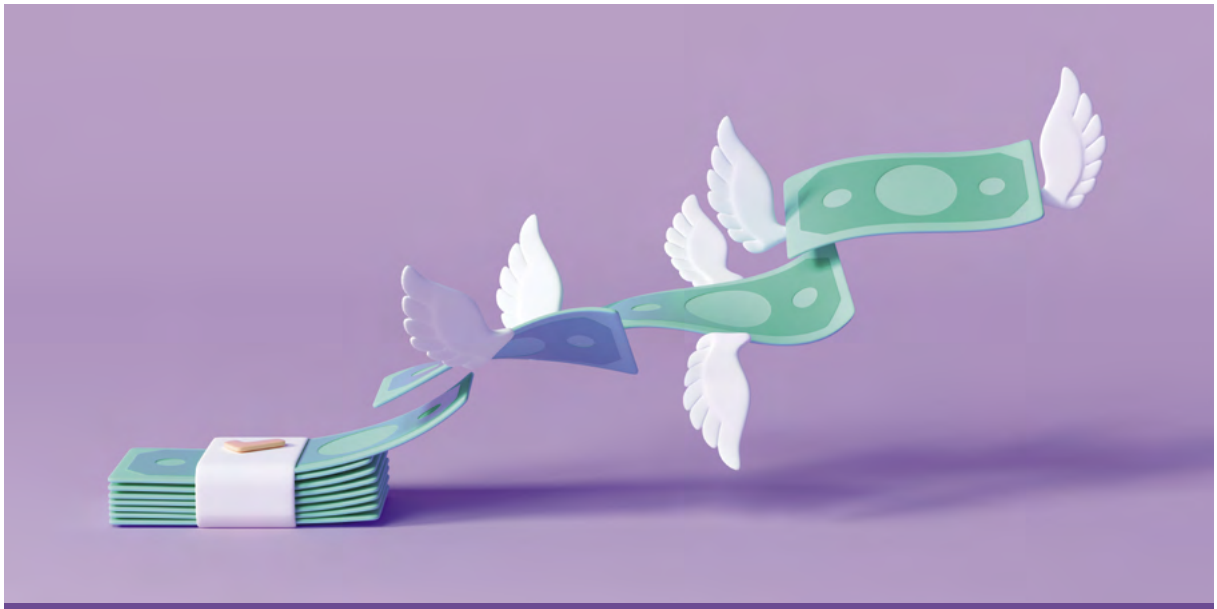
6

PRESTATAIRE DE SERVICE DE PAIEMENT

Permet aux commerçants d'accepter les paiements, physique ou en ligne, souvent réalisés par carte bancaire.

Scoring, facturation, programme de fidélité, paiement fractionné





ANCIENS ET NOUVEAUX MOYENS DE PAIEMENT : un écosystème complexe, des acteurs nouveaux

D'un point de vue économique, il importe que l'opération de paiement, contrepartie d'une transaction sous-jacente (commande d'un objet, délivrance d'un service, livraison d'un actif financier) et qui se traduit par un mouvement de fonds, se dénoue auprès du bon destinataire, si possible rapidement et à un coût modique. Les opérations qui nous intéressent ici ont lieu entre une personne physique et un professionnel, typiquement entre un commerçant et son client. Du point de vue du client, l'objectif est la fluidité et la simplicité d'utilisation, mais les techniques mises en œuvre pour parvenir à cet objectif peuvent être très complexes. Elles reposent sur des infrastructures développées par les banques et achetées par les commerçants, qui comportent deux aspects principaux : un corps de règles de gestion des transactions et une répartition des coûts (« modèle économique »).

La principale infrastructure de paiement en France pour les particuliers est l'infrastructure monétique physique des cartes de paiement dites "bancaires", qui a représenté, en 2019, 58 % du nombre des paiements scripturaux[32]. Cette infrastructure est très coûteuse puisqu'elle représente, rien qu'en France, plusieurs milliards d'euros de commissions par an[33], mais également très performante en termes de rapidité et facilité d'usage. Elle est également peu fraudée (0,064 % en 2019 selon le rapport de l'Observatoire sur la sécurité des moyens de paiement[34]). Son seul véritable concurrent est le paiement en espèces qui représentait, en 2019, 59 % du nombre total des transactions en France[35].

Complexe, le secteur du paiement se structure autour de grandes catégories d'acteurs aux intérêts pas toujours convergents : les banques, les réseaux de carte bancaire ou « *schemes* », les commerçants (grands et petits), les prestataires de services de paiement physiques (PSP) ou en ligne (e-PSP), dont certains sont spécialisés dans le virement, les porte-monnaie numériques (« *wallets* »), les solutions de cashback, mais également les e-commerçants, les prestataires de monnaie électronique et les acteurs de paiement sur mobile (dits X-pay), qui sont pour ces derniers des acteurs purement numériques. Pour certains, ils sont issus d'une externalisation des services bancaires (*schemes*, PSP), pour d'autres, leur intérêt est plutôt de s'intermédier entre le client et la banque pour capter la valeur économique qui repose bien souvent sur les données correspondantes (e-PSP, solutions X-pay). Souvent, ils s'appuient sur l'infrastructure de paiement existante où ils opèrent des optimisations visant à réduire les délais ou les frais de transaction, ou proposent de nouveaux services basés sur l'analyse des données de transaction.

Le système de carte bancaire est ainsi partiellement réutilisable pour le commerce en ligne, pour lequel **80 % du chiffre d'affaires est réalisé en France via une carte bancaire**[36]. Mais les enjeux des paiements en ligne et les acteurs correspondants sont bien différents, avec des risques pour la protection des données plus élevés car, si le circuit monétique physique est fermé par des règles de gestion strictes de l'information, le mouvement des données sur internet est par construction ouvert et peu coûteux. Ainsi, le risque de fraude y est plus élevé (pour la carte bancaire, 0,17 % contre 0,01 % en point de vente physique).

Figure 5

Représentation de l'écosystème des paiements.

Source : Étude Wavestone pour la CNIL, décembre 2019

32 - Cartographie des moyens de paiement scripturaux, bilan de la collecte 2020 (PDF, 2,2 Mo), page 112, banque-france.fr.
33 - Entre 1,2 et 1,8 Md€ par an à la charge des commerçants (600 Md€ en 2019 en France montants des paiements par carte selon la Banque de France entre 0,2 et 0,3 % de commission d'interchange sur ces montants) ; pour les cartes 30 à 50 € par an et par carte à dire d'expert avec 71 millions de cartes en circulation en 2019 soit entre 2 et 3,5 Md€ à la charge des porteurs de carte. Pour sa part le rapport Pauget-Constans évaluait ce montant à 2,6 Md€ en 2012 (source : economie.gouv.fr).
34 - Observatoire sur la sécurité des moyens de paiement, rapport annuel 2019 (PDF, 1,8 Mo), page 19, banque-france.fr.
35 - *Study on the payment attitudes of consumers in the euro area* (SPACE) [en anglais], décembre 2020, ecb.europa.eu.
36 - Contre 11,5 % pour les porte-monnaie électroniques, 4 % via le crédit à la consommation et seulement 1 % pour les virements ou prélèvements (source : chiffres Fevad 2018).

UN HISTORIQUE DES DONNÉES ET MOYENS DE PAIEMENT AU XX^{E} SIÈCLE

Premier des moyens de paiement contemporains, les cartes de crédit ont été introduites aux États-Unis au début du XX^{e} siècle. Leur fonction est de faire l'interface entre l'identité du client, son compte, pour assurer pour une transaction donnée une relation de confiance entre le vendeur et l'acheteur.

En 1914, Western Union, alors la principale entreprise télégraphique aux États-Unis, fournit à ses clients des cartes en papier indiquant leur identité et permettant d'associer à leur compte leurs factures. Apparaissent ainsi dans de nombreuses firmes et grands magasins des systèmes permettant de faire le lien entre l'identité d'un client et l'historique de ses transactions. Ces dispositifs de paiement n'étaient pas universels : limités à chaque magasin (ou chaîne de magasins), ils remplissent également le rôle de carte de fidélité. Ils ne sont pas, à cette époque, associés à un compte bancaire.

Il faut attendre les années 1950 et 1960 pour qu'émergent progressivement des systèmes de cartes de crédit universels avec la constitution, par des partenariats entre banques, de larges infrastructures qui deviendront les réseaux American Express, Visa et Mastercard. L'essor des grands *schemes* de carte est progressif. À l'époque, le système de crédit repose sur l'envoi de copie carbone et leur transcription manuelle, lourde à gérer tant pour les commerçants que pour les banques. Du fait de ces difficultés opérationnelles, peu de données transactionnelles sont conservées par les entreprises de cartes de crédit sur leurs clients. Ce n'est qu'à partir des années 1970, avec l'essor de l'informatique et sous la contrainte des évolutions règlementaires (visant à davantage de transparence), que sont constituées les premières bases de données conservant un historique standardisé des transactions pour chaque individu listant la date, le montant, le lieu et une brève description de chacune. Ces données sont encore peu nombreuses et peu profondes, compte tenu de l'état des technologies.

Maîtrisant l'ensemble de son infrastructure (au contraire de Visa et Mastercard qui sont adossés à un réseau de banques), American Express est un des premiers industriels à accumuler ces données transactionnelles et à les transformer en base de données marketing. Les clients d'American Express sont segmentés et les listes vendues à des entreprises pour qu'elles proposent des publicités ciblées aux clients d'American Express. Pour les compagnies aériennes, hôtels, fabricants automobiles et autres commerçants, ces partenariats donnent accès à de précieuses données sur les transactions réalisées par leurs clients. C'est également ainsi qu'il faut comprendre la volonté actuelle d'American Express d'intégrer les tickets de caisse parmi ses données de paiement[37].

La croissance rapide des cartes de crédit universelles Visa, Mastercard et American Express place les commerçants en situation de perdre l'exclusivité des informations qu'ils détenaient sur leurs clients. Au travers de leurs cartes de fidélité et de leurs propres cartes de crédit, ils avaient pu constituer progressivement des bases de données leur permettant de mieux connaître les comportements d'achat de leurs clients, en associant les achats à un client dans toutes les enseignes de la marque. Les cartes de fidélité rendent possible la récolte d'informations telles que l'identité du consommateur, la date et l'heure de la transaction ainsi que les produits achetés. Les grands réseaux de cartes bancaires actuels prennent au contraire appui sur les acteurs bancaires et la confiance qu'ils suscitent, réservant de ce fait l'accès aux données de paiement aux banques tout en les réutilisant pour leur propre compte afin de développer des services de lutte anti-fraude par exemple. C'est aussi le cas en France avec le groupement d'intérêt économique « Cartes bancaires », réseau national créé en 1984, contrôlé par les banques françaises et qui centralise les données de la très grande majorité des transactions, mais adossé aux grands réseaux globaux notamment pour les paiements internationaux.

Retenons de cet historique, à l'heure où les systèmes de paiement sont révolutionnés par le commerce en ligne, que les données de paiement et la connaissance client sous-jacente font l'objet d'une rivalité entre banques et commerçants, par prestataires interposés, dont l'issue résulte de l'état des techniques et de la configuration des acteurs et peut se traduire par une exploitation intense.

37 - « *Digital Receipts feature from American Express helps Card Members identify, and remember, purchases and helps merchants reduce disputes* » [en anglais], 18 février 2021, americanexpress.com

LA CARTE ET LE MODÈLE « 4 COINS », UN MODÈLE SÉCURISÉ MAIS COMPLEXE

Aujourd'hui, le parcours des données de paiement dans le cas le plus fréquent en France, celui d'une transaction par carte bancaire, est à la fois complexe et stabilisé. Il met en jeu un traditionnel modèle « 4 coins » (payeur-banque du payeur-banque du bénéficiaire-bénéficiaire), valable en point de vente physique comme à distance :

- **Du côté du client porteur,** une carte comportant un identifiant pseudonyme appelé PAN ou Primary Account Number, le numéro figurant sur la carte bancaire, permettant avec ou sans code PIN de l'authentifier auprès du compte de sa banque dite « banque émetteur », celle qui dénoue finalement le paiement.

- **Du côté du commerçant,** équipé d'un terminal de paiement électronique (TPE) en point de vente ou d'une fonction paiement en ligne (par SDK ou prestataire externe), les données alimentent un double circuit : un « rail » monétique d'une part, permettant à la banque du commerçant ou « banque acquéreur » de demander une autorisation de prélèvement à la banque émetteur sur le compte du client authentifié par son PAN puis de recevoir l'autorisation correspondante ; et un circuit caisse permettant une traçabilité locale des transactions, avec des données plus riches (email, données d'achats…) et des interconnexions possibles avec des services tiers (fidélité, facturation, réservation…).

Dans ce modèle complexe la qualité des règles suivies par les données de paiement est cruciale, tant pour la sécurité des opérations (protection des identifiants) que pour le contrôle de ses données par le client. Si la circulation des identifiants sur les flèches en vert sur la figure 6 est chiffrée et normée par les grands *schemes* internationaux (normes EMV, normes PCI-DSS etc.), ces règles ne sont pas obligatoires et la bonne protection du circuit caisse dépend du comportement du commerçant et de la qualité des logiciels de caisse.

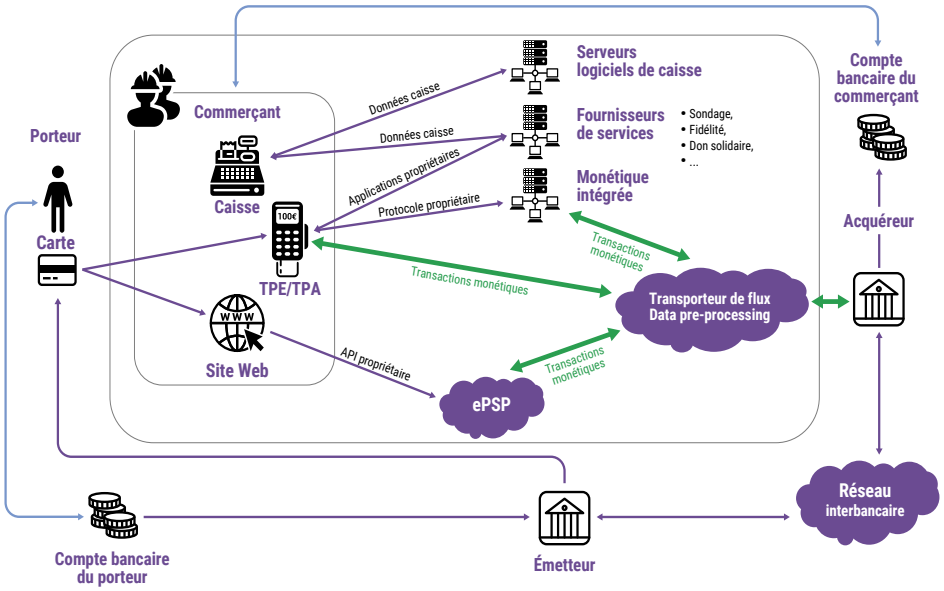
Du point de vue de la sécurité et de la circulation des données, le modèle « 4 coins » fonctionne de manière dégradée pour une transaction à distance, qui comme l'indique le schéma ne passe pas dans les premières étapes de la transaction par les infrastructures très sécurisées des *schemes* internationaux.

En outre, la distinction y est moins claire entre les données de paiement proprement dites et les données accessoires utilisées pour le e-PSP ou le site lui-même à des fins de lutte anti-fraude, de connaissance client, de publicité ciblée… sans que la personne concernée ait conscience de ces opérations et par quels prestataires elles sont réalisées.

Figure 6

La circulation des données de paiement, paiement par carte bancaire.

Source : Association du Paiement, janvier 2021



LES SERVICES DE PAIEMENT, UN MARCHÉ BIFACE

Le modèle à quatre coins illustre également la nature particulière des services de paiement, prototype de marché biface[38], dont les opérations mettent en relation deux types de clientèles différentes : les consommateurs finaux d'une part et les commerçants d'autre part. Ces opérations supposent l'existence d'un ou plusieurs intermédiaires (réseau de carte bancaire, PSP…) avec d'un côté du marché, l'émission de l'instrument de paiement et de l'autre côté, l'acquisition de la transaction.

Chaque acteur sur ce marché a la possibilité d'équilibrer son modèle économique, en faisant varier le prix au consommateur (par exemple en facturant la délivrance de la carte de paiement, ou le dépôt de chèques) ou en utilisant une commission prélevée au commerçant, selon la disposition à payer de l'une ou l'autre clientèle. Ce type de marché se caractérise aussi par des effets de réseau croisés : comme l'illustre le cas de la carte, un moyen de paiement est d'autant plus plébiscité par les consommateurs qu'il est souvent accepté par les commerçants, et réciproquement.

Cette nature de marché s'est abondamment développée dans le domaine du numérique, où les moteurs de recherche ou les réseaux sociaux proposent leurs services gratuitement aux consommateurs et facturent la publicité aux annonceurs. De même, dans le domaine des paiements, American Express a fait le choix de proposer des conditions très avantageuses aux consommateurs (allant jusqu'à lui offrir une forme de rémunération sous forme de « *miles* ») mais impose un taux de commission élevé aux commerçants.

À l'image des acteurs numériques et comme présenté ci-dessus, l'exploitation des informations liées aux paiements est également un des facteurs du modèle économique de ces intermédiaires, qui peut venir apporter de nouvelles sources de revenus sous forme de ciblage marketing ou de services de lutte contre la fraude. Sur ce dernier point, la Banque de France elle-même insiste sur la nécessaire conformité au RGPD de ces traitements impliquant une collecte croissante[39].

Du point de vue de la protection des données, la nature biface de ce marché place les acteurs du paiement en situation, du moins en théorie, de pouvoir collecter des données personnelles des deux côtés du marché (bancaires d'un côté, d'achat ou contextuelles de l'autre) pour, le cas échéant, les enrichir, les combiner et les réutiliser pour diversifier leurs revenus. Ce type d'acteur est incité à collecter plus de données que le consommateur ne l'aurait spontanément souhaité[40].

C'est pourquoi, comme l'illustre la suite de ce Livre blanc, il existe une tendance naturelle, sur le marché des paiements, à une collecte de données « enrichies » pour « créer de nouveaux services » et de même, ce marché a tendance à attirer les acteurs dont les modèles d'affaires reposent sur la combinaison et la réutilisation des données. Toutefois, en raison de la force des effets de réseaux, les évolutions du marché des paiements sont lentes et les nouveaux risques (à la fois concurrentiels et de protection des données) ne se déploient que progressivement[41].

38 - ROCHET J.C., TIROLE J., « *Platform Competition in Two-Sided Markets* », *Journal of the European Economic Association*, juin 2003, academic.oup.com.
39 - Banque de France, « Paiements et infrastructures de marché à l'ère digitale », 2018, page 49, banque-france.fr.
40 - KIRPALANI R., PHILIPPON T., « *Data Sharing and Market Power with Two-Sided Platforms* » [en anglais], NBER Working Paper n°28023, décembre 2020.
41 - LI B.G., MCANDREWS J., WANG Z., « Two-sided Market, R&D and Payments System Evolution » [en anglais], Journal of Monetary Economics Volume 115, November 2020, Pages 180-199.
42 - « Enquête sectorielle « FinTech » : l'Autorité de la concurrence rend son avis », 29 avril 2021, autoritedelaconcurrence.fr

ZOOM SUR...

L'enquête sectorielle de l'Autorité de la concurrence sur les Fintechs (avril 2021)

L'Autorité de la concurrence s'est saisie d'office pour avis, début 2020, de la situation concurrentielle dans le secteur des nouvelles technologies appliquées aux activités financières et plus particulièrement, aux activités de paiement. Au-delà de ce regard porté sur le secteur d'un point de vue concurrentiel, son avis[42], auquel la CNIL a contribué, met en lumière le rôle important que peuvent jouer les données personnelles (et leur régulation) dans l'articulation des modèles d'affaires en matière de paiement.

L'avis distingue trois familles d'acteurs aux stratégies différentes. Les groupes bancaires traditionnels, d'une part, s'adaptent aux évolutions de l'offre et de la demande en investissant dans les Fintechs pour créer des synergies ou conquérir de nouveaux marchés, en nouant des accords de partenariat avec les grands acteurs du numérique et en continuant d'investir dans l'expérience client et des services facilement utilisables. Les Fintechs, aux profils et modèles économiques très variés (jeunes pousses, banques en ligne voire grands détaillants) renouvellent l'offre et s'appuient de plus en plus sur les banques pour bénéficier de leur capital de confiance en matière de vie privée, de leurs canaux de distribution, de leur connaissance des clients ou de leur fonction conformité. Les grands acteurs du numérique, enfin, s'appuient sur leur large communauté d'utilisateurs et surtout, ont accès à d'importants volumes de données qu'ils peuvent exploiter avec leur maîtrise des technologies de traitement de données et de l'intelligence artificielle. Leurs coûts marginaux sont plus faibles que ceux des banques et ils bénéficient d'autres sources de revenus qui leur permettent de proposer des services présentés comme gratuits à leurs utilisateurs et privilégient l'ergonomie de leurs solutions. L'avis met ainsi l'accent sur ces avantages concurrentiels absolument considérables.

L'Autorité de la concurrence relève ensuite des points de vigilance, dont certains sont particulièrement intéressants du point de vue du dialogue entre régulateurs. D'abord, elle note que le paiement a tendance à disparaître en tant que service autonome, rendant la définition du marché pertinent plus malaisé. Ensuite, elle relève le sujet d'un accès plus concurrentiel à la puce NFC des ordiphones pour le développement du paiement mobile, qui révèle un arbitrage entre sécurité et innovation. Enfin, elle revient sur l'avantage concurrentiel conféré aux grands services numériques, du moins certains d'entre eux, par la combinaison et la réutilisation des données de paiement (voir page 20) dans d'autres lignes de métier, et les effets de verrouillage des consommateurs dans un écosystème donné que peut comporter le déploiement de ces solutions.
« Les données de paiement pourraient, combinées aux données collectées dans le cadre de leurs autres activités, donner à ces acteurs une connaissance du marché inégalable et, partant, un avantage concurrentiel incomparable et très difficilement réplicable par un concurrent. (...) Par exemple, dans le cadre d'une opération de concentration, eu égard aux limites posées par le Règlement européen sur la protection des données, la faculté, pour les entreprises concernées, de combiner différents ensembles de données auparavant détenus de manière séparée, pose question » (p. 110 de l'avis).

LA PLACE CENTRALE DES ENTITÉS BANCAIRES : L'ARGUMENT DE LA CONFIANCE

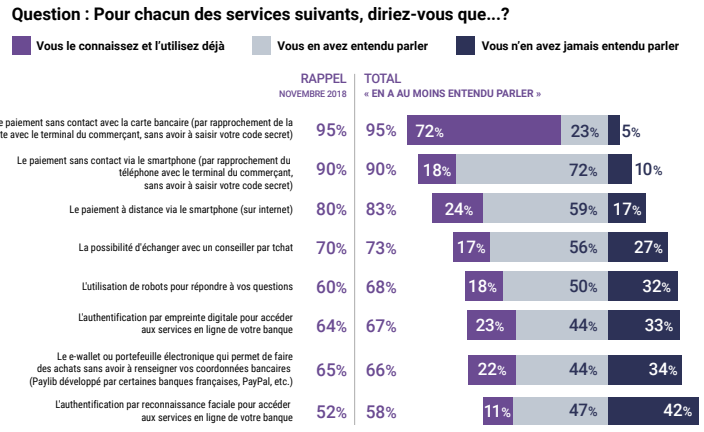
Avant la révolution des paiements à laquelle nous assistons, le couple banque – réseau de carte bancaire était au centre du jeu, et le reste à bien des égards aujourd'hui. Ce sont les banques commerciales qui, aujourd'hui, gèrent le risque et assurent l'interface entre et avec les consommateurs, avec un bon niveau de confiance de ces derniers.

Selon une enquête réalisée par l'Ifop pour la Fédération bancaire française[43], les banques inspirent confiance à 60 % des répondants (35 % d'opinions dans l'autre sens), intègrent de plus en plus les nouvelles technologies pour 85 % des répondants (10 % sont d'une opinion contraire), même si 34 % des répondants affirment n'avoir pas téléchargé d'application de banque en ligne (notamment les plus de 50 ans et les retraités). De fait, 70 % des répondants font confiance aux banques pour sécuriser leurs données personnelles, contre 35 % aux GAFA par exemple. Au sein des services bancaires, les innovations concernant les moyens de paiement sont parmi les plus connues et utilisées, en particulier le paiement sans contact, le paiement par smartphone et même les autres formes de portefeuille numérique utilisées par 22 % des répondants. Même si l'attente des répondants est située plutôt au niveau de la sécurité que de l'innovation, le paiement s'avère ainsi une stratégie innovante pertinente (et source de diversification des revenus) pour les banques.

Figure 7

Les nouveaux moyens de paiement sont les services bancaires les mieux connus des Français.

Source : Ifop/FBF, février 2021



Mais le modèle d'affaires bancaire est lui-même en évolution du fait de la dématérialisation des services, désormais intégrée. Selon l'enquête du cabinet Deloitte sur « Les Français et les nouveaux services financiers », au début de 2020, 10 % des Français se déclarent clients d'une banque mobile (par exemple Ma French Bank, Orange Bank, Revolut ou N26), et 64 % d'entre eux l'utilisent comme compte principal (+16 points en un an). Les banques traditionnelles restent pour l'instant privilégiées pour les opérations de banque classiques telles que la demande d'un crédit, mais la banque en ligne apparaît pour les opérations simples telles que le paiement comme un bon compromis en termes d'image et de confiance, alors que la confiance dans les nouveaux acteurs est moindre. Dans ce contexte, les stratégies de « plateformisation » choisies par certaines banques en ligne, accueillant au sein de leur système de nouveaux services développées par des nouveaux acteurs indépendants, en profitant du caractère « nativement digital » de leurs systèmes d'information, apparaît comme une alternative crédible au modèle bancaire traditionnel. Ainsi la banque peut donner accès sur ses systèmes à des services proposés par des acteurs tiers comme : vérification d'identité, recherche immobilière, prêts de pair à pair, etc. Selon l'ACPR, « le rôle des banques en ligne et des néobanques dans la course à l'innovation mérite d'être souligné. Dans le domaine du mobile ou de l'usage innovant des données à des fins de marketing, ces nouveaux acteurs se montrent particulièrement actifs. (…) Lorsqu'ils appartiennent à des groupes bancaires déjà établis, ils peuvent ainsi jouer en leur sein le rôle de laboratoire d'innovation et d'expérimentation. Dans tous les cas, ils se sont imposés comme des acteurs essentiels des transformations à venir de la banque de détail »[44]. Gageons que cette transformation des métiers bancaires ne leur fera pas perdre leur acquis de conformité en matière de protection des données.

43 - Les Français, leur banque, leurs attentes, étude n°2, février 2021, fbf.fr.
44 - *Étude sur les modèles d'affaires des banques en ligne et des néobanques* (PDF, 723 ko), coll. Analyses et Synthèses, octobre 2018, acpr.banque-france.fr.

LA VAGUE DES FINTECHS : DE NOUVELLES ATTENTES DU CLIENT, DE NOUVEAUX USAGES

Ce que nous appelons aujourd'hui les « Fintechs », contraction de « finance » et de « technologie », naît dans les pays anglo-saxons à la suite de la crise financière de 2008. L'innovation s'est alors déplacée vers des acteurs de type jeunes pousses, proposant de nouveaux services dans des conditions de fluidité et d'expérience consommateur privilégiées, alors que naissait parallèlement au développement de la banque en ligne le principe de l'« *open banking* ».

Alors que les nouvelles Fintechs n'avaient d'autre choix que d'utiliser les identifiants bancaires de leurs clients, dans des conditions de sécurité discutables, il a paru préférable de standardiser leurs accès aux comptes bancaires en contrepartie d'une obligation d'ouverture pour les banques. Les Fintechs sont présentes dans plusieurs types de services financiers mais dans le domaine des paiements, elles sont présentes via deux grandes familles, les initiateurs de paiement, à l'image de l'allemand Sofort, qui avait besoin de la visibilité sur le solde du compte bancaire pour lancer une opération de paiement, et les agrégateurs de compte, à l'image des français Bankin, Budget Insight ou encore Linxo, qui délivrent une information consolidée sur l'ensemble des comptes bancaires d'un client. Ce mouvement a conduit à l'adoption de la seconde directive européenne sur les services de paiement, en 2015.

> ***« Les Fintechs imposent de nouveaux standards bancaires en offrant à leurs clients des solutions alternatives moins coûteuses et plus personnalisées »***

La mise en place de la DSP2 a eu plusieurs conséquences importantes en matière de données de paiement :

- **elle a renforcé la règle prévue par le RGPD** selon laquelle le client et non la banque ou le PSP est souverain sur l'usage qui est fait de ses données ;
- **elle a élargi considérablement le champ des données de paiement** sans en donner de définition précise tout en permettant des usages annexes aux services de paiement, eux-mêmes non définis ;
- **elle a créé sur le marché un standard de sécurité** avec l'authentification forte et les API, dont pourront demain s'inspirer d'autres services et usages utilisant cette disposition des individus à s'authentifier.

Du point de vue économique, le danger majeur de l'*« open banking »* pour les banques est notamment celui d'être intermédiées et de perdre la maîtrise de la relation client. Elles pourraient risquer d'être cantonnées à un rôle de gestionnaire à faible valeur ajoutée. Mais en réalité, les relations entre banques et Fintechs relèvent plutôt de la symbiose. Pour rester dans la course, les banques doivent s'adapter et tout miser sur l'expérience client et l'accompagnement, quitte à absorber certaines Fintechs pour profiter de leur expérience ou de leur service. Certaines Fintechs proposent également des services à destination des banques pour les accompagner dans leur processus de transformation numérique.

Grâce à ces nouveaux acteurs, enfin, on assiste au développement de services complémentaires aux moyens de paiement à destination des clients (cartes de fidélité, tickets dématérialisés, services de banque mobile) ou des professionnels (gestion de la fraude, analyse des données clients, gestion des programmes de fidélité), en complément du « paiement nu » qui n'est plus considéré aujourd'hui comme un modèle d'affaires attractif. Autre exemple, le développement du paiement dit « fractionné » ou en plusieurs fois, à la frontière du paiement et du crédit : il suppose une évaluation par la Fintech du risque de crédit, avec d'importants traitements de données. Ainsi, les moyens de paiement électroniques sont souvent un point d'entrée pour repenser la connaissance et la relation avec les clients. Mais ces acteurs ne sont pas non plus exempts de risques financiers, comme l'illustre le scandale Wirecard[45] en Allemagne l'an

45 - Ce prestataire de services d'acquisition de paiement opérant sous agrément bancaire et coté à la Bourse de Francfort était spécialisé dans le traitement des paiements en ligne. Il a fait faillite en 2020 après la découverte d'opérations fictives dans des pays émergents ou en développement, maquillés dans ses comptes.

dernier, illustrant un biais trop favorable des investisseurs par rapport aux paiements en ligne.

Au final, la mise en œuvre opérationnelle de la directive DSP2 ne devrait pas se traduire par une disruption des banques par les acteurs Fintechs. Ces derniers ont en effet besoin de la collaboration des banques pour offrir à leurs clients une expérience de qualité (comme l'illustre la mise en place délicate des interfaces d'échange de données ou API, alors que l'Autorité bancaire européenne a récemment appelé les superviseurs nationaux à faire lever les entraves en la matière) et la tendance est plutôt au rachat des Fintechs par les groupes bancaires.
Du point de vue de la conformité, ces évolutions ne constituent sans doute pas une fragilisation, même si d'autres déterminants que le simple succès commercial interviennent dès lors dans les modèles d'affaires. On se souvient peut-être du succès rapide sur le marché britannique de la jeune pousse Pingit, lancé par Barclay's en 2012, mais dont le déploiement a été ensuite entravé par des conflits internes au sein du groupe. Ces évolutions ne sont de toute façon pas terminées, puisque la Commission européenne doit lancer fin 2021 le processus de revue de la directive DSP2.

Enfin, la question de la confiance est cruciale pour ces acteurs. Selon l'étude de Deloitte sur « Les Français et les nouveaux services financiers », déjà citée, bien que les Fintechs soient vues comme des produits d'avenir, une perception assez marquée des risques associés aux Fintechs par le public persiste même si les services proposés par ces dernières sont de mieux en mieux connus. Seuls 40 % des répondants accepteraient de leur confier davantage de données personnelles, par exemple, témoignant d'un important enjeu d'accompagnement par la CNIL en la matière.

ZOOM SUR...

La portabilité des données de paiement

La question de la portabilité (partage de ses données à la demande d'une personne) des données de paiement n'est pas simple car elle est à la frontière de deux réglementations, l'une sectorielle (la DSP2) et l'autre générale (le RGPD). Le Comité européen de la protection des données a publié le 15 décembre 2020 des lignes directrices pour éclairer l'articulation entre ces deux textes[46]. Ces lignes directrices rappellent la distinction entre l'accord contractuel au sens de la DSP2 et le consentement au sens du RGPD. Elles précisent que les données de paiement dans le champ de la DSP2 ne peuvent être réutilisées qu'avec le consentement du client. Enfin, elles expliquent qu'il n'appartient pas aux banques d'apprécier le caractère proportionné de la collecte de données par les agrégateurs, ces derniers étant pleinement responsables de la conformité de leurs traitements.

En outre, la CNIL a récemment publié une recommandation sur l'exercice des droits des personnes par l'intermédiaire d'un mandataire[47]. Cette recommandation précise qu'un agrégateur autorisé par l'ACPR est tenu, dans le champ de la DPS2, de respecter les modalités d'accès et de transmission prévues par cette directive, et ne peut exercer à cette fin les droits prévus par le RGPD, tels que le droit à la portabilité ou le droit d'accès, en qualité de mandataire auprès du prestataire gestionnaire du compte. Il est en revanche possible pour un mandataire, même lorsque ce dernier est par ailleurs prestataire de service d'information sur les comptes, d'exercer les droits d'accès et de portabilité prévus par le RGPD, en qualité de mandataire, auprès d'un prestataire gestionnaire de compte, si la DSP2 n'a pas vocation à s'appliquer à cette opération. C'est par exemple le cas, si l'accès aux données est réalisé dans le cadre de la fourniture d'un service non soumis à la DSP2, ou si les données accédées ne proviennent pas d'un compte de paiement au sens de la DSP2.

Dans ce dernier cas de figure, la CNIL a retenu une approche favorable à l'innovation. Elle recommande que les données puissent être portées à intervalles réguliers si telle elle est la demande du client, sans qu'une telle demande soit regardée comme abusive dès lors que les données se renouvellent rapidement. Dans le cas d'une demande directe de portabilité d'un responsable de traitement vers un autre, elle recommande d'utiliser les possibilités techniques existantes des API déjà développées pour les besoins de la mise en œuvre de la DSP2, de préférence à l'extraction de contenus via les identifiants du client. La recommandation suggère des garanties pour authentifier et sécuriser ces opérations.

46 - *Adopted guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR* [en anglais] (PDF, 308 ko), edpb.europa.eu
47 - « Exercice des droits par un mandat : la CNIL publie sa recommandation », 25 juin 2021, cnil.fr.

La parole à...

BERTRAND PEYRET

SECRÉTAIRE GÉNÉRAL ADJOINT DE L'ACPR

Bertrand PEYRET *est Secrétaire général adjoint de l'Autorité de contrôle prudentiel et de résolution (ACPR), en charge plus particulièrement de la supervision bancaire et des autorisations. Auparavant, il a exercé les fonctions d'Inspecteur de la Banque de France puis de Directeur du contrôle des banques et enfin de Directeur du contrôle des assurances à l'ACPR. Il a été membre du groupe des superviseurs de haut niveau, présidé le groupe HubGovernance (initiative sur les insuffisances en matière de données) et participé à différents sous-groupes du Conseil de stabilité financière.*

> ***Il est important que des autorités comme l'ACPR et la CNIL soient vigilantes et collaborent pour s'assurer du respect des réglementations***

Qu'est-ce que le partage des données dans le secteur financier ?

Aujourd'hui, il s'agit principalement de la possibilité de partager des données de paiement (opérations de paiement, solde des comptes, bénéficiaires enregistrés, etc.). Depuis une dizaine d'années, des services nouveaux ont émergé, fournis par de nouveaux acteurs, souvent des Fintechs. Ils reposent sur l'accès et l'utilisation de ces données de paiement. Depuis 2018 et la transposition de la deuxième directive sur les services de paiement (DSP2), une réglementation encadre ces activités en définissant deux nouveaux services : le service d'initiation de paiement, qui permet par exemple d'effectuer pour le compte du client un virement au profit d'un commerçant en ligne, ou le service d'information sur les comptes qui consiste entre autres à collecter les données d'un ou de plusieurs comptes de paiement.

Comment s'effectue ce partage ?

La réglementation prévoit que les prestataires de services de paiement qui gèrent des comptes de paiement accessibles en ligne doivent mettre à disposition des prestataires agréés pour fournir les nouveaux services d'initiation de paiement ou d'information sur les comptes, une interface d'accès conforme aux exigences de la DSP2. Cette interface, que l'on appelle souvent « API DSP2 », permet de collecter des données ou de transmettre des ordres de paiement, dans le respect du mandat confié par le client et dans des conditions techniques destinées à assurer la sécurité et la qualité du service.

Voit-on apparaître des nouveaux cas d'usage ?

Tout à fait. À l'origine le service d'information sur les comptes était pensé pour permettre à un utilisateur d'avoir une vue unique de l'ensemble de ses comptes de paiement gérés par plusieurs prestataires de services de paiement. Aujourd'hui, cette vision est dépassée : les prestataires de services d'information sur les comptes proposent de nombreux services qui vont plus loin et permettent, par exemple, une gestion plus active d'un patrimoine en proposant des possibilités d'investissement ou facilitent l'obtention d'un crédit.

Les banques traditionnelles fournissent-elles aussi ces services ?

Historiquement, les banques se sont relativement peu investies dans ces services d'information sur les comptes ou d'initiation de paiement. L'utilisation des données des clients s'est surtout limitée à leur utilisation pour répondre aux obligations légales : lutte contre la fraude ou lutte contre le blanchiment des capitaux et le financement du terrorisme.
Mais la situation est en train de changer. L'intérêt des banques dans ce domaine est de plus en plus marqué : cela se concrétise par leur entrée dans le capital de Fintechs et par la fourniture directe de services aux clients relatifs à la gestion de leurs données de paiement.

Les BigTechs fournissent-ils des services basés sur l'utilisation des données financières ?

Les GAFA[48] et les BATX[49] sont de plus en plus actifs sur le marché européen des paiements. Jusqu'à présent, ces acteurs ont surtout investi le segment des solutions de paiement – c'est-à-dire les applications faisant l'interface entre un utilisateur et sa banque pour initier des opérations de paiement. Ces solutions reposent généralement sur l'utilisation des données des cartes de paiement émises par les établissements bancaires des utilisateurs, à l'image d'Apple Pay ou de Google Pay. Dans ce cas, l'intérêt pour les Bigtechs se situe en grande partie dans le recueil des données des utilisateurs, qui leur permettent de développer leurs activités historiques comme le ciblage publicitaire ou la vente de leurs produits. Néanmoins, on voit aussi apparaître des activités de place de marché dans lesquelles ces Bigtechs peuvent entrer en possession des fonds des utilisateurs, ce qui nécessite l'obtention d'un agrément de prestataire de services de paiement.
Ces activités ainsi que le poids économique des Bigtechs, qui leur permet de développer et de déployer à grande échelle ces nouvelles technologies de paiement, justifient la vigilance des autorités de régulation du secteur financier. Il ne doit pas y avoir de différence de traitement, en termes de contrôle, entre ces acteurs et les Fintechs ou les banques.

Est-ce que toutes les données peuvent être partagées ?

Non, pas complètement. Déjà il faut rappeler que les prestataires de services d'information sur les comptes ou d'initiation de paiement ne peuvent accéder qu'aux comptes et aux informations convenus avec leurs clients. Ensuite, la DSP2 ne traite que des données des comptes de paiement accessibles en ligne. L'accès aux informations relatives aux contrats d'assurance ou aux comptes d'épargne ou de titres n'est par exemple pas couvert par la DSP2.

Va-t-on vers une accélération du partage des données financières et l'open finance ?

Dans le plan d'action pour la finance digitale de la commission européenne, rendu public le 24 septembre 2020, un des axes consiste à promouvoir l'innovation en établissant un espace commun des données financières. L'enjeu est aussi bien de faciliter l'accès à ces données en les standardisant et en prévoyant un format d'échange électronique, que de promouvoir les solutions innovantes facilitant les reporting réglementaires, et enfin de renforcer l'open finance.

Beaucoup d'utilisateurs apprécient de pouvoir bénéficier de services innovants et sur mesure améliorant par exemple la gestion de leur patrimoine ou facilitant l'accès à d'autres services. Toutefois, à partir du moment où ces services reposent sur l'utilisation de données financières et non financières, cela justifie que des autorités comme l'ACPR et la CNIL soient vigilantes et collaborent pour s'assurer du respect des réglementations applicables dans ce domaine.

Quelles sont les autres utilisations potentielles de ces technologies ?

Les possibilités qu'offre le traitement d'information de masse via les technologies d'intelligence artificielle et de big data sont déjà en partie exploitées par les établissements assujettis aux contrôles de l'ACPR. L'utilisation de ces informations peut permettre de réduire le risque dans le cadre d'octroi de crédit mais elles peuvent aussi être utilisées pour traiter plus rapidement des demandes d'indemnisation par des assureurs.

De plus, dans certains domaines comme la lutte contre la fraude ou le blanchiment des capitaux, l'utilisation de solutions innovantes fondées sur de tels outils pourraient permettre d'identifier plus rapidement et plus sûrement les situations à risque. Dans ce domaine également l'adoption de mesures au niveau européen pour faciliter l'échange de données entre établissements, tout en respectant les obligations notamment liées au secret professionnel et à la protection de la vie privée est souhaitable.

48 - Acteurs américains : Google, Amazon, Facebook, Apple
49 - Acteurs chinois : Baidu, Alibaba, Tencent, Xiaomi

LE PAIEMENT, « CHEVAL DE TROIE » DES GRANDS ACTEURS DU NUMÉRIQUE ?

Cette vague d'innovation dans les paiements s'accompagne également de l'arrivée des grands acteurs de l'économie numérique dans le secteur. Si leur point d'entrée est aujourd'hui le paiement et notamment le paiement mobile (Google, Samsung Pay, Apple Pay), à plus long terme, leur souhait est de proposer d'autres services financiers.

Les systèmes de paiement sur mobile (solutions dites X-pay) se développent sur la base de l'infrastructure de la carte bancaire, qui reste omniprésente dans ce système. Les *wallets* (Apple Pay, Google Pay) s'appuient sur la carte bancaire. Celle-ci est enregistrée dans le téléphone, et, l'application de paiement est utilisée pour régler les achats au lieu de la carte bancaire physique. La suite du traitement du flux financier est identique à celui de la carte bancaire. Cette stratégie a permis l'association aisée des banques, puisqu'aucun acteur n'est a priori concurrencé dans ce schéma, même si les partenariats signés avec Apple sont coûteux pour les banques qui perdent une partie de la commission prélevée chez le commerçant, mais qui font le pari que ce modèle va se développer.

Deux stratégies différentes sont à distinguer toutefois entre les fabricants de téléphones (Samsung, Apple) et les fournisseurs de services (Google). Le modèle économique des premiers repose sur une commission prise sur chaque transaction (d'un montant variable selon les accords négociés entre les banques et Apple ou Samsung), ainsi que sur l'augmentation des ventes de téléphones grâce à l'enrichissement des fonctionnalités.

À l'inverse, le modèle des seconds repose sur la collecte et la valorisation de données en contrepartie d'un service gratuit. Par ces services de paiement, ils cherchent à occuper une place stratégique au cœur de la chaîne des données de paiement et ainsi à enrichir leur capital en données sur chaque individu. Ce dernier modèle, que les banques déploient moins volontiers, nécessite une plus grande vigilance des individus, l'utilisation des données allant au-delà des usages sécuritaires.

Amazon poursuit une stratégie de plateforme similaire à celle d'Alipay (voir page suivante). Le bouton Amazon Pay est mis à disposition de tout site commerçant classique, ce qui lui permet de se positionner comme un acteur central au-delà de la place de marché de sa plateforme (le client utilisant alors son compte Amazon pour payer en s'y connectant à partir de son terminal). L'entreprise commercialise également (hors de l'UE) sa technologie de paiement instantané JustWalkOut mise en œuvre dans ses magasins physiques, qui permet au client d'être débité de ses achats sans avoir besoin de passer en caisse. Pour Amazon, l'enjeu est la prédiction de l'acte d'achat via l'observation de l'historique et des données contextuelles, le ciblage des recommandations, les données de paiement étant la résultante du modèle d'affaires.

Que le paiement soit source de rentabilité ou d'enrichissement des données, il permet surtout aux grands acteurs du numérique d'entrer sur le marché des services financiers en général, en s'associant à des acteurs historiques pour des raisons réglementaires. Les Amazon, Apple et Google se sont ainsi associés respectivement à JP Morgan, Goldman Sachs et Citigroup pour lancer des cartes de crédit et envisager la création de comptes courants.

Le développement d'autres opérations de banque constitue une opportunité pour collecter des informations complémentaires sur les individus, à partir desquelles ces entreprises seront demain en capacité de calculer des scores de risque et proposer des produits plus complexes tels que des crédits. Elles visent en particulier les exclus du système bancaire, dans un contexte où les banques accordent plus difficilement des crédits depuis la crise de 2008, ce qui soulève des enjeux éthiques et juridiques. Amazon propose déjà des services financiers à destination des commerçants de sa plateforme, tout comme Stripe et Paypal qui proposent des prêts aux petits commerçants.

Il convient de souligner que ces stratégies imaginées et développées aux États-Unis ne sont pas toujours transposables en raison des obligations en vigueur en Europe, et notamment de ce qu'il serait possible de faire en restant conforme au RGPD. Ces stratégies restent encore à consolider sur le marché européen, mais elles obligent d'ores et déjà les acteurs traditionnels à réagir. De l'avis du cabinet d'études Xerfi, avec l'enquête lancée par la Commission européenne à l'été 2020 contre Apple qui restreint l'accès à la puce NFC des téléphones de la marque à la seule

solution Apple Pay, seul le modèle d'Amazon est une réelle menace pour les acteurs du paiement en place[50], avec 30 millions d'utilisateurs en France et le déploiement de l'assistant vocal Alexa[51]. La solution Amazon Pay s'intermédie en complément des PSP traditionnels : Amazon Pay qui dispose déjà des données pertinentes opère le paiement et propose au commerçant un reporting des transactions et le PSP joue le rôle de simple passerelle avec le site du marchand. Bien entendu, l'analyse relatée ici sur le marché des paiements n'est pas nécessairement transposable aux autres services financiers (assurance, crédit).

ZOOM SUR...
Les acteurs chinois

Sous d'autres longitudes, l'exemple de l'entreprise chinoise Alibaba témoigne également de ces recompositions. Son service de paiement Alipay est utilisé par plus d'un milliard d'utilisateurs (dont deux à cinq millions d'utilisateurs en France). Il propose une solution de paiement mobile, de virements, de services fiduciaires et des services aux particuliers (réservation de billets d'avion, gestion de fortune, livraison des commandes, etc.). Surtout, le système est complètement intégré à la plateforme de e-commerce. Alibaba peut ainsi avoir une connaissance intégrale des transactions effectuées par chaque commerçant et chaque client.

Selon Hubert Testard, ancien chef du service économique régional de Pékin, « Alibaba et Tencent ne sont pas perçus comme une menace immédiate par les acteurs européens des moyens de paiement. Leur progression en Europe sera probablement, comme aujourd'hui en Asie du Sud-Est, principalement déterminée par le rythme et l'importance des prises de participation ou des acquisitions qu'ils vont réaliser, avec le souci évident de ne pas heurter de front les régulateurs et les responsables politiques européens ». Même si Tencent est présente au capital de la française Lydia par exemple, s'adapter au RGPD est encore « un vrai challenge pour les acteurs chinois, qui sont accoutumés à un cadre réglementaire totalement différent sur leur propre marché.[52]» .

En Chine, Alibaba et Tencent sont perçus par certains analystes comme les acteurs de demain du secteur bancaire. S'ils se concentrent aujourd'hui sur les moyens de paiement, ils sont des acteurs centraux du système de *scoring* social chinois, dispositif qui pourrait être utilisé demain pour déterminer la capacité d'emprunts des individus. Leur capacité de disruption du système bancaire (via leur activité de prêts en ligne) est telle que les pouvoirs publics ont éprouvé le besoin de les reprendre en main en interrompant en novembre dernier l'introduction à la bourse de Shangaï d'Ant Group, filiale bancaire d'Alibaba, à la surprise générale.

50 - « Les offensives sur le marché du paiement », Xerfi, février 2021
51 - Voir, à ce sujet, le Livre blanc de la CNIL sur les assistants vocaux dont les recommandations valent aussi pour les données de paiement - *À votre écoute, exploration des enjeux éthiques, techniques et juridiques des assistants vocaux* (PDF, 6,4 Mo), septembre 2020,cnil.fr.
52 - « Paiements en Europe : les géants de la FinTech chinoise à l'attaque », 20 décembre 2019, asiepacifique.fr.

Figure 8

Les solutions de paiement proposées en France par les GAFA.

Source : Autorité de la concurrence

VERS LA NUMÉRISATION DU PAIEMENT : de nouveaux enjeux et des risques pour la vie privée évolutifs

LA DÉMATÉRIALISATION CROISSANTE DES PAIEMENTS, UN PHÉNOMÈNE AMPLIFIÉ PAR LA PANDÉMIE DE COVID-19

Les habitudes de paiement évoluent lentement mais ont tendance à suivre les habitudes d'achat des consommateurs, d'une part, et des considérations de facilité et de confiance, d'autre part. Le paiement, lorsqu'il implique le dévoilement de données personnelles pouvant exposer les consommateurs à un risque de fraude, constitue un moment de « friction » pendant lequel les personnes s'interrogent sur les risques, notamment financiers, encourus.

Ainsi, le développement des paiements à distance a été longtemps handicapé par les risques perçus de ces situations, qui ne sont pas sans fondement objectif (voir page 27). Mais ce qui est vrai pour les risques financiers l'est aussi pour les risques de dissémination non maîtrisée des données personnelles en général, le paiement à distance impliquant, précisément pour combattre la fraude, des vérifications supplémentaires et donc le traitement et la combinaison d'une plus grande quantité de données.

Aujourd'hui toutefois, le commerce en ligne paraît entré dans les mœurs et la crise sanitaire du COVID-19 n'a fait qu'accélérer cette tendance. Ainsi, selon le Baromètre trimestriel de l'audience du e-commerce en France Fevad -Médiamétrie (4e trimestre 2020), près de 4 cyberacheteurs sur 10 ont accru leurs achats en ligne en 2020, 85 % d'entre eux ayant déclaré dépenser plus qu'habituellement. 85 % des cyberacheteurs déclarent préférer la livraison à domicile mais le « *click and collect* » a séduit l'année dernière plus de 4 cyberacheteurs sur 10. L'achat en ligne sur mobile, un temps délaissé pendant l'année 2020, revient au niveau observé fin 2019. En outre, plus d'un quart des cyberacheteurs ont réalisé leurs achats sur le web auprès de leurs commerces de proximité.

La pandémie a ainsi sans doute contribué à estomper la frontière entre commerce physique et commerce en ligne, de manière peut-être irréversible. Ceci dit, toujours selon ce baromètre, la sécurité des données et des transactions sur un site de e-commerce reste un critère de sélection pour 68 % des adeptes des achats en ligne.

La crise sanitaire a également amplifié le recours au paiement « sans contact » via la carte bancaire avec le recours à la puce NFC (pour *near field communication*), dont les risques de détournement sont plus importants que l'authentification classique par présentation de la carte et d'un code à 4 chiffres. Ce risque a été mis en balance l'an dernier avec le risque sanitaire de composer ce code, mais aussi avec la facilité d'usage avec un plafond relevé à 50 euros à partir du 11 mai 2020, sur recommandation de l'Autorité bancaire européenne. Selon le rapport 2020 de l'Observatoire de la sécurité des moyens de paiement, déjà cité, parmi ces paiements, on a observé l'an dernier une progression marquée de la part des paiements réglés en mode sans contact qui passe de 9 % en 2019 à 19 %, en 2020, les paiements sans contact ont ainsi représenté en 2020 5,1 milliards d'opérations (soit + 37 % par rapport à 2019). Les paiements par carte en ligne ont, quant à eux, profité des effets de la crise, avec une progression de 13,2 % en nombre de transactions et de 9,3 % en valeur.

Si le risque lié au protocole NFC n'est pas nul, il peut être relativisé si l'on en croit le rapport de l'OSMP déjà cité : avec un taux de fraude de 0,013 %, en baisse en 2020 malgré l'augmentation de son utilisation, le sans contact apparaît plus proche des paiements en point de vente avec code (0,009 %) que des paiements en ligne (0,174 %), qui s'accroît en revanche légèrement en 2020.

La dématérialisation croissante des paiements entretient ainsi les stratégies de développement dit « *phygital* » des grandes enseignes, qui imaginent des parcours connectés en point de vente via une application de fidélité permettant ensuite le paiement via des coupons de réduction et demain, l'envoi des tickets de caisse de manière dématérialisée avec une expérience client la plus fluide possible. Si ces stratégies concernent plus les données d'achat que les données de paiement proprement dites, la dématérialisation a le potentiel de réduire voire de faire disparaître l'aspect « frictionnel » du paiement, déjà évoqué, ce qui limite les opportunités pour les personnes de s'interroger sur les risques que comportent ces opérations pour les données correspondantes. En outre, alors que les espèces ne sont pas utilisables pour ce type de paiement, la dématérialisation nourrit mécaniquement le recul de l'anonymat et les risques de suridentification des paiements, du moins tant que la banque centrale n'émet pas elle-même une monnaie numérique (voir page 45).

LA NUMÉRISATION DES PAIEMENTS : NOUVEAUX ENJEUX ET NOUVEAUX RISQUES

Corollaire du développement du e-commerce, les paiements en ligne ont suscité l'essor très rapide d'acteurs e-PSP aux offres compétitives, comme l'américain Stripe (créé en 2006) ou le néerlandais Adyen (créé en 2011, dont la capitalisation boursière talonne celle de la BNP), devenus en quelques années des acteurs de premier ordre dans le paiement sur internet.

Le développement du paiement électronique, outre des économies d'échelles impossibles à réaliser avec le commerce physique, offre également une opportunité de connaissance précise sur les habitudes des consommateurs, via l'analyse des données recueillies sur le terminal utilisé (de bureau ou mobile).

En grossissant, ces acteurs agrègent autour de leur modèle d'initial d'autres services et options, pour pouvoir proposer aux sites marchands une gamme complète de solutions à l'image du suédois Klarna, qui propose de la tokenisation[53], des *« wallets »*, des cartes prépayées et même une forme d'affacturage (à l'image du *Lastschrift* allemand). La donnée de paiement peut alors être utilisée pour de multiples usages : expérience utilisateur, score de lutte anti-fraude, facturation, score de crédit… ce qui suppose que l'utilisateur final en ait été informé et en ait pleinement conscience.

Signe de ce dynamisme des acteurs e-PSP face aux PSP de monétique physique traditionnelle, le secteur est en phase de consolidation, avec le rachat d'Ingenico par Worldline pour 7,8 milliards d'euros en 2020 par exemple. Ingenico est le leader mondial dans le marché des terminaux de paiement physiques et un acteur important du marché des paiements électroniques. Worldline est le principal prestataire de paiement sécurisé en ligne. L'objectif de ce rachat est d'avoir une taille critique nécessaire aux investissements liés aux nouvelles règlementations et de développer des services à valeur ajoutée en maîtrisant tous les outils de la chaîne du paiement. La stratégie est similaire pour leurs concurrents. Les américains FIS, et Global Payments ont en 2019 acquis respectivement le britannique Worldplay, First Data et TSYS. Ces mouvements semblent indispensables dans cette industrie, qui s'est internationalisée et où les volumes sont cruciaux.

En réponse à ces phénomènes d'intégration et afin de conserver un lien direct avec leurs clients, certains acteurs de la grande distribution proposent leurs propres services de paiement électronique. L'application de paiement de Starbucks a jusqu'en 2019 compté plus d'utilisateurs qu'Apple Pay. En France, Système U a par exemple lancé en février 2019 U Paiement, une application de portefeuille numérique, qui intègre un système de paiement par QR Code et un programme de fidélité (cagnotte, dématérialisation des tickets, envoi de promotions). Carrefour, la FNAC, Casino offrent des services similaires sur leurs applications, tandis que certaines enseignes ont mutualisé ce service en s'appuyant sur l'application Lyf Pay.

Numérisation des solutions de paiement

La sécurité de ces applications est un enjeu central. Elle n'atteint pas toujours le niveau de sécurité des banques. Starbucks App a été piraté à deux reprises, et, dans les deux cas, les pirates pouvaient accéder aux données des cartes de crédit et transférer de l'argent depuis les comptes bancaires des utilisateurs. En outre, les applications des grands détaillants ont souvent accès à un grand nombre de données sur leurs utilisateurs (transaction, appareil, localisation) qu'ils peuvent commercialiser à des tiers, comme le fait Starbucks. Dans ces deux cas se pose la question de la conformité au RGPD de ces solutions, la sécurité des données étant l'un des grands principes de la protection des données, tout comme le contrôle sur qui peut accéder ou non à quelles données, avec des enjeux liés notamment à la transparence et à l'information des individus.

Une autre caractéristique des modèles d'affaires actuels, pouvant donner lieu à une surexposition des données personnelles, est leur nature « multicanal ». Comme l'illustre l'essor des solutions *« click and collect »* ou la digitalisation de la distribution, un même bien ou service peut être commandé en ligne ou en boutique ou agence, être payé à distance ou lors du retrait. Cette interpénétration des parcours en ligne ou en point de vente, sur des architectures techniques différentes, crée de nouvelles possibilités de croisement des données de paiement avec des données de terminal ou de géolocalisation, avec des risques de réidentification et d'exploitation des données supérieurs. Dans ce contexte, la question de la réutilisation des données est centrale (voir page 60 et suivantes).

53 - Voir la définition de ce terme dans le Glossaire.

ZOOM SUR...

Le paiement crypto : « cryptomonnaies » et Libra

La première monnaie privée virtuelle utilisable à grande échelle, le Bitcoin, a été créée en 2008. Elle est émise et circule sur un registre distribué décentralisé et public fonctionnant par consensus et assurant la traçabilité des transactions, mais aussi une pseudonymisation très poussée justifiant le qualificatif de cryptomonnaie. Depuis, d'autres monnaies virtuelles ont été créées, toujours sur la base de la technologie *blockchain*, mais bénéficiant, grâce à un mécanisme de réserve, d'un change stabilisé par rapport à une des grandes monnaies souveraines, dites « stablecoins », à l'image de la plus diffusée, le Tether. L'association Libra fondée à l'initiative de Facebook a annoncé pour sa part un projet de *stable coin* fondé d'abord sur un panier de monnaies, puis devant la résistance des banques centrales et des régulateurs du monde entier, sur la parité avec le seul dollar américain et sur la base d'une *blockchain* dite à permission permettant d'exercer un contrôle sur les « nœuds » validateurs des transactions. Ce projet, appelé aujourd'hui Diem, serait finalement déployé à partir des États-Unis, sur la base d'une coopération avec une banque spécialisée dans les cryptoactifs.

Ces monnaies virtuelles sont aujourd'hui plus utilisées comme réserve de valeur (actif d'investissement alternatif) que comme moyen d'échange pouvant donner lieu à des paiements. Cette fonction de paiement se heurte en effet à d'importantes limites comme (i) le recours à une architecture totalement nouvelle, parallèle aux infrastructures de paiement existantes organisées par les banques centrales autour des règlements interbancaires (ii) l'absence de cours légal de ces monnaies privées, qui sont soit très volatiles, soit garanties par un émetteur dont le risque de contrepartie est sans commune mesure avec un émetteur étatique, rendant la confiance en cette monnaie toute relative et (iii) les importants frais de transaction : pour le Bitcoin, de l'ordre de plusieurs dollars, voire plusieurs dizaines de dollars pour Ethereum, rendant les usages en paiement de détail non rationnels.

Toutefois, la détention de plus en plus importante de ces monnaies par les agents économiques (pour l'équivalent de plusieurs centaines de Md$) pourrait rendre leur usage attractif pour les paiements. Tesla a ainsi annoncé un temps accepter les Bitcoins en paiement pour ses produits, suivi de PayPal qui va dans les mois à venir permettre les paiements en cryptomonnaies sans aucun frais. Enfin, Visa a annoncé l'intégration du stable coin USDC à son réseau.

Il est trop tôt pour prévoir la place qu'occuperont à terme ces moyens de paiement alternatifs pour des usages de paiement de détail. On peut penser qu'ils seront utilisés dans certains domaines comme le financement participatif ou les envois internationaux d'argent, du fait de l'articulation avec les monnaies numériques de banque centrale si elles sont lancées (voir page 45). Les pouvoirs publics appellent traditionnellement le public à la vigilance face aux risques financiers, mais aussi sécuritaires de ces moyens de paiement, la conformité de la technologie *blockchain* avec le RGPD étant en cours d'examen par le Comité européen de la protection des données[54].

Enfin, la question de l'impact sur le climat de ces nouvelles solutions de paiement peut également être posée, eu égard au caractère très gourmand en énergie du système Bitcoin par exemple. Du point de vue de l'impact global, les moyens de paiement classiques et les nouveaux moyens de paiement électroniques ne sont pas nécessairement équivalents.

54 - Voir aussi une première approche de la CNIL sur ces questions : « *Blockchain* et RGPD, quelles solutions pour un usage responsable en présence de données personnelles ? », 24 septembre 2018, cnil.fr

« *CASHLESS SOCIETY* », ANONYMAT ET LIBRE CHOIX ENTRE PLUSIEURS MOYENS DE PAIEMENT

La numérisation des paiements et le développement de moyens de paiement électroniques rend, on l'a vu, les opérations de paiement plus intensives en données toutes choses égales par ailleurs.

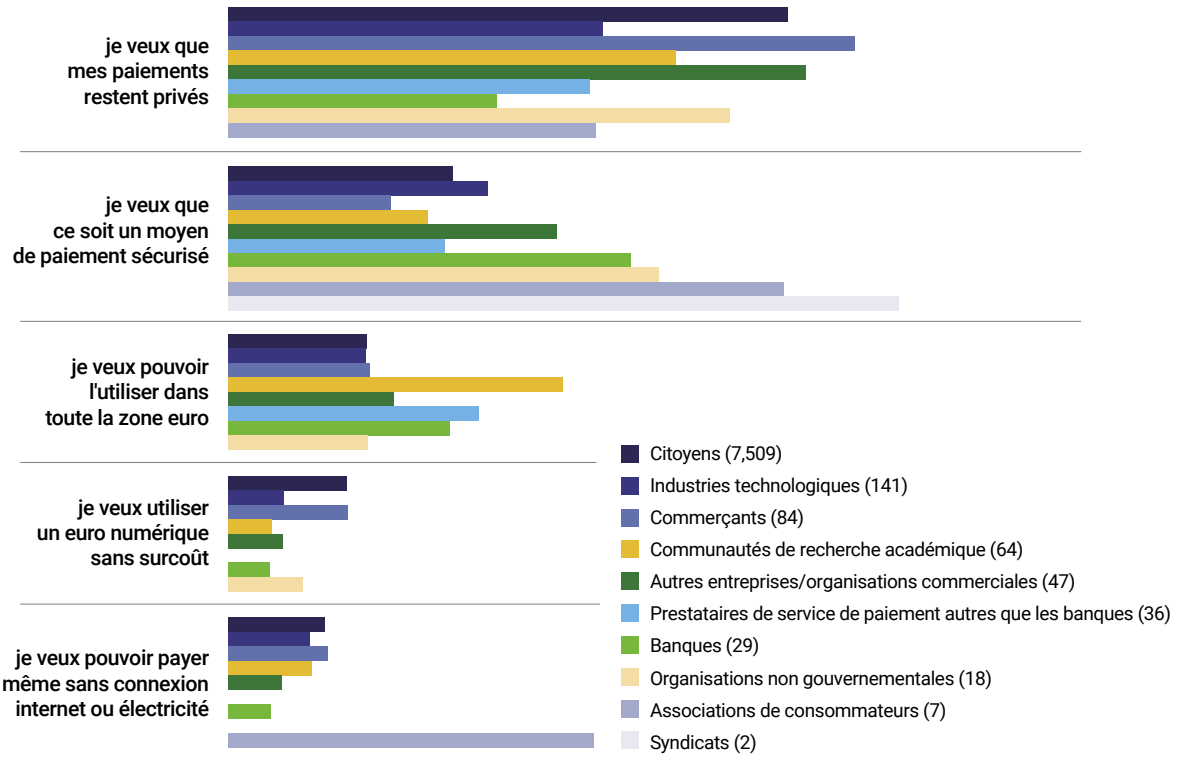
En accroissant le périmètre des opérations pour lesquelles une forme d'identification sur un compte de monnaie scripturale est nécessaire, au détriment de la simplicité et de la modicité du paiement en espèces, elle est mécaniquement facteur de recul de l'anonymat dans les paiements. L'avènement d'une société « sans cash » ne reflète toutefois pas la réalité de demain et au vu de la demande exprimée par les citoyens, les pouvoirs publics devraient prendre en compte des objectifs de maintien de l'accès de la population aux espèces, pour des raisons d'inclusion financière mais aussi économique et sociale.

Par exemple, d'un point de vue technique, les porte-monnaie électroniques au sens de la directive « monnaie électronique » de 2009 sont susceptibles d'être anonymes dans la mesure où leur ouverture ne requiert pas techniquement d'identification régalienne et qu'ils ne sont pas nécessairement liés à un compte bancaire ou à une carte. De ce point de vue, la monnaie électronique s'assimile à un titre au porteur par opposition à un titre de créance nominatif. Toutefois, la législation anti-blanchiment supprime presque entièrement ces possibilités d'anonymat avec une valeur monétaire maximale stockée de 150 €, l'impossibilité de recharger le support via une source non identifiée et une surveillance des transactions à partir de 50 € (article R. 561-16-1 du CMF). Ces limitations n'apparaissent pas disproportionnées au regard des risques dès lors que les citoyens disposent par ailleurs d'un accès, suffisant aux espèces.

Figure 9

Caractéristique la plus importante d'un euro numérique par type de répondant à la consultation publique.

Source : BCE, avril 2021



La question de la protection de la vie privée dans les transactions se pose en des termes renouvelés dans le débat qui entoure la création des monnaies numériques de banque centrale. L'objectif du développement de ces formes monétaires, et notamment d'un euro numérique en Europe, est double :

- **Appuyer l'innovation en matière d'usages de paiement** de détail sur une forme numérique de la monnaie souveraine, émise par le système européen des banques centrales et ayant cours légal, au lieu de la voir se déployer en-dehors du système bancaire classique sur la base de « cryptomonnaies » privées.

- **Fournir aux citoyens européens une forme numérique de monnaie** banque centrale dans les usages en ligne qui deviennent une nouvelle norme, sans pour autant évincer l'usage des espèces. **Pour atteindre ses objectifs et susciter notamment la confiance du public, eu égard aux risques potentiels de surveillance des transactions, l'euro numérique devra avoir des caractéristiques aussi proches que possible des espèces**, en permettant des transactions proches de l'anonymat (voir encadré), ce que permet aujourd'hui la technologie *blockchain* par exemple.

Un autre aspect important pour la protection des droits et libertés dans le domaine des paiements, qui rejoint la protection des consommateurs, est **le libre choix entre plusieurs moyens de paiement.** Du point de vue de l'anonymat des transactions, de l'intensité de la collecte de données personnelles ou encore du point de vue de l'inclusion numérique, tous les moyens de paiement ne sont en effet pas équivalents. Les personnes devraient avoir des alternatives physiques aux paiements en ligne lorsque c'est techniquement possible ; pour une même opération, il est essentiel qu'elles aient le choix entre plusieurs moyens de paiement, dont les espèces ou une monnaie numérique ayant des caractéristiques similaires, tant pour des raisons de sécurité qu'afin de pouvoir choisir elles-mêmes le niveau de collecte de données personnelles auxquelles elles sont soumises. Ainsi, le degré de protection de la vie privée et des données personnelles mérite de constituer un facteur de distinction concurrentielle entre les différents moyens de paiement.

ZOOM SUR...

Les monnaies numériques de banque centrale

En octobre 2020, la BCE a lancé une consultation publique sur un possible euro numérique en vue de créer cette version numérique de l'euro à l'horizon 2024. De nombreuses banques centrales travaillent sur des projets similaires comme la Banque royale de Suède, la Fed américaine ou la Banque populaire de Chine qui est très avancée dans la phase de test d'un yuan numérique. Ces projets ont été accélérés par la publication du projet Libra/Diem (2019/2020).

Le retour de consultation publié par la BCE en avril dernier montre que la protection de la vie privée dans les transactions est le souci n°1 des répondants, qu'ils soient particuliers, commerçants, banques et PSP, ONG ou encore académiques (voir figure 9), avant la sécurité qui est également en lien avec cette préoccupation. De fait, les risques et implications d'un euro numérique de détail en termes de vie privée et de protection des données personnelles, sont massives, une monnaie numérique de banque centrale ayant le potentiel, comme l'illustre l'exemple chinois, de tracer les transactions sur l'ensemble des systèmes de paiement.

De nombreux choix technologiques restent à paramétrer, notamment le choix entre une modalité basée sur un compte ou une modalité basée sur la détention au porteur, le degré d'intermédiation des banques commerciales, la possibilité d'utiliser son portefeuille d'euro numérique sans connexion ni électricité et enfin, le régime LCB-FT applicable. Le degré d'anonymat de l'euro numérique mais aussi la minimisation de la collecte, de l'identification et de la surveillance des transactions seront clé pour le succès du futur euro numérique. L'exigence de protection des données et de la vie privée dès la conception et par défaut devra être respectée.
La CNIL et la Comité européen de la protection des données ont entamé un dialogue avec la Banque de France et les institutions européennes compétentes sur cet important projet[55], qui a été lancé par la BCE le 14 juillet dernier sous la forme d'une phase pilote expérimentale de deux ans.

55 - Cf. EDPB letter to the European institutions on the privacy and data protection aspects of a possible digital euro - to the European Central Bank, 8 juillet 2021, www.edpb.org

La parole à...

DAVID BOUNIE,

ÉCONOMISTE SPÉCIALISTE DES PAIEMENTS

> ***Une solution pour l'euro numérique consisterait à autoriser un anonymat des paiements en dessous d'un certain seuil***

DAVID BOUNIE *est Professeur et Directeur du Département Sciences Économiques et Sociales de Télécom Paris, Institut Polytechnique de Paris, et Academic Fellow de l'Institut Louis Bachelier. Ses recherches portent sur la finance numérique, et sur la façon dont les technologies numériques transforment l'industrie de la finance dans les pays développés et en développement. Il est cofondateur de la Chaire Finance Digitale.*

Vous conduisez des recherches sur la finance numérique depuis près de vingt ans et travaillez avec les commerces, les banques et les banques centrales en France et à l'international. Quelle est selon vous l'innovation technologique majeure en matière de paiement numérique ?

Sans hésitation, les monnaies numériques de banque centrale. Les consommateurs et les commerces sont confrontés à de multiples innovations dans le domaine des moyens de paiement numériques, à la fois pour réaliser des paiements en face à face (sans contact) et des paiements à distance (internet). Il existe également de nombreuses solutions de paiement à distance dédiées proposées par les banques, les plateformes numériques et les grands acteurs de l'internet, et ces dernières se sont lancées également dans l'émission de crypto-actifs et de monnaies numériques privées (le Diem avec Facebook par exemple).

Ces innovations prennent leur essor dans un contexte où la pandémie a renforcé l'usage de la carte au détriment des espèces. Pour faire face à ces évolutions, et pour permettre à l'ensemble de la population, y compris les plus fragiles, de disposer de moyens de paiement acceptés sur l'ensemble du territoire, hors ligne et en ligne, les banques centrales envisagent la création d'un cash numérique. Le cash numérique est l'équivalent du cash physique : il est universellement accepté et dispose du cours légal sur l'ensemble du territoire (y compris virtuel). Le cash est détenu dans un portefeuille sur un *smartphone* (*wallet*), et est distribué par la banque centrale, les banques ou d'autres prestataires de paiement. Les utilisateurs créditent ensuite leur compte et s'identifient via différentes technologies. Le *wallet* dispose d'un identifiant, un solde courant, une limite de paiement. Le *wallet* offre plusieurs services tels que le paiement, le transfert de personne à personne, le remboursement de lignes liées aux cartes de crédit, et intègre des possibilités de services programmables (*smart contracts*). Le service de transfert d'argent entre particuliers peut être utilisé en mode *offline*, contrairement aux autres services de paiement sur mobile qui fonctionnent uniquement sur internet.

En quoi, selon vous, le cash numérique de banque centrale est une innovation majeure ?

Sa création soulève de nombreuses questions. Au-delà des questions de concurrence avec les autres moyens de paiement (cash et carte) et de ses effets sur le système bancaire et monétaire, comment désigner par exemple ce nouveau produit par rapport au cash et à la carte

(e.g. tarification, rémunération) ? Quels services faut-il offrir aux consommateurs et aux commerces ? Faut-il garantir un anonymat dans les transactions à l'image des pièces et billets ? Et dans ce cas, comment assurer un contrôle des paiements afin de lutter contre la fraude, le blanchiment d'argent et le terrorisme ?
Nous ne savons pas encore quelle sera la forme exacte de ce nouveau moyen de paiement en Europe, ni quels services seront proposés aux utilisateurs. Mais il est d'ores et déjà clair que c'est bien une révolution qui est à l'œuvre et qui se distingue des premières générations de monnaie électronique de la fin du siècle dernier. La raison est simple : les banques centrales ont la possibilité d'avoir un contact direct avec les particuliers et les entreprises et de mettre en œuvre un cash numérique programmable. Cette innovation est capitale car elle offre la possibilité à une banque centrale de conduire une politique monétaire ciblée au niveau de l'individu (entreprise) ou de groupes d'individus. Par exemple, il sera possible de mettre en place des prêts programmables, limités dans le temps et l'espace, pour aider certaines personnes ou commerces.

En matière de cash numérique, ne doit-on pas distinguer un « modèle européen » et un « modèle chinois » ?

En fait, pour bénéficier de ces services innovants, il est nécessaire de disposer d'informations sur les transactions, les personnes et/ou les commerces. La Chine a proposé une première voie. Les autorités chinoises ont choisi une infrastructure à deux niveaux : la Banque Centrale émet le e-yuan et gère les infrastructures de paiement, et les banques/commerces distribuent le e-yuan via des comptes dédiés en fournissant directement les portefeuilles. Ce fonctionnement leur donne ainsi une connaissance parfaite de l'ensemble des flux de paiement. Ses motivations sont nombreuses et contingentes à l'économie chinoise, marquée notamment par l'interdiction des cryptomonnaies, le contrôle des flux de capitaux et le contrôle de l'État sur les grandes plateformes de l'internet (Alibaba et Tencent). Les plateformes de paiement dominantes sur le marché chinois sont en effet des acteurs non bancaires, et donc non assujettis à la réglementation bancaire.
Mais ce modèle est peu adapté au marché européen, dominé par des acteurs privés régulés, et des consommateurs soucieux de la protection de leurs données personnelles. Les pièces et billets offrent des garanties d'anonymat dans les transactions qui sont chères aux consommateurs et aux commerces, et les paiements numériques n'offrent pas tout à fait les mêmes garanties en raison en particulier des contraintes réglementaires qui pèsent sur les obligations des banques (lutte contre la fraude, le blanchiment et le terrorisme). Quelle sera donc la proposition de la Banque Centrale Européenne en matière de cash numérique ? Une solution consisterait à autoriser un anonymat des paiements en dessous d'un certain seuil. Mais cette solution pourrait être perçue comme une concurrence déloyale par les banques assujetties dans le cadre des moyens de paiement existants comme la carte bancaire à des règles claires en matière de sécurité et de contrôle des paiements.

Dans le contexte de ces innovations, voyez-vous des points de vigilance pour les régulateurs sur les marchés ?

Un point de vigilance majeur porte sur l'usage des données individuelles de paiement comme instrument de ciblage des consommateurs de la part des grandes plateformes de l'internet. Les plateformes numériques utilisent généralement les données personnelles pour mieux connaître les consommateurs, mais revendent également ces données à des entreprises qui souhaitent à leur tour identifier les consommateurs. Jusqu'à présent, les plateformes numériques n'ont aucune connaissance sur les achats réellement effectués par les consommateurs, à moins de passer des accords avec des acteurs des paiements comme les systèmes de paiement par carte américains par exemple. Ce partenariat permet d'avoir une vision quasi 360° de la vie des consommateurs, en ligne et hors ligne.
Les plateformes numériques pourraient à terme distribuer les *wallets* et le cash numérique, au même titre que les banques. La frontière entre les marchés – réseaux sociaux / plateforme numérique / paiement – pourrait devenir de plus en plus ténue, et accroître la domination des plateformes numériques. Cette évolution poserait de nouveaux défis concurrentiels et d'innovation pour les banques, et les régulateurs, modifiant à terme l'ensemble de l'intermédiation financière. Il va devenir capital pour les autorités de concurrence de bien veiller à définir les marchés pertinents, notamment dans le contexte de l'analyse prospective des opérations de fusion et acquisition dans un marché des paiements de plus en plus fragmenté. Enfin, outre la doctrine des marchés pertinents et du bien-être du consommateur basé essentiellement sur le prix des services, il est nécessaire également de prendre en compte la qualité des services numériques, et notamment la protection des données personnelles. Cette évolution nécessite à terme une collaboration étroite entre les autorités de la concurrence et de la protection des données, y compris dans les analyses de concentration des marchés.

LES ÉVOLUTIONS TECHNOLOGIQUES EN COURS : QUELS « *GAME CHANGERS* » DEMAIN?

Les bouleversements induits par la réglementation (DSP2) et ceux économiques dus à la concurrence des grands services numériques s'accompagnent de mutations causées par le déploiement de technologies nouvelles, certaines non spécifiques au paiement (comme les chaînes de blocs ou l'informatique en nuage) que nous ne commenterons pas ici, d'autres qui lui sont propres : on peut citer, sans être limitatif, le virement instantané, le « *request to pay* » et le paiement sur ordiphone (paiement mobile).

Le virement instantané existe déjà dans la zone SEPA depuis 2017 sous le nom de SCT Inst mais il n'est pas encore généralisé. C'est un virement de compte bancaire à compte bancaire, effectué en moins de 10 secondes et irrévocable compte tenu de sa rapidité. Le modèle d'affaires du paiement instantané n'est pas encore trouvé : certaines banques sont réticentes, mettant l'accent sur le risque de fraude ou sur la difficulté de procéder aux contrôles anti-blanchiment sur les montants, ou appliquent des frais alors que les virements SEPA classiques sont gratuits. La Banque Centrale Européenne a appelé récemment[56] les banques de détail à rendre cette modalité plus accessible, en particulier car elle constitue une alternative ergonomique et efficace aux services de paiement intermédiés par les acteurs numériques.

En-dehors des transferts d'argent entre particuliers de pair à pair (à l'image de l'application américaine Venmo, rachetée par PayPal en 2018) les cas d'usage sont encore peu nombreux à se mettre en place (on peut penser au *cash-back*), compte tenu de la faible généralisation du dispositif dans la zone SEPA. La BCE a développé un système de règlement dédié aux paiements instantanés, baptisé TIPS (Target Instant Payment Settlement), à adhésion facultative mais que la BCE souhaite rendre obligatoire pour toutes les banques d'ici à la fin de l'année. Avec 14 millions de transactions pour un montant total de 7 milliards d'euros en 2019, ce qui est très faible par rapport aux 28 658 milliards d'euros de transactions en 2019 (toujours selon le rapport annuel de l'OSMP), le virement instantané présente encore un caractère très marginal.

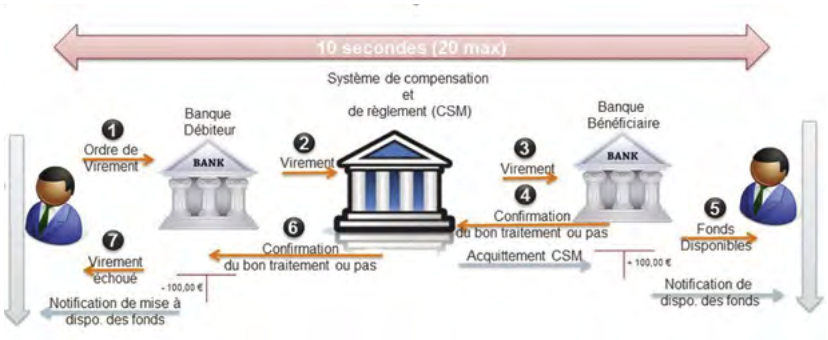
Du point de vue de la circulation des données, les protocoles conçus par les réseaux de carte ne lui sont pas applicables et les spécifications « SCT Inst » ont été définies pour une circulation de données plus large avec une taille de message de paiement à 140 caractères. Ces spécifications impliquent, hors de la solution de paiement avec un lien par sms comme proposé par certaines applications, le traitement du numéro de compte bancaire (IBAN) qui comporte une certaine sensibilité. Bien que l'IBAN ne soit pas une donnée sensible au sens de la DSP2, sa tokenisation dans le cadre du protocole « SCT Inst » serait sans doute une avancée en termes de sécurité (voir page 63).

D'une façon générale, **une tendance à l'enrichissement des données de paiement** est perceptible avec le projet de norme ISO 20022, qui devrait être généralisé en Europe d'ici la fin de l'année prochaine. Cette norme, opérée par SWIFT, permettra à des messages plus volumineux de véhiculer plus de données pour permettre des services additionnels (réconciliation, automatisation de la facturation, facilitation des paiements transfrontaliers) mais aussi la lutte contre la fraude, allant plus loin que le simple paiement.

Figure 10

Fonctionnement du virement instantané SCT Inst.

Source : Sébastien Chesnais.



56 - « Virement instantané : l'Europe demande aux banques de baisser leurs tarifs », 24 mai 2021, le monde.fr.

Le Forum européen des paiements a par ailleurs adopté le système ***« request to pay »*** (demande de payer). Il s'agit d'un service de messagerie venant s'ajouter aux infrastructures existantes et permettant de préparer l'opération de paiement proprement dite, en envoyant au payeur une requête lui demandant de s'authentifier auprès de sa banque et au commerçant la confirmation de l'acceptation de sa requête. Le paiement est ensuite dénoué entre les banques du payeur et du payé, via un virement « SCT Inst ». L'objectif est de proposer au consommateur une expérience de paiement mieux préparée et sans frictions avec de nouveaux services de facturation, recouvrement ou paiement de pair à pair. Ce projet dont le déploiement est prévu cette année intéresse les banques, les Fintechs mais aussi les GAFA, impliqués dans le projet.

Dans les spécifications, le message de données fondé sur la norme ISO 20022 sera également enrichi pour permettre notamment d'accueillir des données de facturation, mêlant ainsi données de paiement et données d'achat : les messages peuvent embarquer la facture en pièce jointe ainsi qu'une référence de paiement (identification) dans un champ appelé « *RTP Remittance information* ». Cela ne pose pas de difficulté pour la facturation interentreprises mais implique le mouvement de données enrichies dans un usage de détail. Cela pose la question, dans les spécifications, de la pseudonymisation des donnés directement identifiantes comme la référence du payeur (nom, adresse) et l'IBAN, au lieu de leur circulation en clair.

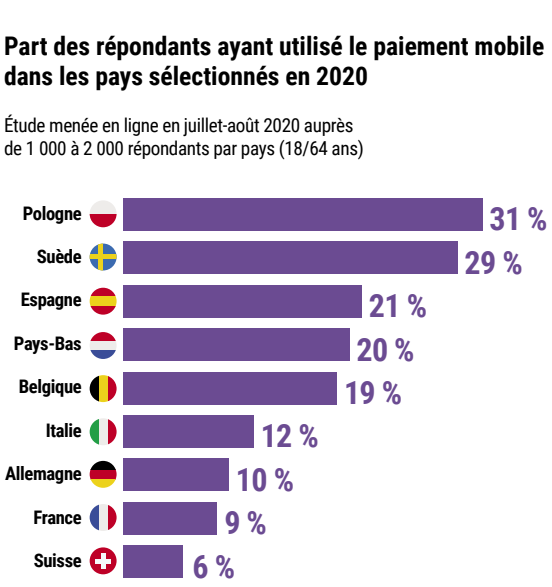
Il est encore un peu tôt pour savoir si ces évolutions seront des « *game changers* » (« qui change la donne ») pour le domaine des paiements. Voyons ce qu'il en est à présent pour **le paiement mobile**, déjà évoqué. Son taux de pénétration est resté très faible en France jusqu'à la période actuelle. L'arrivée de la solution la plus répandue sur le marché, Apple Pay, est récente (2016) et sa généralisation à l'ensemble des banques l'est encore plus. Selon la dernière étude du *Global Consumer Survey* menée à l'été 2020, seul environ un Français interrogé sur dix déclarait utiliser un mode de paiement par ordiphone. Il s'agit d'un des taux d'adoption les plus faibles en Europe, avec des pays comme l'Allemagne (10 %) et la Suisse (6 %). D'autres pays européens tels la Pologne, la Suède, l'Espagne ou les Pays-Bas sont déjà bien plus avancés en la matière, avec une part d'utilisateurs qui était comprise entre 20 % et 31 % à l'été 2020 (voir figure 11), et sans doute encore plus aujourd'hui du fait de la pandémie.

Toujours d'après le *Statista Global Consumer Survey,* qui compile des données de consommation sur plus de 50 marchés dans 55 pays, l'application Paylib s'impose sur le podium des services de paiement mobile les plus populaires en France. 28 % des utilisateurs de ce genre

Figure 11

Le paiement mobile a d'importantes marges de progrès en France.

Source : Statista



de services déclaraient avoir utilisé cette application pour payer dans un point de vente au cours de l'année passée (enquête de mars 2020), contre respectivement 35 % et 41 % pour les géants du secteur, Google Pay et Apple Pay. Parmi les autres services populaires dans l'Hexagone, on retrouve deux autres entreprises françaises particulièrement prometteuses sur ce marché, Lyf Pay (13 %) et Lydia (9 %). Il faut bien sûr garder en tête que ces chiffres constituent avant tout des indicateurs de la renommée de ces différents services auprès des utilisateurs français et qu'ils ne correspondent pas forcément à leurs parts de marché.

Le paiement par ordiphone a un fort potentiel de généralisation à terme, tant en raison de sa facilité d'usage que de sa gratuité pour le client final (les commissions d'ailleurs fort onéreuses sont acquittées par les banques) et de sa compatibilité avec le paiement par carte bancaire. Du point de vue de la protection des données personnelles, se présente une variété de modèles d'affaires, certains plus protecteurs de la vie privée en s'engageant à conserver les données de paiement (mais aussi dans une certaine mesure, d'achat) localement sur le terminal, d'autres ayant recours à plus de centralisation et de combinaison des données, en mêlant cartes de paiement et carte de fidélité sur un même porte-monnaie. Au-delà des questions de sécurité, des travaux à venir des autorités de protection des données sur ce sujet seraient sans doute pertinents.

INTERNET DES OBJETS ET PAIEMENT AUTONOME

Après-demain, le développement de l'internet des objets se doublera de la capacité technique de ces objets connectés à opérer des paiements, sans ou avec peu d'intervention humaine (automaticité) et d'objet à objet, sans routage entre un payeur et un payé personne physique (autonomie).

Les professionnels du paiement imaginent même des techniques de paiement invisibles pour l'utilisateur avec recours à l'intelligence artificielle. À l'heure actuelle, Amazon expérimente d'ores et déjà les points de vente Amazon Go, avec une première boutique ouverte en Europe à Londres en mars 2021, où les paiements sont opérés automatiquement, posant des délicates questions de reconnaissance et de traçage des utilisateurs. Les paiements sont peut-être initiés de manière autonome, mais sont bien *in fine* imputés sur un portefeuille ou un compte d'un utilisateur personne physique disposant d'une capacité financière.

Les cas d'usage sont d'ores et déjà imaginables aujourd'hui : services en temps partagé avec paiement à l'usage, stationnement d'un véhicule, recharge électrique d'un véhicule, commandes passées par un réfrigérateur connecté, micropaiements par ordiphone pour accéder à des contenus culturels ou média… Ces cas d'usage poseront des questions au-delà de la protection des données, de confiance de l'humain dans la machine (auditabilité des algorithmes et interprétabilité des résultats) et de sécurité (pseudonymisation des identifiants stockés dans les objets et authentification tant de l'objet lui-même que de l'utilisateur qui en est responsable).
Les questions qui se poseront demain à la CNIL sur ce sujet ne sont donc pas fondamentalement différentes de celles qui se posent aujourd'hui, mais seront un condensé de toute leur complexité, de la protection des données personnelles à la régulation de l'intelligence artificielle en passant par la sécurité. La confiance que les personnes peuvent placer dans un univers de paiement donné sera demain comme aujourd'hui, au cœur de nos préoccupations.

« ***Les cas d'usage sont d'ores et déjà imaginables aujourd'hui : services en temps partagé avec paiement à l'usage, stationnement d'un véhicule, recharge électrique d'un véhicule, commandes passées par un réfrigérateur connecté, micropaiements par ordiphone pour accéder à des contenus culturels ou média*** »

LES FRICTIONS DÉSIRABLES DU FUTUR DU PAIEMENT

Nous l'avons vu, l'ensemble de l'écosystème du paiement, poussé notamment par les acteurs numériques, cherche à « fluidifier l'expérience de paiement » et à « réduire les frictions » qui peuvent retenir les consommateurs de réaliser un paiement.

Si l'intérêt commercial de ces initiatives est indéniable, la CNIL recommande au contraire, depuis quelques années, d'entretenir des « frictions désirables » qui permettent de contextualiser la collecte de données personnelles et de garantir la bonne information et l'exercice des droits des personnes[57]. Ces frictions peuvent aussi permettre de renforcer l'authentification du payeur et la sécurité globale de la transaction.

À cet égard, l'expérience de la carte bancaire, déployée massivement à partir des années 1980, constitue un modèle d'équilibre entre ergonomie, sécurité, et responsabilisation des consommateurs. En adoptant une authentification à deux facteurs (par exemple : posséder la carte et connaître le code PIN) utilisée par la quasi-totalité de la population, le système bancaire a franchi un cap important de sécurisation qui a permis de maintenir un niveau de fraude très bas. Dans le même temps, cette opération quotidienne est rapide, tout en restant totalement sous le contrôle de la personne qui paye.

À l'heure du paiement sans contact, voire sans caissier, des « frictions désirables » permettant à chacun de garder la maîtrise des paiements qu'il réalise mais également des transferts de données personnelles associées doivent être redéfinies : cela peut prendre la forme de rappels réguliers via l'ordiphone, de notifications ou de nouveaux mécanismes d'alerte au sujet de dépenses inhabituelles (dont le fonctionnement reposerait néanmoins sur des analyses de données avancées). La question des alternatives est également essentielle pour protéger la liberté de choix des utilisateurs et éviter la stigmatisation de pratiques moins automatiques.

« *La question des alternatives est également essentielle pour protéger la liberté de choix des utilisateurs et éviter la stigmatisation de pratiques moins automatiques.* »

57 - *La forme des choix, données personnelles, design et frictions désirables* (PDF, 1,4 Mo), mars 2019, cnil.fr.

GARANTIR LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE DANS LE DOMAINE DES PAIEMENTS : points de vigilance

Comme le démontre le propos introductif, l'écosystème propre aux moyens de paiement intègre une pluralité d'acteurs intervenant à des degrés variables sur la finalité et les moyens des traitements réalisés à partir des transactions et de leurs données accessoires. Chacun de ces acteurs réalise des opérations de traitement sur des données personnelles dans ce cadre. À ce titre, leur niveau de responsabilité vis-à-vis de ces traitements doit être clair, pour déterminer leurs obligations au regard du RGPD et vis-à-vis des personnes concernées.

LA PROTECTION DES DROITS DANS UN ÉCOSYSTÈME FRAGMENTÉ

La question du statut des acteurs de la monétique au regard du RGPD

Le RGPD prévoit trois qualifications possibles. Tout professionnel traitant des données à caractère personnel agit soit en qualité de responsable de traitement, soit en qualité de sous-traitant, soit en qualité de responsable de traitement conjoint. Il est essentiel pour chaque acteur de connaître son rôle puisque la nature des obligations qui lui incombent en dépend.

Le responsable de traitement

Le responsable de traitement est la personne, l'autorité publique, la société ou l'organisme à l'origine du traitement, qui décide de sa mise en œuvre en déterminant à la fois son but (appelé « finalité ») et ses modalités (dits « moyens essentiels », tels que le type de données personnelles traitées ou la durée de leur traitement, ou encore la détermination des destinataires des données)[58].

Le responsable de traitement, du fait de son influence déterminante sur le traitement des données, est tenu de veiller au respect des principes essentiels du RGPD.
Cette qualification est relativement facile à opérer lorsqu'une entité est la seule à traiter un fichier, pour son propre compte. C'est notamment le cas d'un fichier client mis en place par un commerçant. Toutefois, en matière de paiement, plusieurs parties sont nécessairement présentes. En effet, en dehors des paiements en espèces, il est quasiment impossible qu'une seule partie traite les données de paiement, dès lors que le bénéficiaire du paiement dispose lui-même d'un gestionnaire de compte généralement différent du gestionnaire du compte de paiement utilisé par le payeur, et se trouve également susceptible de recourir à plusieurs intermédiaires, tels qu'une passerelle de paiement, un transporteur de flux, un réseau de carte bancaire, un prestataire de service de paiement, etc. Cette spécificité du secteur impose de s'interroger sur une éventuelle sous-traitance ou responsabilité conjointe.

Le sous-traitant

Contrairement au responsable de traitement, le sous-traitant ne traite pas les données pour son propre compte, mais pour le compte et sous l'autorité d'un responsable de traitement. Une très grande variété de prestataires de services revêt la qualité de sous-traitant au sens juridique du terme, notamment dans le secteur des paiements. Il convient toutefois de ne pas confondre les sous-traitants avec les prestataires fournisseurs de solutions n'ayant pas accès et ne traitant pas de données à caractère personnel tels que les éditeurs de logiciels ou les fabricants de matériels, qui ne sont pas concernés par cette qualification.
Une entité ne peut traiter des données en qualité de sous-traitant que sur instruction documentée du responsable de traitement, ce qui exclut par conséquent toute réutilisation propre des données sans l'accord du responsable de traitement.

En pratique, l'analyse d'un faisceau d'indices au cas par cas est nécessaire pour déterminer si une entité est un sous-traitant ou un responsable de traitement. Ainsi peuvent être pris en compte le niveau d'instruction donné, le degré de contrôle de l'exécution de la prestation, la valeur ajoutée fournie par le prestataire ou encore le degré de transparence sur le recours à un prestataire.
L'une des spécificités du domaine des paiements réside dans le nombre restreint d'acteurs en contact direct avec les personnes concernées (tels que les banques, les commerçants, ou les prestataires de service de paiement à

58 - Lignes directrices 07/2020 du CEPD sur les concepts de responsable de traitement et de sous-traitant dans le RGPD, juillet 2021, edpb.europa.eu

destination de particuliers). Si l'absence de relation directe d'un professionnel avec les personnes concernées n'est pas déterminante en matière de qualification, elle doit être prise en compte et peut conduire à considérer que de nombreux prestataires de service traitent les données en qualité de sous-traitant.

Cela semble notamment être le cas lorsque le service en question est à destination de commerçants ou de banques et que les données ne sont pas réutilisées pour le propre compte de ces derniers ou le compte d'autres clients responsables de traitement. La séparation hermétique (logique ou physique) des bases de données de chaque client est un critère pertinent à cet égard afin de s'assurer que le sous-traitant ne traite les données que pour le compte de ses clients responsables de traitement et ne réutilise pas les données transmises par ses clients professionnels pour son propre compte ou pour proposer d'autres services à valeur ajoutée (par exemple pour améliorer ses services ou établir des profils ou même des statistiques à partir de ces données, afin de les commercialiser).

Les responsables conjoints de traitement

Enfin, il existe des situations dans lesquelles plusieurs acteurs sont à l'origine d'un traitement et pour lesquels ils définissent conjointement la finalité et les moyens essentiels. Cela est notamment le cas lorsque deux organismes traitent des données pour une même finalité (telle que la réalisation du paiement) et déterminent les catégories de données traitées ou leurs destinataires. Cette situation peut résulter d'une prise de décision commune comme d'une pluralité de décisions séparées mais convergentes sans lesquelles le traitement n'aurait pas lieu.

Les responsables de traitement conjoints sont tenus de se répartir en toute transparence leurs obligations respectives au titre du RGPD. Un accord doit alors être conclu entre ces derniers pour refléter cette répartition des rôles, et les points essentiels de cet accord doit être rendu accessible aux personnes concernées, lesquelles peuvent toutefois exercer leurs droits (tels que le droit d'accès à leurs données) auprès de chaque responsable de traitement conjoint.

En matière de paiement, il semble envisageable de retenir la notion de responsabilité conjointe, dès lors qu'un certain nombre d'acteurs dans la chaîne de traitement sont susceptibles d'intervenir pour une même finalité (telle que la réalisation du paiement) et de potentiellement déterminer conjointement les moyens de ces traitements.

Les prestataires se présentant comme sous-traitant ne peuvent réutiliser les données pour leur propre compte sans changer de statut et devenir responsable du traitement

Dans le secteur de paiement, un nombre important de prestataires de service se présentent comme sous-traitants. Il est donc déterminant pour ces acteurs d'avoir conscience que cette qualification ne les autorise pas à traiter les données qui leur sont confiées, en dehors des instructions de leur client, pour leur compte et de leur propre initiative.

En effet, étant tenu de ne traiter les données que sur instruction documentée de son responsable de traitement, le sous-traitant doit être autorisé par écrit par ce dernier afin de pouvoir envisager de traiter les données pour son propre compte. Il deviendrait alors responsable de ces traitements. Cette autorisation doit pouvoir résulter d'une liberté réelle du responsable de traitement de l'accorder et ne peut résulter d'une clause insérée par le sous-traitant dans ses contrats standard. Une telle réutilisation est également subordonnée à la vérification, par le responsable de traitement initial, de la compatibilité de ces nouvelles finalités propres du sous-traitant avec la finalité pour laquelle les données ont été initialement collectées.

Pour s'assurer de cette compatibilité (détaillée ci-après), le responsable de traitement initial doit prendre en compte différents facteurs listés à l'article 6.4 du RGPD, parmi lesquels figurent l'existence éventuelle d'un lien entre les finalités, les conséquences possibles du traitement ultérieur envisagé pour les personnes concernées et la nature des données, qui en l'espèce appellent à une vigilance toute particulière et à une appréciation relativement stricte de ce que pourrait être **une finalité compatible**. Le responsable de traitement initial est également tenu d'informer les personnes concernées par ce destinataire (ou de cette catégorie de destinataires des données) dans l'hypothèse où il accorderait une telle autorisation.

Enfin, outre l'obtention de cette autorisation écrite de la part du responsable de traitement initial, l'ensemble des dispositions du RGPD doit être appliquées par le nouveau responsable de traitement, ce qui inclut notamment **l'information des personnes** quant à la finalité du traitement et quant à l'identité de son responsable ainsi que la mise en place de mécanismes permettant l'exercice de leurs droits. De même, si le traitement réalisé ne peut se baser que sur le consentement des personnes, le sous-traitant devenu responsable de ce traitement devra prévoir un moyen de recueillir directement cet accord auprès des personnes concernées, en passant par exemple par son

client si ce dernier est en contact direct avec les personnes en question.

La question de la maîtrise des risques présentés par les traitements

L'un des principes essentiels du RGPD réside dans l'obligation pour les professionnels de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données. Ce principe, souvent désigné par le terme anglais d'« *accountability* », se manifeste à travers plusieurs obligations du RGPD, notamment celle de tenir un registre des traitements, ou encore celle de réaliser des **analyses d'impact relatives à la protection des données** (souvent désignées par le sigle AIPD ou, en anglais, DPIA ou PIA pour *privacy impact assessment*) lorsqu'un traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

Cette analyse doit être réalisée avant la mise en œuvre du traitement envisagé et être mise à jour tout au long du cycle de vie du traitement pour permettre au responsable de traitement d'apprécier les risques pouvant être engendrés par un traitement de données et de mettre en place des garanties permettant de réduire et contrôler ces risques.

Or, cette analyse se révèle fréquemment nécessaire en matière de données de paiement. En effet, pour déterminer si une telle analyse est nécessaire, il convient de vérifier si le traitement en cause remplit au moins deux des neuf critères issus des lignes directrices du G29[59]. Si la nature particulière des données de paiement n'est pas encadrée par une interdiction de traitement de principe, elle appelle à une vigilance particulière de la part des responsables de traitement, en ce qu'elle remplit l'un des critères permettant de déterminer si une AIPD est requise, du fait de leur caractère hautement personnel. En outre, une analyse d'impact sera nécessaire dès que le traitement envisagé remplit un autre critère, tel que l'évaluation ou le *scoring* (y compris le profilage), l'existence d'une décision automatisée produisant un effet significatif sur les personnes concernées, la collecte de données personnelles à large échelle, le croisement de données, ou encore la présence d'une technologie innovante.

La CNIL a publié[60] une liste d'opérations de traitement pour lesquelles la réalisation d'une analyse d'impact relative à la protection des données est obligatoire. À titre d'exemple, elle inclut les traitements de profilage faisant appel à des données provenant de sources externes, lesquels peuvent concerner le secteur des paiements, notamment dans le cadre de finalités commerciales ou lutte contre la fraude.

59 - Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679 (PDF, 1,4 Mo), 4 avril 2017, cnil.fr.
60 - « Délibération n° 2018-327 portant adoption de la liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise », 11 octobre 2018, legifrance.fr

PROPORTIONNALITÉ ET MINIMISATION

Finalité du traitement et principe de minimisation des données

Parmi les grands principes du RGPD, mentionnés à l'article 5 du règlement, le principe de finalité du traitement et celui de la minimisation des données sont d'une importance particulière en matière de paiement. La réglementation impose à tout responsable de traitement de veiller à ce que la finalité de chaque traitement soit déterminée, légitime et explicite. La finalité recouvre le but ou l'objectif poursuivi par le traitement. Elle doit notamment être consignée dans le registre qui doit être tenu par le responsable de traitement, mais doit surtout être portée à la connaissance des personnes concernées dans le cadre des obligations de transparence. Cette obligation n'est pas neutre dans un écosystème complexe tel que celui des paiements, car elle suppose que chaque acteur décidant d'utiliser des données pour son compte se fasse connaître, par une information directe et aisément accessible des personnes concernées, afin que ces dernières puissent tracer l'usage de leurs données, et exercer, si elles le souhaitent, les droits que leur garantit le RGPD.

Par ailleurs, déterminer précisément la finalité des traitements est essentiel pour définir les données qu'il est possible de traiter. En effet, le principe de minimisation prévoit que les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. Il est donc interdit et illicite de collecter voire d'accumuler des données en dehors d'une finalité valable, au seul motif que ces données pourraient s'avérer utiles à l'avenir. Par exemple, la finalité ne peut se résumer à la simple volonté de centraliser des données provenant de sociétés d'un même groupe, sans objectif précis, ou encore elle ne saurait se limiter au souhait d'accumuler suffisamment de données pour envisager ultérieurement d'en tirer une signification ou de développer sur leur base un nouveau service.

Il en va de même s'agissant du recoupement de données de paiement avec d'autres catégories de données, telles que des données comportementales, des données précises quant aux achats réalisés ou encore des données de localisation. L'enrichissement des données de paiement, notamment par l'ajout de données contextuelles, ne constitue pas une finalité en soi. Cela ne signifie pas que ces traitements sont par nature impossibles et illicites, mais que la centralisation, le croisement ou l'enrichissement de données ne sont pas à eux seuls des finalités valables.

À titre d'exemple, la finalité principale en matière de paiement est la **réalisation d'une transaction**. À cet égard, la CNIL considère que s'agissant des paiements à distance par carte bancaire en contrepartie d'un bien ou d'un service, le numéro de carte de paiement, la date d'expiration et le cryptogramme visuel sont les seules données strictement nécessaires à la réalisation du paiement. À l'inverse, l'état civil du porteur de carte, le contenu du panier, ou encore l'adresse de livraison n'apparaissent pas strictement nécessaires à la réalisation du paiement. En tout état de cause, les coordonnées bancaires, le numéro de carte de paiement sont des données dont le traitement est difficilement envisageable en dehors de la finalité de réalisation du paiement. Leur traitement n'est pas interdit par principe en ce qu'elles ne sont pas par nature des catégories particulières de données soumises à l'article 9 du RGPD, mais le caractère hautement personnel de ces données et le principe de minimisation imposent une vigilance accrue.

Une tendance du secteur des paiements en ligne, observée auprès de plusieurs acteurs, consiste à proposer des solutions de paiement en ligne permettant une ergonomie sans friction pour l'utilisateur, ce qui implique différents traitements de données personnelles en amont de la validation de l'achat. Il convient de remarquer que ces traitements poursuivent une finalité distincte de la réalisation de la transaction, qui résiderait davantage dans l'optimisation du parcours de paiement. Il en résulte que si ces données supplémentaires pouvaient se révéler nécessaires pour cette finalité distincte de la finalité de réalisation du paiement, elles doivent alors répondre à des conditions différentes (notamment au regard des bases légales de ces traitements, développées ci-dessous).

Protection des données dès la conception et par défaut

Le principe de minimisation est à rapprocher de l'exigence de protection des données dès la conception et par défaut, qui exige que le responsable de traitement mette en œuvre, tant au moment de la détermination des moyens du traitement que du traitement lui-même, des mesures techniques et organisationnelles (telles que la pseudonymisation, consistant à transformer des données de façon à ce qu'elles ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, par exemple en remplaçant les données directement identifiantes comme les noms et numéros de carte par des valeurs aléatoires).

Par exemple, pour les analyses statistiques à des fins d'amélioration des services de paiement, il convient tout d'abord d'envisager si le traitement de données personnelles est nécessaire (c'est-à-dire si le traitement de données anonymes ne suffirait pas, notamment l'utilisation de statistiques agrégées ne permettant pas d'identifier une personne concernée). À cet égard, il convient de noter que l'anonymisation de données de paiement peut se révéler extrêmement complexe en raison de leur caractère très identifiant. Si le traitement de données anonymes ne suffit pas, il convient d'envisager de pseudonymiser les données, chaque fois que cela est possible.

Dans le domaine des paiements, ces principes se traduisent essentiellement par des mesures portant sur la pseudonymisation, la minimisation des données collectées, de la durée de conservation des données, ainsi que les destinataires. Toutefois, la mise en œuvre de ces principes peut aussi résulter de mesures permettant aux personnes concernées d'opérer un contrôle sur le traitement de leurs données, telles que la mise en œuvre d'un droit d'opposition préalable et n'ayant pas à être motivé à l'égard de certains traitements, notamment à des fins de prospection commerciale.

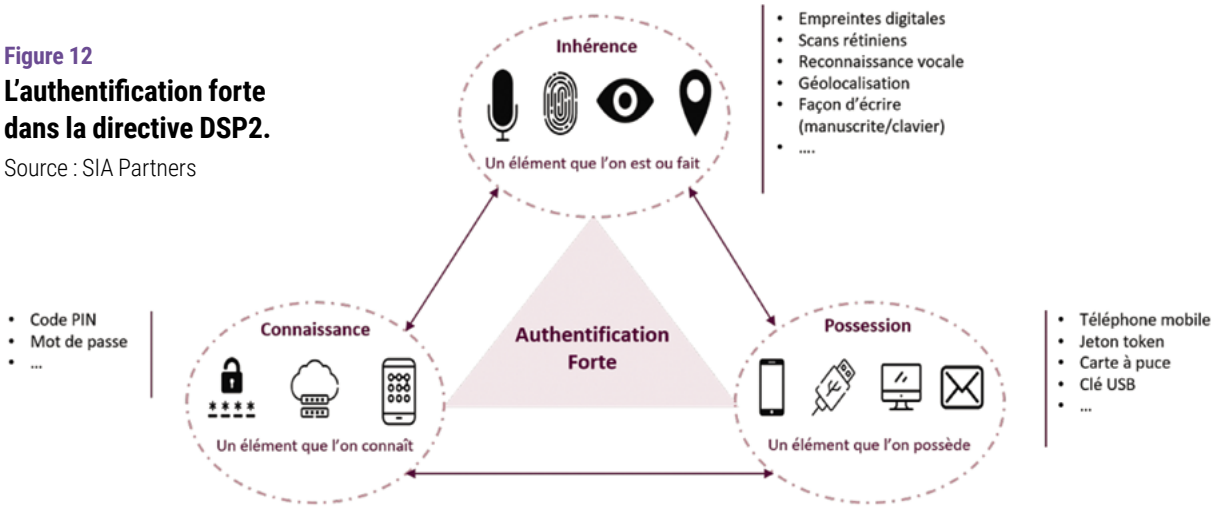
IDENTIFICATION ET AUTHENTIFICATION

Comme on l'a vu, les opérations de paiement, notamment à distance, nécessitent l'identification du payeur et du payé pour que les fonds soient légitimement débités à la bonne personne et atteignent le bon destinataire. Par ailleurs, l'émetteur d'un instrument de paiement (typiquement un établissement de crédit, un établissement de paiement ou un établissement de monnaie électronique) est soumis aux règles anti-blanchiment qui impliquent une identification régalienne du client et une surveillance des transactions effectuées. Toutefois, cet impératif d'identification ne concerne que l'émetteur des instruments de paiement. Comme l'illustre l'exemple de la carte bancaire, il n'est pas nécessaire que le destinataire du paiement, par exemple le commerçant, ait accès à l'identité régalienne du payeur : il lui suffit d'avoir la certitude que le tiers de confiance lui versera les fonds via l'utilisation d'un identifiant pseudonyme qui garantit que son client s'est bien authentifié auprès de l'émetteur de l'instrument de paiement. Même dans un contexte de lutte contre la fraude il n'y a donc pas d'équivalence entre paiement et « identité numérique ».

Il convient de distinguer **identification** (phase qui consiste à établir l'identité de l'utilisateur, permettant de répondre à la question « Qui êtes-vous ? » via un identifiant unique) et **authentification** (phase qui permet à l'utilisateur d'apporter la preuve qu'il est identifié, permettant de répondre à la question « Êtes-vous réellement cette personne ? » via l'utilisation d'un authentifiant que lui seul connaît ou possède). L'authentification consiste pour le tiers de confiance du payeur à faire savoir qu'il a bien identifié ce dernier. Elle n'implique pas l'enrôlement de la personne sur un compte détenu par le marchand, même si ce dernier peut souhaiter le faire pour des raisons de gestion de la clientèle par exemple.

La DSP2 a, en conséquence, instauré un standard d'authentification forte pour les paiements, dite à deux facteurs à choisir parmi trois éléments (voir figure 12), donnant accès au compte bancaire du client : l'inhérence (ce que l'on est), la connaissance (ce que l'on connaît) et la possession (ce que l'on possède). Ces trois catégories ne sont toutefois pas équivalentes du point de

Figure 12
L'authentification forte dans la directive DSP2.
Source : SIA Partners



vue du RGPD, la catégorie « inhérence » relevant la plupart du temps de la qualification de données biométriques, protégées par l'article 9 du RGPD. L'authentification forte n'est pas obligatoire lorsque la transaction est à faible risque (score de lutte antifraude, tel que calculé par le prestataire de services de paiement, inférieur à un certain seuil), lorsqu'elle est inférieure à 30 euros ou résulte d'un abonnement, notamment. La réglementation distingue bien, conceptuellement, authentification et lutte antifraude qui correspondent à deux opérations différentes. Le standard 3DSv2 développé par les grands réseaux de carte bancaire pour lutter contre la fraude en ligne, et qui utilise d'ailleurs un jeu enrichi de données[61], en est également une illustration. Ces deux notions ne sont donc pas soumises à la même analyse pour ce qui est la protection de la vie privée, y compris parce que l'authentification forte crée un moment de « friction » pour les personnes, alors que des diligences de lutte anti-fraude invasives et « passives » pour les individus n'ont pas le même effet.

En outre, reflétant par-là la polysémie du terme « identité », il existe **plusieurs niveaux d'identification**, allant de l'anonymat de l'usage des espèces à l'identité régalienne certifiée par les pouvoirs publics en passant par l'identité déclarative ou pseudonyme via un login et mot de passe. Dans la plupart des actes de paiement en situation contractuelle, l'usage d'un identifiant déclaratif auprès du commerçant ou du service souscrit suffit et une « suridentification régalienne » à des fins d'authentification ne serait pas souhaitable. L'attribut d'identité étant une donnée personnelle, sa divulgation doit être requise en conformité avec le RGPD, en respectant les principes de nécessité, minimisation et proportionnalité de la collecte décrits ci-dessus.

ZOOM SUR...

Des usages de la biométrie à bien évaluer

Les données biométriques sont des données sensibles au sens du RGPD et à ce titre, sont particulièrement protégées. Elles ne peuvent être traitées que pour des finalités particulièrement justifiées. Elles ne peuvent pas, notamment, être traitées sur la base de l'exécution d'un contrat ou sur le fondement de l'intérêt légitime du responsable de traitement, mais seulement, pour un intérêt commercial, sur la base du consentement. Pour les raisons décrites ci-dessus, la CNIL admet plus facilement le traitement des données biométriques dans un usage d'authentification, plutôt que d'identification des personnes.

Dans un contexte de généralisation des mécanismes d'authentification biométriques sur les ordiphones, particulièrement utilisées en matière de paiement, la CNIL a rappelé que les personnes doivent garder la maîtrise de leur gabarit biométrique via un stockage en local[62]. C'est dans ce cas que les traitements mis en œuvre, à l'initiative et sous le seul contrôle de la personne concernée, peuvent être couverts par l'exemption domestique mentionnée à l'article 2.2 c) du RGPD. Cela exclut toute authentification biométrique imposée ou « passive » (dont la personne concernée n'aurait pas conscience). Cela implique aussi que les fournisseurs d'application proposent un mode d'authentification alternatif à la biométrie (par exemple la saisie d'un code), sans contrainte additionnelle. Enfin, le dispositif doit comporter par défaut des garanties élevées de sécurité.

Dans le cadre de l'essor actuel de la « biométrie comportementale », les modalités biométriques auparavant statiques (empreinte digitale, scan rétinien, visage) deviennent dynamiques (frappe, démarche, manière de tenir un objet) et, combinées entre elles et avec l'aide de l'intelligence artificielle, pourraient aboutir à un haut niveau d'identification unique des personnes. Les cas d'usage concernés s'étendent à la détection de la fraude. La pertinence de collecter un consentement, qui peut être ensuite retiré à tout moment, aux fins d'obtenir une évaluation de lutte anti-fraude, pose évidemment question du point de vue du responsable de traitement, comme l'est celle de la proportionnalité de l'usage d'identifiants biométriques à cette fin, du point de vue du régulateur. Ces difficultés se doublent de celles relatives à la collecte de données de type traceur sur un terminal, sur le fondement de la directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, dite « ePrivacy ».

61 - Device ID, adresse IP, identité du porteur, adresse pour la livraison, numéro de téléphone, certains champs n'étant pas obligatoires mais fortement recommandés : voir les spécifications « EMV 3-D Secure » sur emvco.com.
62 - « Biométrie dans les smartphones des particuliers : application du cadre de protection des données », 24 juillet 2018, cnil.fr.

CIRCULATION, RÉUTILISATION, CONSERVATION

Collecte, utilisation et circulation des données de paiement

Le domaine des paiements est marqué par un nombre important d'acteurs intervenant dans une chaîne de traitements complexe. Il nécessite autant qu'il permet la circulation de certaines données de paiement pour la réalisation des transactions. C'est d'ailleurs là la première caractéristique du modèle de paiement à trois coins, qui semble être le schéma le plus minimaliste et consiste en un échange d'information entre le porteur de la carte, le bénéficiaire du paiement (un commerçant par exemple), et la banque lorsque cette dernière est à la fois celle du bénéficiaire et du porteur de la carte. Si la collecte, la circulation, le transfert ou le partage de données de paiement ne font pas l'objet d'un encadrement spécifique par le RGPD, il s'agit d'opérations de traitement de données personnelles devant à ce titre répondre à l'ensemble des exigences de cette réglementation.

Comme pour tout traitement de données personnelles, un tel traitement implique notamment la nécessité de poursuivre une finalité déterminée, explicite et légitime, mais aussi l'exigence d'une **base légale** valable. Comme pour l'application du principe de minimisation, c'est la finalité qui permet de déterminer la base légale applicable au traitement.

En effet, pour être licite, un traitement doit être fondée sur l'un des fondements mentionnés à l'article 6 du RGPD. En matière de données paiement, les bases légales les plus fréquentes sont l'exécution d'un contrat auquel la personne concernée est partie, le fondement de l'intérêt légitime, le consentement des personnes concernées, le respect d'une obligation légale à laquelle le responsable de traitement est soumis. Outre des conditions de validité propres, les bases légales retenues par le responsable de traitement déterminent le cas échéant l'exigence de garanties complémentaires. (voir encadré).

ZOOM SUR...

Différentes bases légales[63] possibles pour un traitement de données de paiement

Parmi les différentes bases légales possibles prévues par l'article 6 du RGPD, un traitement de données personnelles dans le domaine des paiements peut reposer sur quatre d'entre elles :

L'exécution d'un contrat :
https://www.cnil.fr/fr/le-contrat-dans-quels-cas-fonder-un-traitement-sur-cette-base-legale.

Il peut s'agir des traitements poursuivant la finalité de réalisation d'un paiement dans le cadre d'un contrat de vente conclu entre un commerçant et son client. Attention, l'appréciation objective de la condition de nécessité signifie qu'il ne suffit pas que le contrat en question prévoie ce traitement pour pouvoir être considéré comme nécessaire à l'exécution du contrat. Ainsi, par exemple, les traitements poursuivant des finalités de prospection commerciale n'apparaissent pas nécessaires à l'exécution d'un contrat de vente.

suite page 60 >

63 - « Les bases légales », cnil.fr

L'intérêt légitime :
cnil.fr/fr/les-bases-legales/interet-legitime

Il peut a priori concerner des traitements visant à garantir la sécurité du réseau et des informations, mis en œuvre à des fins de prévention de la fraude, ou nécessaires aux opérations de prospection commerciale auprès de clients d'une société. Au regard de la complexité du secteur des paiements et de l'opacité de son fonctionnement du point de vue des personnes concernées, il convient d'apprécier les attentes raisonnables des personnes avec prudence, particulièrement à l'égard des acteurs ne disposant pas d'une relation directe avec ces dernières. La sensibilité particulière des données de paiement rend une grande partie de leurs traitements particulièrement intrusifs, notamment lorsqu'ils impliquent un profilage ou un croisement avec d'autres données, ce qui a pour effet de limiter la possibilité de recourir à cette base légale de l'intérêt légitime. Au titre des mesures compensatoires, il peut être prévu, pour un traitement de profilage des comportements d'achat en ligne des individus, un droit d'opposition inconditionnel et surtout pouvant être exercé avant que le traitement n'ait lieu, au bénéfice des personnes, afin de leur permettre de faire cesser le profilage dont ils font l'objet.

Le consentement :
cnil.fr/fr/les-bases-legales/consentement

Il peut fonder un traitement portant sur des données de paiement. Attention, refuser de consentir à un traitement qui n'est pas nécessaire à l'exécution du contrat ne devrait pas avoir de conséquence sur son exécution ou sur la prestation du service (conformément à l'article 7.4 du RGPD). Par exemple, un responsable de traitement fournissant un système de paiement à destination de personnes concernées recueille le consentement de ses clients pour l'utilisation de leurs données de transaction à des fins de personnalisation de la publicité. Le consentement pourrait être considéré comme libre si le refus éventuel de la personne concernée n'impacte pas l'utilisation de son système de paiement. Il en irait de même pour une banque qui peut valablement recueillir le consentement de ses clients pour recevoir des offres personnalisées de partenaires commerciaux, liées à l'utilisation de leur carte bancaire, lorsque le refus n'a pas d'incidence sur la fourniture du compte courant et de la carte bancaire.

Enfin, certains traitements peuvent être nécessaires au respect, par le responsable de traitement, d'obligations légales qui lui incombent.
cnil.fr/fr/les-bases-legales/obligation-legale
notamment en matière de lutte contre le blanchiment et le financement du terrorisme.

La réutilisation des données de paiement

Lorsqu'un responsable de traitement envisage de traiter des données personnelles pour une finalité autre que celle pour laquelle elles ont été collectées, le RGPD encadre spécifiquement ces **traitements ultérieurs**. Le principe, posé par l'article 6.4 du RGPD, est que le consentement de la personne concernée doit être recueilli pour que ces traitements soient licites, à moins que ce traitement ne soit nécessaire à une obligation légale, ou qu'il ne s'agisse d'une finalité compatible avec celle qui motivait initialement la collecte des données. Afin d'apprécier la compatibilité de cette finalité ultérieure, plusieurs facteurs doivent être pris en compte, tels que le lien entre les finalités, le contexte de la collecte, la nature des données, les conséquences possibles du traitement ultérieur envisagé pour les personnes concernées, ou encore l'existence de garanties appropriées comme le chiffrement ou la pseudonymisation.

En matière de paiement, les finalités compatibles devraient par conséquent être appréciées très strictement, compte tenu de la sensibilité particulière des données en cause. Ainsi, il pourrait être envisagé de considérer que traiter ultérieurement des données de paiement afin de produire des analyses statistiques permettant d'améliorer le système de paiement mis en œuvre par un responsable de traitement est une finalité compatible ne nécessitant pas le recueil du consentement de la personne concernée lorsque des garanties appropriées sont mises en place.

À l'inverse, la réutilisation par un réseau de carte bancaire d'un historique de transaction pour déterminer les habitudes de consommation de la personne et revendre ces données à un établissement de crédit souhaitant enrichir le profil de ses futurs emprunteurs n'apparaît pas comme étant une finalité compatible, compte tenu des conséquences pour la personne concernée et du caractère excessif de l'opération au regard de ses attentes raisonnables supposées vis-à-vis du commerçant. Le consentement de cette dernière serait donc requis pour pouvoir envisager de tels traitements ultérieurs.

En matière de réutilisation des données, certaines réglementations sectorielles peuvent imposer des limitations s'additionnant aux critères posés par le RGPD. C'est notamment le cas de la DSP2 dont il résulte (notamment de ses articles 66 et 67) que toute finalité autre que la fourniture d'un service d'information sur les comptes ou d'un service d'initiation de paiement, n'est pas une finalité compatible pour les prestataires de ces services. Ces derniers doivent donc recueillir le consentement de la personne concernée pour traiter ces données à d'autres fins (à moins que ces traitements ultérieurs résultent du droit de l'Union ou d'un État membre conformément à l'article 6.4 du RGPD).

La conservation des données de paiement

En application du principe de limitation de la conservation, toute donnée personnelle ne doit être conservée que pendant une durée nécessaire au regard des finalités pour lesquelles elle est traitée. Il est donc important de raisonner par finalité (article 5.1 e) du RGPD). Un responsable de traitement doit définir et respecter une durée de conservation proportionnée à la finalité du traitement mis en œuvre. Une durée de conservation adéquate permet notamment de limiter les incidences considérables sur les personnes concernées en cas de détournement de données bancaires, ou de fraude à la carte bancaire.

En matière de paiement, il convient de distinguer la conservation de données justifiée par la **réalisation du paiement** des conservations justifiées par **d'autres finalités**, telles que des fins de preuve des transactions réalisées ou de facturation.

À titre d'exemple, la CNIL a déjà eu l'occasion de se prononcer sur certaines durées de conservation en matière de paiement à distance par carte bancaire dans sa délibération n°2018-303 récemment modifiée[64] :

- Ainsi, la CNIL estime que pour la **réalisation d'un paiement unique**, la conservation des données de paiement peut se justifier jusqu'au paiement complet ou jusqu'à la réception du bien ou à l'exécution de la prestation de service (voire jusqu'à la fin du délai de rétractation prévu pour les ventes de biens et fournitures de prestations de services à distance). En cas d'abonnement avec tacite reconduction, la donnée peut être conservée jusqu'à la dernière échéance de paiement.

- Pour la **gestion des réclamations**, les données de paiement peuvent être conservées 13 mois suivant la date de débit ou 15 mois en cas de cartes de paiement à débit différé. Les données ainsi conservées à des fins de preuve doivent être conservées en archive intermédiaire et n'être utilisées qu'en cas de contestation de la transaction. De manière plus générale, l'archivage intermédiaire devrait être envisagé à chaque fois qu'il est possible, par tout responsable de traitement. Ce procédé est en effet une mesure technique contribuant à assurer la sécurité des données traitées.

- À l'inverse, certaines données ne doivent être conservées au-delà de la réalisation de la transaction. C'est le cas du cryptogramme d'une carte de paiement, dont la conservation n'est pas justifiée.

Enfin, **la dématérialisation des tickets** de caisse ou de paiement étant régulièrement envisagée par les acteurs du secteur des paiements, il convient de préciser que cette dématérialisation ne saurait avoir pour effet de justifier une durée de conservation plus longue ou la mise en œuvre d'autres traitements au regard d'autres finalités, notamment de prospection commerciale. Ces traitements devraient en tout état de cause respecter les conditions de licéité précédemment décrites, notamment en matière de traitements ultérieurs. À titre d'exemple, une adresse électronique recueillie à des fins d'envoi d'un ticket de caisse ou de paiement dématérialisé ne saurait être utilisée à des fins de prospection commerciale sans respecter les principes en la matière (à savoir le recueil du consentement de la personne concernée, ou l'information et la possibilité de s'opposer préalablement au moment de la collecte s'agissant de prospection concernant des produits ou services analogues à ceux déjà fournis par l'entreprise), la finalité de prospection commerciale et la finalité d'envoi des tickets de manière dématérialisée étant deux finalités bien distinctes.

Sur ce sujet, la CNIL contribuera aux discussions sur le décret d'application de l'article 49 de la loi n° 2020-105 du 10 février 2020 relative à la lutte contre le gaspillage et à l'économie circulaire, qui prévoit d'interdire l'impression systématique des tickets au 1er janvier 2023.

64 - « Le paiement à distance par carte bancaire », 28 février 2019, cnil.fr

ZOOM SUR...

Conservation des données de carte à des fins de facilitation des achats ultérieurs

Le principe de limitation des finalités prévu à l'article 5.1 b) du RGPD impose de manière générale au responsable de traitement de ne pas utiliser les données traitées et collectées à d'autres fins que celles initialement prévues. En principe, les commerçants doivent donc recueillir le consentement de leurs clients à la conservation de leurs données bancaires au-delà d'une transaction pour faciliter leurs achats ultérieurs. Ce consentement ne se présume pas et doit prendre la forme d'un acte de volonté univoque, par exemple au moyen d'une case à cocher. Il doit également être susceptible d'être retiré à tout moment par la personne concernée.

Toutefois, dans certains cas, la souscription à un abonnement complémentaire peut témoigner de la volonté du client de s'inscrire dans une relation commerciale régulière avec le commerçant en achetant fréquemment sur son site internet. Dans ce cas, ces commerçants peuvent envisager de conserver par défaut les données bancaires saisies par les clients adhérents à ces abonnements complémentaires, sur le fondement de leur intérêt légitime. Les conditions de cette conservation par défaut sont détaillées dans la délibération de la CNIL à ce sujet[65] et impliquent notamment une information préalable suffisamment complète des personnes concernées, la possibilité de s'opposer facilement et à tout moment à cette collecte ou conservation, ainsi que la mise en œuvre de mesures de sécurité appropriées.

LA SÉCURITÉ DES DONNÉES DE PAIEMENT

Du point de vue de la sécurité des données, les pratiques (et les modèles d'affaires) apparaissent hétérogènes, notamment pour les paiements en ligne où la circulation en clair des données de paiement présente des risques pour les personnes.

En outre, les questions de sécurité sont démultipliées dans un cadre de numérisation toujours plus important, qui se matérialise par la volonté de trouver des solutions compatibles avec une multitude de terminaux, qu'il s'agisse aujourd'hui de terminaux mobiles ou demain d'objets connectés en capacité d'initier des paiements.

Ainsi, indépendamment des niveaux de sécurité rendus obligatoires dans les environnements de paiement situés au plus proche des organismes financiers, il est primordial que chaque acteur prenne la juste mesure du **besoin de sécurisation** des données de paiement ou des données d'achat. En effet, tous les acteurs doivent faire face à une évolution massive des attaques, notamment par le biais de rançongiciels. À ces attaques criminelles ayant pour but principal d'extorquer une somme financière à l'organisme visé ou d'effectuer un chantage, s'ajoute souvent désormais une exfiltration des données dans le but de réaliser un effet de levier dans l'obtention des sommes demandées en échange d'une clé de déchiffrement des données rendues indisponibles. Cette exfiltration de données a pour finalité indirecte de permettre le cas échéant aux cybercriminels la revente desdites données.
Parallèlement, la multiplication des supports de paiement

65 - « Le paiement à distance par carte bancaire », 28 février 2019, cnil.fr. Voir aussi la décision du Conseil d'État « Cdiscount », 10/9 CHR du 10 décembre 2020, n°429571.

peut conduire à de nouveaux schémas d'attaque reposant sur une mauvaise gestion de la sécurité d'acteurs nouveaux venus sur le marché du paiement : ainsi, depuis deux ans, la CNIL a pu constater le développement d'attaques par « bourrage d'identifiants » (ou « *credential stuffing* » en anglais) consistant à tenter de se connecter à un compte avec des couples identifiants/mots de passe ayant préalablement fait l'objet de fuites de données[66]. Cette technique permet à certains attaquants de se connecter à des « cagnottes » de chaînes de distribution et de récupérer les quelques dizaines ou centaines d'euros qui y sont stockées. Plus largement, la CNIL a reçu en 2020 2 825 notifications de violations de données dont 311 pour les activités financières et d'assurance, en croissance de 5 % en 2020 par rapport à 2019 (24 % pour l'ensemble des notifications).

Les solutions d'aujourd'hui, comme celles de demain, doivent être pensées dans un contexte de forte criminalité numérique, celle-ci n'ayant de cesse de s'accroître et de s'adapter. En ce sens, il est important d'intégrer au plus tôt dans les projets et ce durant tout le cycle de vie de la donnée, les enjeux de sécurité. On peut penser notamment aux **objets connectés** dont il a été souvent constaté qu'ils avaient des niveaux de sécurité insuffisants, notamment pour des questions de réduction des coûts.

Les attentes des clients demandant plus de rapidité dans l'exécution du service ou sa mise à disposition, la volonté d'un parcours client simplifié, ne sont pas des attentes incompatibles avec un niveau de sécurité adéquat. Ainsi, comme évoqué plus haut dans le présent Livre blanc, la CNIL s'interroge sur les impacts de l'utilisation de l'IBAN original du client et de sa diffusion en vue de permettre un paiement instantané dans le cadre du SCT Inst. En effet, tout comme cela est le cas de certaines solutions de paiements mobiles sans contact aujourd'hui, la tokenisation des numéros de carte bancaire en vue de réaliser un paiement semble plus à même de répondre aux enjeux de sécurité. À cette tokenisation s'ajoute une durée de vie limitée de la donnée, limitant un usage ultérieur en cas de piratage des environnements d'un commerçant par exemple.

La pratique de la tokenisation apparaît dès lors à même de proposer une meilleure protection des données de paiement et de sécurité. Elle apporte également une protection indéniable aux porteurs de carte. En effet, en cas de piratage malheureux d'un acteur de la chaîne de traitement, qu'il est nécessaire de prendre en compte dans l'analyse de risques, ce numéro n'est plus utilisable et propose une pseudonymisation en complexifiant le lien avec le porteur. Cette solution sécurise ainsi financièrement le porteur, tout en protégeant celui-ci du point de vue de sa vie privée. Elle protège également l'organisme de paiement en limitant le risque de paiement frauduleux et de réutilisation d'un numéro de carte pouvant être réutilisé à plusieurs reprises à l'insu du porteur.

La CNIL élaborera des recommandations pratiques en direction de l'écosystème et des régulateurs s'agissant de la tokenisation de ces données : champ des données concernées, techniques à utiliser, bonnes pratiques… (voir page 84).

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), une donnée jetable générée aléatoirement appelée jeton (token), dont l'utilisation est limitée à un usage unique et qui peut être borné dans le temps.

« Il est primordial que chaque acteur prenne la juste mesure du besoin de sécurisation des données de paiement ou des données d'achat »

66 - « La violation du trimestre : attaque par *credential stuffing* sur un site web », 12 janvier 2021, cnil.fr

La parole à...

VALÉRIE FASQUELLE,

BANQUE DE FRANCE

> ***Il est absolument nécessaire de sensibiliser les utilisateurs aux risques associés à la divulgation de leurs données bancaires***

Valérie FASQUELLE, *diplômée de l'Institut d'Études Politiques de Paris et de l'Université de Paris-Dauphine, a été Directrice des Infrastructures, de l'Innovation et des Paiements à la Banque de France. Au travers des différentes responsabilités qu'elle a exercées, Valérie FASQUELLE a été au cœur des grands projets d'infrastructures conduits par l'Eurosystème entre 2004 et 2015 comme Target 2 et Target 2 Securities. La Banque de France a un intérêt tout particulier dans le domaine de la monnaie et des paiements : elle dispose en particulier d'un mandat de surveillance de la sécurité des moyens de paiement scripturaux qui lui a été conféré par la loi.*

Au-delà des aspects touchant à la protection de la vie privée des citoyens, les données de paiement soulèvent des enjeux évidents de lutte contre la fraude, mais également de souveraineté. Valérie Fasquelle, ancienne Directrice des infrastructures, de l'innovation et des paiements à la Banque de France, nous présente ces enjeux auxquels fait face le régulateur à l'heure actuelle.

Quelles sont les données de paiement sensibles et où se trouvent-elles dans notre quotidien ?

Les données de paiement sensibles sont des données « susceptibles d'être utilisées pour commettre une fraude » selon la DSP2. Cependant, la multiplication des usages numériques et les promesses d'une expérience de paiement toujours plus fluide ont participé à la dissémination de ces données de paiement (par exemple, enregistrement des données de paiement dans le navigateur internet, l'application mobile ou sur les sites marchands). En outre, les acteurs de paiement comme les Fintechs cherchent de plus en plus à exploiter le potentiel des données de transaction pour proposer des services plus innovants et plus adaptés à leurs clients. La dissémination des données de paiement auprès d'une multitude d'acteurs constitue donc une tendance structurante de l'industrie des paiements. Celle-ci concourt en retour à la recherche continue de vulnérabilités par les cyber-fraudeurs qui déploient des méthodes de plus en plus sophistiquées pour subtiliser les données de paiement sensibles.

Quels sont les moyens pour empêcher l'exploitation de ces données de paiement à des fins de fraude ?

La lutte contre la fraude repose en partie sur la capacité à protéger les données de paiement sensibles à tous les niveaux. Des standards de sécurité et des règlementations sur les services de paiement (notamment le RGPD et la DSP2 respectivement) encadrent les professionnels et les activités connexes au paiement et définissent l'ensemble des exigences nécessaires à la protection, aux

traitements et aux échanges de ces données. Néanmoins, il est absolument nécessaire de sensibiliser les utilisateurs aux risques associés à la divulgation de leurs données ou à l'utilisation de sites internet et d'applications de sources non fiables afin qu'ils deviennent les premiers acteurs dans la lutte contre la fraude.

Concrètement, quels sont les apports de la DSP2 en matière de sécurité des données pour les consommateurs ?

La DSP2 a permis de renforcer la sécurité des accès aux comptes de paiement des utilisateurs de la même façon qu'elle a renforcé la sécurité des paiements au sens large : par l'introduction d'une obligation de recours à l'authentification forte du titulaire du compte. Là où un simple mot de passe statique suffisait auparavant pour se connecter à sa banque en ligne ou mobile, la règlementation prévoit désormais le recours à un second facteur d'authentification : par exemple, un mot de passe reçu par SMS, ou un déverrouillage par empreinte biométrique. La règlementation tient toutefois compte du besoin de trouver un juste équilibre entre simplicité et sécurité : pour l'accès aux comptes, l'authentification forte n'est requise qu'une fois tous les 90 jours, dans la mesure où les risques sont bien plus réduits que dans le cadre d'opérations de paiement, par définition plus sensibles à la fraude et donc soumises à une authentification forte de manière quasi systématique.

La DSP2 a aussi permis d'encadrer les pratiques d'accès aux comptes de paiement par des acteurs tiers, appelés agrégateurs d'informations sur les comptes, qui offrent des services de présentation de l'état des comptes et des dépenses généralement assortis d'offres à valeur ajoutée en matière de conseil en gestion de budget (par exemple : alertes, propositions d'offres bancaires plus adaptées ou de crédit…). Ces acteurs opéraient précédemment en-dehors de tout cadre règlementaire au moyen de techniques dites de *webscrapping* : ils collectaient les identifiants bancaires de leurs clients et les utilisaient pour se connecter à la banque en ligne de ceux-ci pour y récupérer les relevés de comptes ou d'opérations. La DSP2 assujettit désormais ces acteurs à une obligation d'enregistrement auprès des autorités bancaires (l'ACPR en France), et prévoit que le banques mettent en place des interfaces dédiées (ou API) pour permettre l'accès aux données de leurs clients sans recourir aux techniques de *webscrapping*. Ainsi, la DSP2 a permis à la fois de restaurer le caractère strictement personnel des identifiants de connexion des titulaires de compte, tout en accompagnant le développement d'une nouvelle activité fondée sur l'exploitation des données dans un cadre sécurisé, avec des exigences sécuritaires, des règles et des responsabilités bien définies.

Vous mentionnez également des enjeux de souveraineté concernant la gestion des données de paiement : pouvez-vous nous en dire plus ?

La réalisation d'une opération de paiement en Europe dépend de plus en plus souvent de la participation d'acteurs tiers (ex : Visa, Apple Pay, Google Cloud etc.) souvent établis en dehors de l'Union européenne. Dans un contexte de croissance continue de l'usage des moyens de paiement scripturaux, cela peut constituer une vulnérabilité pour l'indépendance stratégique de l'économie européenne, au regard du risque de continuité, mais également en cas de menaces de rétorsions ou de transfert non motivé de données à un tiers (par exemple dans le cadre d'opérations de renseignement ou d'enquêtes judiciaires). Par ailleurs, au-delà du strict mandat de surveillance des banques centrales, la dépendance aux acteurs non-européens rend plus incertaine la correcte mise en œuvre des règles européennes de protection des données personnelles (parmi lesquelles figurent les données de paiement). Enfin, dans le contexte de la révolution numérique, les activités de paiement fournissent deux actifs stratégiques (des données et une relation client quotidienne) indispensables au maintien de la compétitivité européenne.

Quelles solutions préconisez-vous afin de mieux prendre en compte la dimension de souveraineté européenne dans la conservation, le traitement et l'échange de données de paiement ?

La question du traitement et de la conservation des données suscite un intérêt croissant, et à juste titre. Nous suivons avec attention les projets de la Commission européenne dans le cadre de sa stratégie pour les données, dont plusieurs initiatives doivent être précisées en 2021. En France, le Comité national des paiements scripturaux (CNPS) – que préside la Banque de France – s'est fait l'écho des craintes de la Place française, et promeut la mise en place d'une politique de localisation des données de paiement sur le territoire européen, tel que le préconise un rapport du Conseil Général de l'Économie remis au Ministre de l'économie en février 2020[67].

67 - LEMERY S. et STEINER R., Mise en œuvre d'une politique de localisation des données critiques de paiement en Europe, Rapport n°2019/16/CGE/SG, 2020, economie.gouv.fr.

LA LUTTE CONTRE LA FRAUDE

Dans le secteur des paiements et plus particulièrement des paiements en ligne, les traitements à des fins de lutte contre la fraude concentrent une grande partie des points d'attention précédemment évoqués en matière de protection des données à caractère personnel.

Tout d'abord, s'agissant de la qualification des organismes, il semble que plusieurs acteurs de la chaîne soient techniquement en mesure de traiter les données de paiement pour cette finalité. Il peut notamment s'agir du commerçant, de la passerelle de paiement, des prestataires de service de paiement, du réseau de carte bancaire ou du gestionnaire de compte.

La lutte contre la fraude pose ensuite la question de la minimisation des données. En effet, seules les données nécessaires à ces opérations peuvent être traitées, ce qui suppose une analyse au cas par cas des données susceptibles de pouvoir être traitées, au regard du contexte de la fraude, des données déjà disponibles et des autres mécanismes d'ores et déjà mis en place pour éviter de telles fraude (par exemple une authentification renforcée). Un équilibre doit donc être trouvé entre proportionnalité du traitement et efficacité des dispositifs. D'une manière générale, la CNIL privilégie des dispositifs qui s'appuient sur la sécurisation des moyens de paiement ou d'authentification aux traitements cherchant à multiplier les collectes de données pour évaluer le risque de fraude : il est en effet bien plus difficile de respecter ses obligations d'information et de droits accordés aux personnes en cas de collecte massive de données.

Un équilibre doit donc être trouvé entre proportionnalité du traitement et efficacité des dispositifs

À cet égard, dans le domaine des paiements en ligne, une attention particulière doit être portée à la possible application de la directive ePrivacy, et notamment de sa transposition à l'article 82 de la loi Informatique et Libertés, qui exige le recueil d'un consentement auprès de l'utilisateur afin de permettre l'action tendant à accéder, par voie de transmission électronique, à des informations déjà stockées dans son équipement terminal de communications électroniques, ou à inscrire des informations dans cet équipement. En d'autres termes, l'utilisation d'un **traceur sur le terminal** d'une personne concernée pour collecter des données nécessite le consentement de la personne concernée, et ce, indépendamment de la base légale retenue pour traiter ultérieurement les données personnelles ainsi collectées.

Cette obligation de collecter le consentement concerne notamment les services dit de *scoring* contextuels, reposant sur des données liées au contexte de la transaction comme l'adresse IP, les données de localisation, les données du navigateur utilisé etc., mais aussi les *scorings* par **biométrie comportementale**, c'est-à-dire reposant sur les données de dynamique de frappe de clavier, des mouvements de la souris, des habitudes d'utilisation du terminal, ou de l'utilisation d'écrans tactiles.

Comme on l'a vu, ce deuxième type de *scoring* peut également être concerné par l'encadrement spécifique des données biométriques par le RGPD (article 9), dès lors qu'il s'agit de traiter les caractéristiques comportementales propres à la personne concernée pour contribuer à son identification unique. Le consentement explicite de la personne concernée, ou l'adoption d'un règlement type par la CNIL pourrait se révéler nécessaire pour permettre ces traitements.

Par ailleurs, s'agissant de la base légale de ces traitements, s'il semble difficile de considérer que les traitements de lutte contre la fraude sont nécessaires à la réalisation du paiement ; l'intérêt légitime semble la base légale la plus pertinente pour ce traitement, à condition que ses conditions de validité, telles que décrites plus haut, soient remplies. Il suppose toutefois que ces traitements

s'inscrivent dans les attentes raisonnables des personnes concernées et qu'un certain nombre de garanties visant à protéger les intérêts, droits et libertés des personnes concernées soient mises en place.

Une autre difficulté des traitements de lutte contre la fraude en matière de paiement provient du partage de données entre différents responsables de traitement, voire même de recours à des outils reposant sur la mutualisation de données. **Ces mutualisations de données** soulèvent plusieurs enjeux en matière de protection des données, à commencer par la qualification des acteurs. Il semble que l'organisme opérant la mutualisation des données doive en principe être qualifié de responsable de traitement, dès lors que ce dernier détermine généralement les données qu'il mutualise, dans quels buts et par quels moyens (déterminant ainsi la finalité et les moyens du traitement). La question de la répartition des rôles entre les organismes alimentant cette base, et les acteurs en tirant profit (notamment en interrogeant la base mutualisée), est également essentielle. Lorsque plusieurs acteurs contribuent à déterminer les moyens du traitement (par une décision commune ou des décisions convergentes) et poursuivent une même finalité (telle que celle de lutter contre la fraude), la responsabilité conjointe doit être envisagée et encadrée dans les conditions prévues par l'article 26 du RGPD.

À titre d'exemple, en matière d'établissement d'une liste de personnes présentant un risque de fraude, la CNIL estime généralement qu'une **information** en deux niveaux est pertinente :

- L'information générale des personnes concernées sur l'existence d'un dispositif de lutte contre la fraude pouvant conduire à l'inscription sur une liste des personnes présentant un risque de fraude.

- En cas de détection d'une anomalie, d'une incohérence ou d'un signalement susceptible de relever d'une fraude, le responsable de traitement a la possibilité d'inscrire une personne sur une liste de personnes présentant un risque de fraude. La personne concernée, susceptible d'être inscrite sur cette liste, pourra être contactée, selon le type de fraude suspectée (interne ou externe), pour apporter des éléments complémentaires. Au terme des investigations, en cas de décision prise produisant des effets juridiques (tels que le refus de procéder au paiement ou à la conclusion d'un contrat de vente), une information écrite et individuelle doit être adressée, précisant les mesures prises par le responsable de traitement et lui donnant la possibilité de présenter ses observations, sans préjudice des dispositions légales applicables.

En matière de base mutualisée, il apparaît que tant la transmission des données pour constituer et alimenter cette base que l'utilisation du résultat de cette mutualisation doivent être portées à la connaissance des personnes concernées. À titre d'exemple, dans une délibération autorisant la mise en œuvre d'une base mutualisée à des fins de lutte contre la fraude dans la vente en ligne[68], la CNIL avait retenu que l'information était délivrée sur les formulaires de collecte des e-commerçants utilisant (et alimentant) ce traitement.

Le respect des conditions encadrant les traitements de données ultérieurs précédemment décrites, ainsi que l'exercice des droits des personnes concernées, présentent également une importance particulière en matière de lutte contre la fraude. À ce titre, il apparaît essentiel que les responsables de traitement prévoient des moyens adaptés afin d'assurer l'effectivité de l'exercice des droits, notamment en clarifiant les rôles respectifs des acteurs, lorsque ces derniers se trouvent dans une situation de sous-traitance (conformément à l'article 28 du RGPD) ou de responsabilité conjointe (article 26 du RGPD).

Enfin, l'article 22 du RGPD encadre toute **décision entièrement automatisée** prise sur le seul fondement d'un traitement, notion qui pourrait être illustrée, par exemple, par la pratique consistant à refuser une transaction sur le seul fondement d'un score établi automatiquement et sans intervention humaine. À cet égard, le RGPD impose une série de conditions à appliquer au cas par cas, et notamment le droit, pour les individus concernés, de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé et produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire.

68 - « Délibération n° 2013-367 autorisant la société ONEY TECH à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité la lutte contre les risques de fraude au paiement sur internet », 28 novembre 2013, légifrance.fr.

ZOOM SUR...

La dérogation à l'authentification forte pour les paiements électroniques ayant un risque de fraude

L'un des objectifs de la DSP2 est de renforcer la sécurité des paiements. À cet égard, elle instaure (en son article 97) une obligation d'authentification forte des paiements électroniques initiés par le payeur. Cette obligation incombe aux prestataires de services de paiement, et l'authentification forte est définie comme 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).

Cependant, le règlement délégué (UE) 2018/389 de la Commission du 27 novembre 2017 chargé de préciser les exigences en matière de sécurité et d'authentification prévoit plusieurs exceptions à l'obligation d'authentification forte, dont l'une implique un certain nombre de traitements de données à caractère personnel. Plus précisément, il prévoit (en son article 18) que les prestataires de services de paiement sont autorisés à ne pas appliquer l'authentification forte du client lorsque le payeur initie une opération de paiement électronique à distance que le prestataire de services de paiement considère comme présentant un faible niveau de risque. Ce niveau de risque fait l'objet d'une notation impliquant la prise en compte d'un certain nombre de données personnelles relatives au paiement en cause et plus généralement au payeur. Il s'agit notamment de la localisation éventuellement anormale du payeur ou du bénéficiaire, des habitudes de dépenses antérieures de paiements du payeur, de l'historique de ses opérations de paiement et de l'identification de comportements de paiement anormaux de sa part par rapport à l'historique de ses opérations de paiement.

Conformément à l'article 94 de la DSP2, les traitements de données personnelles opérés aux fins de cette directive, tels que ceux mis en œuvre dans le cadre du protocole 3D Secure[69] (voir figure 13), sont soumis à la réglementation en matière de protection des données. Il convient donc de rappeler quelques points d'attention en la matière.

Tout d'abord, ces traitements doivent reposer sur une base légale. Outre l'existence de certaines obligations légales spécifiques, il semble que l'intérêt légitime doive être considéré comme étant la base légale la plus appropriée pour fonder ces traitements dès lors que leur finalité est de prévenir les risques de fraude dans le but de permettre une facilitation des paiements en dérogeant à l'obligation d'authentification.

Chaque responsable de traitement opérant ces traitements a donc l'obligation de s'assurer et de pouvoir justifier du respect du principe de minimisation et de mise en balance des intérêts des personnes concernées, qu'il s'agisse de la collecte des données, de leur transmission à un autre responsable de traitement, ou de leur durée de conservation.

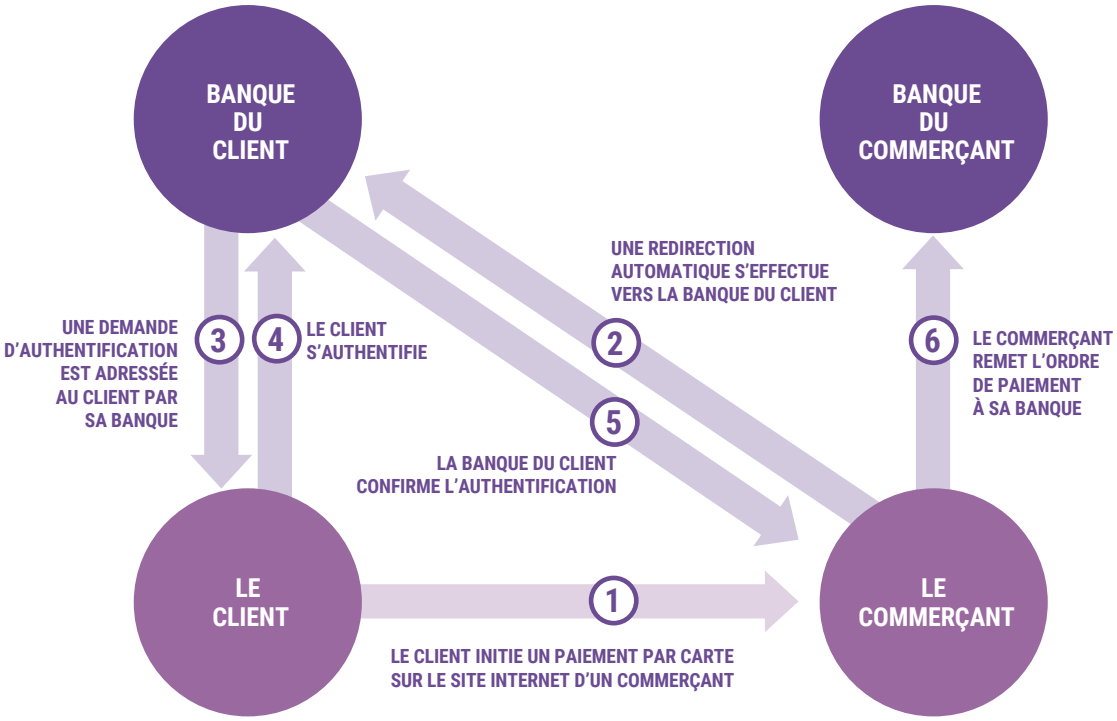
Les personnes concernées doivent être informées de l'existence de ces traitements, et pouvoir le cas échéant exercer leurs droits sur les données, telles que leur droit d'accès ou éventuellement leur droit d'opposition. À cet égard, laisser le choix aux personnes concernées de s'authentifier à chaque paiement électronique pourrait être un moyen pertinent et protecteur qui permettrait par ailleurs l'exercice d'un droit d'opposition au préalable, dès lors que les traitements relatifs à la dérogation du risque faible ne seraient plus nécessaires.

69 - Il s'agit d'un protocole de sécurité, d'authentification et de prévention de la fraude dans les transactions en ligne dont les spécifications sont déterminées par le consortium EMVco.

Figure 13

Fonctionnement du protocole « 3D Secure ».

Source : Banque de France, « Paiements et infrastructures de marché à l'ère digitale », janvier 2021, page 57



LES TRANSFERTS ET LA CIRCULATION INTERNATIONALE DES DONNÉES DE PAIEMENT : un enjeu de souveraineté pour le cadre de confiance européen ?

Les données de paiement sont susceptibles d'une circulation globale, en raison du caractère mondial de certains acteurs comme les grands réseaux de carte bancaire ou les géants du e-commerce, du poids des paiements internationaux dans une économie globalisée (des millions de transactions par jour pour des milliers de milliards de dollars en montant dans le système de compensation SWIFT) et de l'essor du commerce en ligne, dont les opérations sont plus globalisées que le commerce physique.

Ainsi, selon la Conférence des Nations-Unies sur le commerce et le développement (CNUCED), le commerce électronique de détail transfrontalier s'est élevé à quelque 440 milliards de dollars en 2019, soit une augmentation de 9 % par rapport à 2018. La part des acheteurs en ligne effectuant des achats transfrontaliers est passée de 20 % en 2017 à 25 % en 2019. Le poids des transactions transfrontalières dans le commerce en ligne a d'ailleurs justifié le lancement, en 2019, de négociations spécifiques à ce sujet dans le cadre de l'Organisation mondiale du commerce. En Europe, en 2019, la part de ventes en ligne transfrontalières représentait 23,5 % du total des ventes en ligne et si la plupart des échanges transfrontaliers en Europe (55 %) étaient générés par des acteurs de l'Union européenne, 45 % étaient le fait d'acteurs de pays tiers[70].

L'enjeu de la protection des données de paiement des citoyens européens a ainsi des implications géopolitiques indéniables et il est au cœur d'enjeux de souveraineté, à plusieurs titres. On peut penser à la souveraineté des États, au sens de leur non-soumission à d'autres États, dans l'acception juridique classique. On peut penser aussi à la souveraineté des personnes sur leurs données, selon le principe d'« autonomie informationnelle » qui sous-tend le RGPD. Avec ce qu'on peut appeler **la souveraineté en matière de données**, ces deux perspectives se rejoignent : c'est en se donnant les moyens de protéger effectivement les données personnelles de leurs ressortissants (de l'accès des autorités étrangères, de l'exploitation économique d'acteurs privés tiers, etc.) et de faire prévaloir les valeurs européennes que les États européens évitent la dépendance (technologique, économique, politique) envers d'autres États.

La souveraineté en matière de données rejoint ainsi la souveraineté numérique, selon la juriste Pauline Türk : « La notion de souveraineté numérique ne se limite donc pas à la stricte perspective juridique classique, attachée au pouvoir des États. Elle renvoie dans son acception la plus large, au pouvoir de commandement et au droit à l'autodétermination dans un monde numérique. (…) Contre la logique de patrimonialisation des données personnelles, la consécration d'un droit à l'autodétermination informationnelle permettrait de garantir le droit des individus à maîtriser l'usage et le devenir des données personnelles fournies, ainsi que les "traces" laissées par l'activité numérique. Certains droits qui en sont dérivés ont déjà été consacrés, notamment au niveau européen, par le Règlement général sur la protection des données personnelles (RGPD) entré en vigueur en 2018, ou par la Cour de justice de l'Union européenne (droit à l'oubli, au déréférencement, à la portabilité des données, au consentement, à l'information et à la rectification…). »[71].

70 - *« Cross-Border Commerce Europe publishes the second edition of the "TOP 500 Cross-Border Retail Europe": an annual ranking of the best 500 European cross-border online shops »* [en anglais], 4 juillet 2020, cbcommerce.eu.
71 - TÜRK P, professeure de droit public à l'université Côte d'Azur, « Définition et enjeux de la souveraineté numérique », *Les Cahiers français,* n° 415, mai-juin 2020.

UNE QUESTION DE L'ACCÈS DES AUTORITÉS ÉTRANGÈRES POSÉE DE LONGUE DATE

Le sujet n'est pas nouveau pour les données de paiement. Il s'est, par exemple, illustré au début des années 2000 par les craintes exprimées alors au sujet d'un programme de surveillance des transactions bancaires internationales mis en place par les États-Unis en 2001. Celui-ci s'appuyait sur un service de transactions financières interbancaires de droit belge (SWIFT[72]), initialement afin de traquer le financement des réseaux terroristes mais qui a été accusé ensuite de s'être rapidement mué en outil de surveillance des transactions financières des individus et des entreprises conduisant, notamment, le G29[73] à exprimer ses vives préoccupations.

Ainsi, dans un avis du 22 novembre 2006, il a considéré qu'en l'absence de transparence et de mécanismes effectifs de supervision, les données ainsi transférées à partir de l'Europe vers la succursale de la société SWIFT établie aux États-Unis puis de celle-ci vers les autorités américaines contrevenait aux règles européennes en matière de protection des données personnelles.

Le bon fonctionnement du système de compensation interbancaire international a conduit l'Europe à conclure avec les États-Unis en 2010 après une première version rejetée par le Parlement européen, un accord pour légaliser les transferts de données en question[74]. Cet accord a été jugé insuffisant par le G29, qui a écrit en juin 2011 au gouvernement américain déplorant notamment le défaut d'information des personnes et le manque d'effectivité de l'accord. Toutefois, le détournement du système SWIFT par les États-Unis, allégué à l'époque, a eu pour conséquence le développement de protocoles de communications financières locaux en Europe comme EBICS[75].

Dans l'affaire SWIFT, tout comme près de 15 ans après, dans l'affaire Schrems II, l'applicabilité territoriale du droit américain au sein des systèmes de paiement entre en conflit avec le champ territorial du droit européen des données personnelles, dès lors que des personnes situées en Europe sont concernées. Pour le comprendre, il faut d'abord examiner dans quelles conditions des données personnelles peuvent être transférées hors d'Europe.

L'applicabilité territoriale du droit américain au sein des systèmes de paiement entre en conflit avec le champ territorial du droit européen des données personnelles

72 - Acronyme pour *Society for Worldwide Interbank Financial Telecommunication*.
73 - Ancien groupe d'autorités de protection des données européennes, préfigurateur du CEPD.
74 - « Accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance du financement du terrorisme », Journal officiel n° L 195 du 27 juillet 2010, eur-lex.europa.eu.
75 - Acronyme pour *Electronic Banking Internet Communication Standard*.

HORS DE L'UE, UNE PROTECTION DES DONNÉES PERSONNELLES VIA LA « BULLE DE CONFIANCE »

La confiance occupe une place prépondérante en matière de données personnelles. Au sein de l'Europe, un principe de libre circulation s'applique à ces données. En revanche, lorsqu'elles sont appelées à être exportées en dehors de l'Union européenne ou de l'Espace économique européen, des règles particulières s'appliquent.

À l'instar de la Directive 95/46/CE et de la loi Informatique et Libertés du 6 janvier 1978 modifiée, le RGPD organise les conditions de transfert de données personnelles en dehors de l'Union européenne afin que celles-ci puissent continuer à bénéficier d'une protection, une fois transférées vers des pays tiers.

À ce titre, le RGPD pose le principe que les transferts vers un pays tiers sont par principe interdits (art.44), sauf si le pays tiers a été reconnu comme offrant un niveau de protection adéquat par une décision de la Commission européenne dite « décision d'adéquation » (art. 45), ou à défaut de décision d'adéquation, lorsque le transfert est encadré par des « garanties appropriées » (art. 46).

À défaut de décision d'adéquation ou de garanties appropriées, les données peuvent dans certaines situations particulières, limitativement énumérées et strictement interprétées par le Comité européen de la protection des données, être transférées sur le fondement de dérogations expressément listées par le RGPD (art. 49).

En outre, depuis mai 2018, le RGPD élargit la gamme d'outils juridiques permettant d'encadrer les transferts. Ils peuvent désormais être utilisés tant par les responsables de traitement que par les sous-traitants. En outre, il concerne aussi les transferts ultérieurs : ceux relatifs aux transferts de données depuis l'Union européenne vers un pays tiers, par exemple, puis vers un autre pays tiers ou une organisation internationale.

La personne concernée doit enfin être informée lors de la collecte de ses données de la possibilité d'un transfert en-dehors de l'UE : cette indication figure le plus souvent dans les politiques de confidentialité du service souscrit.

Transferts internationaux : la « boîte à outils » du RGPD

La décision d'adéquation est un outil facilitateur. Elle permet la libre circulation des données vers le pays tiers ou l'organisation internationale et ne requiert pas de la part de l'exportateur des données d'autres démarches (autres outils de transferts ou obtention d'une autorisation de la CNIL).

L'évaluation de l'adéquation doit avoir pour objet d'analyser que le niveau de protection des données personnelles est essentiellement équivalent à celui garanti dans l'Union européenne. Cette analyse doit être menée au regard d'une liste de critères, notamment : le respect des droits de l'homme et des libertés fondamentales, la législation pertinente relative à la protection des données personnelles, tant générale que sectorielle, y compris en ce qui concerne la sécurité publique, la défense, la sécurité nationale et le droit pénal et l'accès des autorités publiques aux données personnelles, les droits effectifs et opposables ainsi que les recours dont disposent les personnes concernées, l'existence et le fonctionnement effectif d'une autorité de contrôle indépendante (art. 45-2).

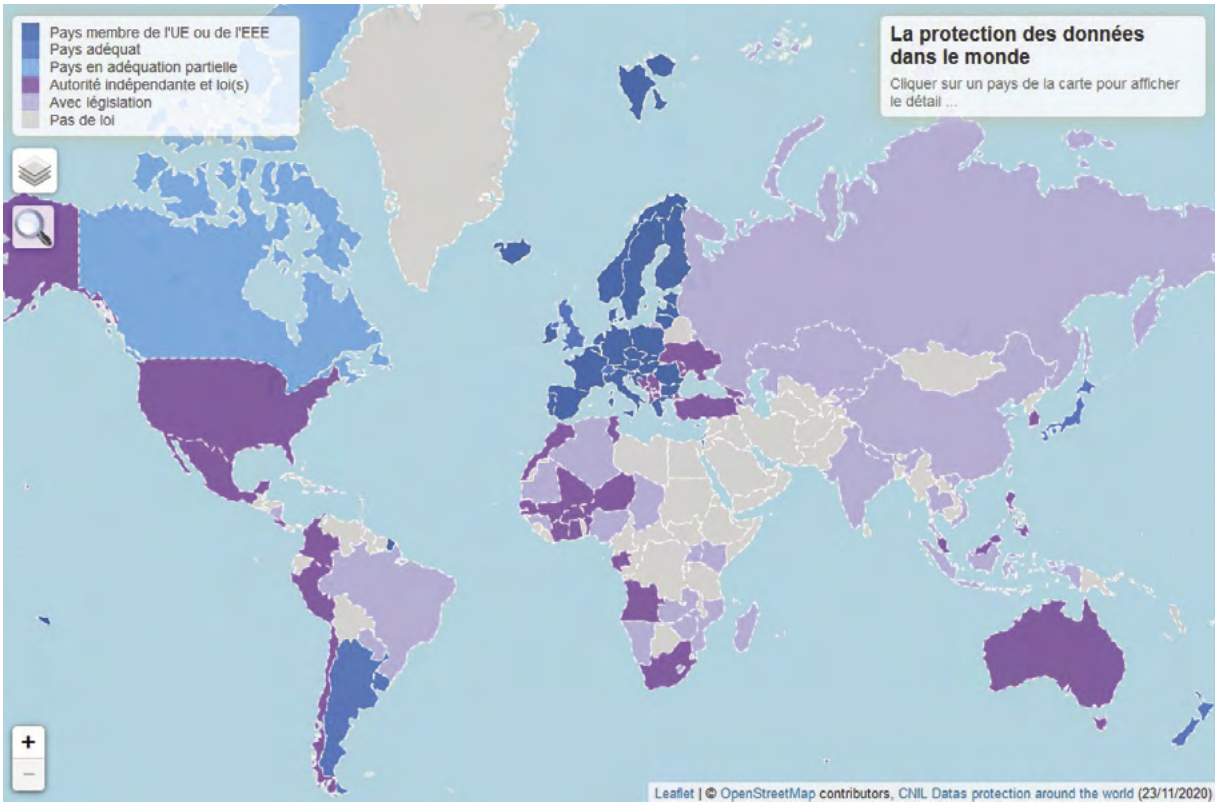
Ainsi, un prestataire de services de paiement traitant ou sous-traitant les données en Suisse ou au Japon, par exemple, est couvert par ce principe d'adéquation (voir figure 14). Attention, le pays de traitement des données n'est pas nécessairement le pays du siège du prestataire, généralement établi dans l'UE s'il veut pouvoir réaliser des opérations de paiement en Europe de par les règles sectorielles applicables.

Les décisions d'adéquation doivent faire l'objet d'un réexamen périodique, au moins tous les quatre ans, par la Commission européenne afin de tenir compte de tous les développements pertinents dans le pays tiers ou l'organisation internationale concernés. De plus, indépendamment du réexamen périodique, la Commission doit

Figure 14

Carte des pays adéquats à l'été 2021.

Source : CNIL



suivre de manière continue les développements susceptibles d'affecter et de remettre en cause ses décisions d'adéquation.

À défaut de décision d'adéquation, il est nécessaire de s'appuyer sur un des huit autres instruments juridiques d'encadrement des transferts internationaux prévus par l'article 46 du RGPD. Parmi ceux-ci, l'organisme doit opérer son choix au regard de sa nature, de sa taille, de son organisation interne, de sa maturité en matière de protection des données, de son marché concurrentiel, etc.

Parmi les outils de transfert, sont prévues **les règles d'entreprise contraignantes** (Binding Corporate Rules dites BCR) qui bénéficient d'une forte attractivité auprès des groupes internationaux auxquels elles sont principalement destinées. Ainsi, de grandes banques internationales mais aussi les grands réseaux américains de carte bancaire, dont les données sont transférées aux États-Unis, y ont recours. Par ailleurs, les mécanismes nationaux ou européens de certification approuvés (qui n'ont pas encore trouvé à s'appliquer pour les données de paiement) ont pour cible principale les TPE/PME et constituent un facteur de différenciation leur permettant d'obtenir des marchés.

Les codes de conduite prévus à l'article 40 et 41 du RGPD font aussi partie des outils de conformité qui permettent à un secteur d'activité d'accompagner la mise en conformité des professionnels à travers des recommandations pratiques et opérationnelles tout en harmonisant les pratiques au niveau du secteur. Le recours à des codes de conduite comme outils de transfert, adoptés au niveau européen par le CEPD, pourrait représenter un outil précieux dans le secteur des paiements où l'encadrement des transferts peut s'avérer complexe. En effet, les services de paiement reposent souvent sur une chaîne d'acteurs, dont les rôles respectifs sont complexes à appréhender, dont certains sont de taille mondiale, avec présence parfois de traitements ultérieurs, alors même que le risque d'accès non conforme aux règles européennes pour ce type de données est plus élevé (voir page 22).

Les clauses contractuelles types (CCT) sont un autre outil de transfert susceptible d'être utilisé. Il s'agit de modèles de clauses contractuelles adoptés par la Commission européenne permettant d'encadrer les transferts de données personnelles réalisés par des responsables de traitement vers des destinataires situés hors de l'Union européenne. Elles ont pour but de simplifier la tâche des responsables de traitement dans la mise en œuvre de

contrats de transfert. Il existe deux types de clauses adaptées à chaque situation : les transferts de responsable de traitement à responsable de traitement et les transferts de responsable de traitement à sous-traitant.

La Commission européenne a récemment adopté des clauses révisées[76] à la suite de l'arrêt de la CJUE dit « Schrems II » en juillet 2020 (Voir encadré).

ZOOM SUR...

L'arrêt Schrems II

Dans son arrêt du 16 juillet 2020, la Cour de justice de l'Union européenne (CJUE) a invalidé la décision dite « *Privacy Shield* », adoptée en 2016 par la Commission européenne à la suite de l'invalidation du « Safe Harbor », qui permettait le transfert de données entre l'Union européenne et les opérateurs américains adhérant à ses principes de protection des données sans autre formalité. La Cour a jugé que le droit américain en matière d'accès aux données par les services de renseignement (en particulier la section 702 du *Foreign Intelligence Surveillance Act* (FISA) applicable aux opérateurs de communications électroniques et l'*Executive Order* 12333 applicable aux câbles sous-marins) ne permet pas d'assurer un niveau de protection essentiellement équivalent[77] à l'Europe, en l'absence notamment de mécanismes de recours effectif disponibles pour les citoyens européens.

La Cour a, par ailleurs, précisé qu'en règle générale, les clauses contractuelles types peuvent toujours être utilisées pour transférer des données vers un pays tiers (qu'il s'agisse des États-Unis ou d'un autre pays tiers). Cependant, la CJUE a souligné qu'il incombe alors à l'exportateur et à l'importateur de données d'évaluer en pratique si la législation du pays tiers permet de respecter le niveau de protection requis par le droit de l'UE et les garanties requises par les CCT.

Si ce niveau ne peut pas être respecté, les entreprises doivent prévoir des mesures supplémentaires[78] pour garantir un niveau de protection essentiellement équivalent à celui prévu dans l'Espace économique européen et elles doivent s'assurer que la législation du pays tiers n'empiétera pas sur ces mesures supplémentaires de manière à les priver d'effectivité.

Concrètement, pour les exportateurs de données à caractère personnel vers les États-Unis (ou tout autre pays tiers), la poursuite des transferts sur la base des CCT dépendra donc des éventuelles mesures techniques et organisationnelles supplémentaires qu'ils pourraient mettre en place (exemple : chiffrement de bout en bout sans détention des clés de chiffrement, traitement fractionné ou multipartite, minimisation des accès…). L'ensemble formé par les mesures supplémentaires et les CCT, après une analyse au cas par cas des circonstances entourant le transfert, devra garantir que la législation du pays vers lequel sont exportées les données ne compromet pas le niveau de protection adéquat que les clauses et ces mesures doivent garantir. À défaut, ils sont tenus de suspendre ou de mettre fin au transfert de données personnelles. Dans le domaine des paiements, l'analyse de la législation sectorielle du pays tiers peut être indispensable pour les acteurs économique.

Cet arrêt majeur en matière de protection des données à caractère personnel a un retentissement particulièrement important. En effet, il renforce la responsabilisation prévue par le RGPD en insistant sur la nécessité pour les responsables de traitement ou sous-traitants de s'assurer de la conformité aux droits fondamentaux tels que protégés au sein de l'Union européenne de la législation des pays vers lesquels ils transfèrent des données et de la garantie effective des droits des personnes. En ce sens, l'arrêt concourt à la souveraineté en matière de données.

76 - Cf. « La Commission européenne adopte de nouveaux outils pour des échanges sécurisés de données à caractère personnel », juin 2021, ec.europa.eu.
77 - Voir en particulier le considérant 145 de l'arrêt de la Cour, la clause 4(g) de la décision 2010/87/UE de la Commission, la clause 5(a) de la décision 2001/497/CE de la Commission et l'annexe II (c) de la décision 2004/915/CE de la Commission.
78 - *« Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Version 2.0. Adopted on 18 June 2021* » www.edpb.eu.Voir aussi, sur le site web de la CNIL, la rubrique « Responsables de traitement : comment identifier et traiter des transferts de données hors UE ? » (https://www.cnil.fr/fr/responsables-de-traitement-comment-identifier-et-traiter-des-transferts-de-donnees-hors-ue).

LA LOCALISATION EUROPÉENNE DES DONNÉES DE PAIEMENT : DE LA PROTECTION À LA SOUVERAINETÉ ?

Le RGPD poursuit un double objectif de protection des données à caractère personnel et de libre circulation de ces données dans un périmètre vertueux. À ce titre, il relève d'une vision ouverte de la souveraineté : les acteurs de pays tiers qui souhaitent traiter les données des Européens peuvent le faire mais selon les règles et les valeurs européennes. Lorsqu'une législation étrangère rend cela impossible, les données doivent être traitées en Europe. Faut-il, pour les données de paiement qui présentent des enjeux particuliers en termes de vie privée, aller plus loin et imposer leur localisation systématique en Europe ? C'est ce que propose un récent rapport du Conseil général de l'économie (voir encadré page suivante).

La CNIL a récemment suivi un raisonnement similaire à propos des données de santé. *« En raison de la sensibilité et du volume des données ayant vocation à être hébergées au sein de la Plateforme des données de santé, pour lesquelles le niveau de protection technique mais aussi juridique le plus élevé doivent être assurés, y compris en matière d'accès direct par les autorités de pays tiers, la CNIL a fait part de son souhait que son hébergement et les services liés à sa gestion puissent être réservés à des entités relevant exclusivement des juridictions de l'Union européenne.*[79]»

L'obligation de sécurité des données qui pèse sur les établissements bancaires et de paiement ne découle pas uniquement du RGPD. Relevant d'un secteur particulièrement régulé, les établissements bancaires et de paiement font aussi partie de la liste des opérateurs de services essentiels (OSE) devant mettre en œuvre la directive NIS[80] qui prévoit, notamment[81], l'obligation d'appliquer des règles de sécurité spécifiques aux systèmes d'information essentiels, de notifier à l'ANSSI[82] les incidents de sécurité survenus sur ces systèmes et de se soumettre au contrôle de celle-ci.

Dans ce contexte, la localisation des données de paiement sur le territoire européen pourrait, il est vrai, aboutir à une solution permettant de conjuguer souveraineté et sécurité, tout en offrant aux citoyens un plus grand contrôle sur les données qui les concernent, et aux autorités de protection des données un plus grand contrôle sur les traitements correspondants. Elle n'est toutefois ni une condition nécessaire, comme on l'a vu, ni une condition suffisante pour garantir une bonne protection des données de paiement des Européens.

Par exemple, le CLOUD act américain de 2018 est applicable aux entités américaines traitant des données en Europe, dès lors qu'elles ont accès à ces données[83]. Le Comité européen de la protection des données a toutefois relevé à ce sujet que, à moins d'un accord international établissant des garanties, « la licéité de tels transferts de données personnelles ne peut pas être confirmée, sans préjudice de circonstances exceptionnelles dans lesquelles le traitement est nécessaire pour protéger les intérêts vitaux des personnes concernées »[84].

D'ailleurs, les recommandations de l'Autorité bancaire européenne sur l'externalisation en matière de cloud privilégient un stockage des données en Europe. Elles demandent aux établissements bancaires de « prendre des précautions particulières lorsqu'ils concluent et gèrent des accords d'externalisation convenus en dehors de l'EEE, en raison des risques potentiels pour la protection des données et pour le contrôle effectif par l'autorité de surveillance »[85].

L'ensemble de ces questions doit donc être examinée avec la plus grande attention par les responsables de traitement et sous-traitants ayant recours ou susceptibles d'avoir recours à des transferts internationaux de données de paiement. Une analyse au cas par cas, dont le préalable est la bonne identification des transferts ayant lieu sur le terrain et l'analyse de la législation du pays de destination, est nécessaire. Il est souhaitable que ces acteurs s'interrogent ensuite, notamment, sur la question de savoir si les transferts sont effectivement nécessaires à la réalisation des services et, si le transfert apparaît plutôt comme un choix, de réfléchir à des alternatives, afin de minimiser le risque d'accès non conforme aux règles européennes si le transfert apparaît plutôt comme un choix, de réfléchir à des alternatives, afin de minimiser le risque d'accès non conforme aux règles européennes.

79 - « La Plateforme des données de santé (Health Data Hub) », 9 février 2021, cnil.fr.
80 - Directive (UE) 2016/1148 du Parlement européen et du Conseil précisant les éléments à prendre en considération par les fournisseurs de service numérique pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information ainsi que les paramètres permettant de déterminer si un incident a un impact significatif.
81 - Voir décret n°2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et des systèmes d'information des opérateurs de service essentiels et des fournitures de service numérique.
82 - Agence nationale de la sécurité des systèmes d'information.
83 - C'est dans ce contexte que 13 banques européennes ont récemment rejoint la « European Cloud User Coalition » (ECUC), une initiative lancée par le groupe bancaire allemand
85 - « Recommandations sur l'externalisation vers des fournisseurs de services en nuage » (PDF, 138 ko), 28 mars 2018, eba.europa.eu.

La parole à...

RÉMI STEINER et SANDRINE LÉMERY,

CONSEIL GÉNÉRAL DE L'ÉCONOMIE

RÉMI STEINER
a exercé des responsabilités variées dans différents établissements bancaires, notamment en tant qu'administrateur et Directeur général délégué des banques Hervet et UBP (Union de Banques à Paris), dont la fusion avec le CCF a donné lieu à la naissance de HSBC France. En 2011, Rémi Steiner a rejoint le Conseil général de l'économie, alors que le champ d'expertise de cette entité, présidée par le ministre de l'Economie et des Finances, était étendu à l'ensemble des services financiers et aux activités qui s'y rattachent.

SANDRINE LÉMERY
Professeure au Conservatoire national des arts et métiers, titulaire de la chaire d'actuariat, Sandrine Lémery est également vice-présidente de l'Institut des actuaires et présidente du conseil de surveillance du Fonds de réserve pour les retraites. Elle a alterné entre 17 ans de fonctions au sein de l'autorité en charge du contrôle des assurances et 10 ans de fonctions administratives sur des sujets économiques et sociaux. Elle a notamment été première Secrétaire générale de l'Autorité de contrôle prudentiel et de résolution de 2013 à 2018.

> ***« Il existe une étroite articulation entre l'obligation de localisation des données de paiement que nous recommandons et le RGPD »***

Le Comité National des Paiements Scripturaux (CNPS) est une instance d'échanges et de discussions, où se rencontrent les représentants du secteur des moyens de paiement et les acteurs publics intéressés au développement de cette activité. Dans son rôle de coordination et d'orientation, le CNPS a approuvé le 18 février 2019 une nouvelle « stratégie nationale sur les moyens de paiement scripturaux » pour les années 2019 à 2024[86].

C'est dans le cadre de la mise en œuvre de cette stratégie que, le 19 juin 2019, le Ministre de l'économie et des finances a confié au Conseil général de l'économie une mission visant à étudier la mise en œuvre d'une politique de localisation des données de paiement en Europe.

Nous étions invités 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 des évolutions de l'offre de services de paiements, ainsi que de l'entrée en vigueur du règlement général sur la protection des données personnelles (RGPD) et de la deuxième directive sur les services de paiement (DSP2). Nous avons examiné à la lumière d'événements passés les menaces qui peuvent peser sur l'utilisation des données de paiement ; et auditionné un grand nombre d'acteurs représentatifs de la chaîne des paiements et actifs en France : organismes publics, organisations professionnelles, banques et établissements de paiement,

86 - « La stratégie nationale des moyens de paiement scripturaux 2019-2024 », publiée par la Banque de France en février 2019

entreprises du commerce, prestataires de services spécialisés dans le domaine du paiement… Le rapport que nous avons établi a publié sur le site du Conseil général de l'économie[87].

Les recommandations que nous avons formulées ne se limitent pas à la seule question de la localisation des données, il est apparu difficile de les isoler d'autres questions inhérentes aux conditions d'une indépendance européenne en matière de paiement. Toutes s'inscrivent dans la perspective de propositions susceptibles d'être portées par la France afin d'être reprises dans la réglementation européenne.

Dans le cours de nos entretiens, nous avons été sincèrement surpris de constater que l'idée d'une obligation de localisation de données suscitait une large adhésion parmi nos interlocuteurs, même au sein d'entreprises très internationales, pour autant bien sûr que cette obligation ne s'applique pas à l'échelle de la France mais à celle de l'Union européenne. Seul un très petit nombre d'acteurs internationaux s'y sont opposés, et leurs objections ne nous ont pas paru faire obstacle à ce que nous adhérions au principe d'une localisation en Europe des données de paiement.

Nous avons considéré qu'il devait exister une étroite articulation entre l'obligation de localisation que nous recommandions et le RGPD : les données de paiement que nous avons proposé de soumettre à cette obligation sont celles qui se rapportent à des paiements intra-européens effectués par des personnes physiques ou au profit de personnes physiques, donc des données personnelles au sens du RGPD. Nous avons estimé que la CNIL et les délégués à la protection des données dans les entreprises concernées étaient les mieux placés pour veiller au respect de cette règle.

D'ores et déjà, il est évident que le RGPD constitue un rempart précieux contre une utilisation inappropriée des données de paiement. Mais ce rempart n'est pas toujours suffisant : l'identification des responsabilités définies par le RGPD (responsable ou co-responsable de traitement, sous-traitant) et leur articulation ne sont souvent pas claires quand les données personnelles passent de main en main entre les acteurs successifs, souvent très nombreux, du traitement d'une opération de paiement.

Il est fréquent qu'un acteur intermédiaire de cette chaîne de paiement ne soit pas en relation directe avec le donneur d'ordre ou avec le bénéficiaire d'un paiement, et qu'il ne sache pas par ses propres moyens identifier l'un ou l'autre. Pour autant, il n'est pas fondé à considérer que les données sont anonymes, qu'elles échappent aux règles de protection des données à caractère personnel et qu'il peut les utiliser à sa guise.

Par ailleurs, même si le RGPD est en principe applicable à tous, il existe sans doute de profonds écarts en ce qui concerne la possibilité d'apprécier la conformité d'un traitement, de prendre des sanctions et d'assurer le recouvrement d'une amende, selon que le traitement résulte de l'activité « d'un établissement, d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union » ou de celle d'un acteur extra-européen.

À ce stade, les services de la Commission européenne n'ont pas explicitement pris parti en faveur d'une localisation des données de paiement en Europe. Mais les préoccupations de souveraineté qui sous-tendent cette idée conservent toute leur acuité, ainsi que le démontrent l'invalidation en juillet 2020 par la Cour de justice de l'Union européenne de la décision d'adéquation « *Privacy shield* »[88], l'initiative franco-allemande GAIA-X, l'engagement de la BCE en faveur du paiement instantané SCT Inst, ou encore le lancement par les grandes banques européennes du projet EPI (« *European Payments Initiative* »).

87 - LEMERY S. et STEINER R., *Mise en œuvre d'une politique de localisation des données critiques de paiement en Europe*, Rapport n°2019/16/CGE/SG, 2020, economie.gouv.fr.
88 - *Arrêt de la CJUE dans l'affaire C-311/18 Data Protection Commissioner / Maximillian Schrems et Facebook Ireland* (PDF, 344 ko), 16 juillet 2020, curia.europa.eu.

LE PAIEMENT EN EUROPE : UNE ACTIVITÉ DEVENUE STRATÉGIQUE

La Commission européenne a publié, en septembre 2020, une stratégie européenne pour les paiements de détail[89]. Pour la Commission, « autrefois relégués aux services de back office, les paiements ont acquis une importance stratégique et sont devenus le fluide vital de l'économie européenne ».

La Commission note que certaines des mutations importantes décrites dans ce Livre blanc pourraient remettre en question l'autonomie européenne en matière de paiements, et soutient la création du futur réseau européen de carte bancaire EPI (voir encadré page 81).

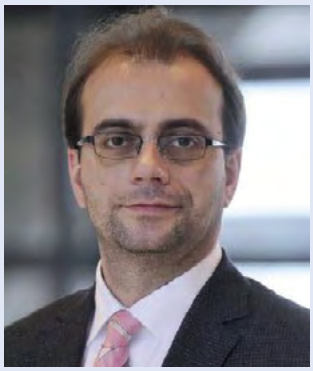
Dans le cadre de cette stratégie, elle soutient la généralisation du paiement instantané en tant que nouvelle norme, prône la normalisation européenne des QR codes pour permettre l'essor du paiement mobile, met l'accent sur la norme SEPA *« proxy Lookup »* qui permet de transférer de l'argent sans exposer son IBAN. Elle souhaite renforcer la facturation électronique, favoriser l'acceptation des paiements numériques mais aussi maintenir la disponibilité de la monnaie de banque centrale en espèces. Elle soutient l'élaboration d'un euro numérique et lancera fin 2021 la revue de la directive DSP2, notamment sur les aspects de lutte contre la fraude et sur les entités exemptées d'agrément DSP2. Elle indique aussi vouloir rendre plus transparents le destinataire, le lieu et la date du paiement. Elle veut garantir un droit d'accès, dans des conditions justes, raisonnables et non discriminatoires, aux infrastructures techniques jugées nécessaires pour soutenir la fourniture de services de paiement (ex. : puce NFC).

89 - « Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions sur une stratégie en matière de paiements de détail pour l'UE », 24 septembre 2020, ec.europa.eu ; citation page 2.

La parole à...

SÉBASTIEN RASPILLER

CHEF DE SERVICE DU FINANCEMENT DE L'ÉCONOMIE DE LA DIRECTION GÉNÉRALE TRÉSOR



SÉBASTIEN RASPILLER

Chef du service du financement de l'économie à la direction générale du Trésor. Diplômé de l'école Polytechnique. Anciennement économiste à l'Insee. Il a ensuite été membre du bureau de politique fiscale du ministère fédéral des Finances allemand, avant d'exercer diverses responsabilités à la direction générale du Trésor, notamment à la tête de la sous-direction du financement des entreprises et du marché financier.

> ***Les données de paiement : plusieurs enjeux de souveraineté essentiels***

La maîtrise des données de paiement, qui regroupent toutes les informations essentielles à la réalisation des opérations de paiement et au contexte des transactions, constitue une question majeure pour les États, avec plusieurs enjeux de souveraineté essentiels :
(i) un enjeu de souveraineté économique, avec en toile de fond le risque critique d'une cessation brutale d'activité d'acteurs tiers de la chaîne des paiements ;
(ii) un enjeu de souveraineté financière, avec la monétisation croissante des données de paiement,
(iii) un enjeu de souveraineté régalienne, lié à la capacité de protéger des données de paiement individuelles et en raison des enjeux de lutte contre le blanchiment et le financement du terrorisme ;
(iv) un enjeu de souveraineté technologique, la maîtrise des données de paiement allant de pair avec un écosystème et des services innovants.

La Stratégie nationale des moyens de paiement scripturaux 2019-2024 a ainsi identifié la maîtrise des données de paiement comme un enjeu-clef, tant au niveau de la génération, du traitement que du stockage de ces données. Ce choix n'est pas isolé dans le monde : plusieurs pays (Japon, Malaisie, Chine, Russie et Inde) se sont déjà décidés, à la lumière de ces enjeux de souveraineté, à assigner des obligations très strictes dans le cadre de politiques de (re)localisation des données assumées, avec en particulier l'obligation faite aux acteurs d'établir leurs infrastructures informatiques traitant les données de paiement sur le sol des juridictions concernées.

Caractérisée par un traitement pour partie extra-européen des données critiques de paiement, l'Europe accuse *a contrario* un retard notable. Le rapport public remis par le Conseil général de l'économie le 15 février 2020 confirme ce constat et les menaces pour la souveraineté européenne liées au contexte actuel, avec de nombreux risques : dépendance politique, entraide judiciaire limitée, espionnage, manque d'effectivité du RGPD, atteinte au *level-playing field*. Par ailleurs, l'émergence de nouvelles solutions de paiement par les grands acteurs technologiques ne fait que renforcer la crainte d'une exploitation désordonnée des données de paiement par des acteurs tiers.

Dans ce contexte, la France est déterminée à promouvoir une Europe des données de paiement véritablement indépendante. Elle soutient ainsi l'initiative European payment initiative qui devrait permettre à la fois de renforcer l'approche européenne des données de paiement (par la création d'un *scheme* pan-européen) et renforcer leur traitement lors des transactions dans le cadre d'une solution paneuropéenne de paiements. Par ailleurs, la France participe activement aux travaux du futur règle-

ment relatif aux cryptoactifs (dit « MiCA »), qui vise entre autres à assujettir les projets privés d'actifs numériques de paiement à un régime d'agrément européen exigeant, lié à une obligation d'établissement des émetteurs de cryptoactifs sur le sol européen, ce qui leur imposerait de se conformer aux normes européennes et en particulier au RGPD. Enfin, la France s'attache, dans le cadre de l'élaboration des textes de la nouvelle stratégie digitale, à convaincre ses partenaires de la nécessité d'explorer plus avant les pistes les plus prometteuses esquissées par le rapport du Conseil général de l'économie précité : il s'agirait tout particulièrement d'approfondir la séparation introduite par le règlement interchanges entre l'entité qui assure la gouvernance (définition des normes) et celle en charge de l'exécution des traitements (*processing* interbancaire), en imposant à ces derniers de localiser leurs *data centers* (stockage, lieu de traitement, *back-up*) en Europe, à l'instar d'autres juridictions étrangères.

ZOOM SUR...

Le projet EPI (European Payments Initiative - Projet interbancaire européen) et ses enjeux de conformité RGPD

En juillet dernier, un consortium de 16 banques européennes issu de 5 pays de la zone euro a lancé un projet de réseau paneuropéen de carte bancaire concurrent des réseaux américains Visa et Mastercard. La nouvelle offre veut proposer des prélèvements classiques mais aussi des virements instantanés SCT Inst et proposer un portefeuille numérique pour les paiements mobiles. Le projet comporte deux enjeux : l'unification du marché européen des paiements et la souveraineté européenne en matière de paiements (les sanctions américaines pouvant impliquer la suspension du fonctionnement des réseaux de carte). Il vise à terme une couverture mondiale, via un co-marquage avec les réseaux américains pour les paiements internationaux.

Une société de préfiguration a été fondée en Belgique et un appel à de nouveaux participants lancé pour fin 2021. Le lancement de la solution de paiement de pair à pair est prévu au premier semestre 2022, le porte-monnaie électronique pour le second semestre 2022, suivis des projets liés à la carte prévus d'ici à 2024 avec une phase de migration à partir des infrastructures existantes. La mise en place du dispositif impliquera d'importants investissements et la mise à jour des infrastructures monétiques existantes, ce qui implique de convaincre les commerçants et les consommateurs de la valeur ajoutée du projet. Si l'inclusion des virements instantanés pose la question du modèle économique du projet et de révision éventuelle du règlement « interchange » de 2015, EPI doit encore décider s'il se lance dans une adoption de la technique « *request to pay* », dans la détention de l'euro numérique voire de cryptomonnaies à l'instar de PayPal.

Pour crédibiliser l'offre d'EPI dans le contexte des paiements, la protection de la vie privée et la conformité RGPD de la nouvelle solution jouera un rôle clé. EPI a tout intérêt à faire de la protection des données un facteur de différenciation concurrentielle et un élément de sa communication, y compris envers les pouvoirs publics. EPI peut travailler à cet objectif dès à présent :

- en intégrant la règle de « *privacy by design* » (article 25 du RGPD) dans la conduite de son projet en amont notamment des choix technologiques et organisationnels qu'il aura à réaliser, pour éviter toute irréversibilité et en s'appuyant sur une étude d'impact solide ;
- en recherchant une pleine conformité à l'arrêt Schrems II par une politique d'externalisation de ses besoins en cloud et en serveurs appropriée et qui évite toute soumission à la législation américaine ;
- en recherchant, si nécessaire, le conseil d'une autorité nationale de protection des données européenne pendant la phase de structuration sur les points les plus complexes d'application du RGPD.

Au-delà, il conviendra d'éviter que la mise en place du projet EPI ne se traduise par la disparition du rôle de promotion de la sécurité actuellement assuré par l'agrément du GIE CB auprès de l'écosystème.

FEUILLE DE ROUTE POUR DES SOLUTIONS D'ACCOMPAGNEMENT ET DE PÉDAGOGIE

Dans le cadre de ses missions, la CNIL a pour objectif d'apporter aux professionnels précision et prévisibilité de sa régulation, en fournissant de la sécurité juridique en tant que de besoin. Elle souhaite également apporter au public une meilleure compréhension des enjeux de protection de la vie privée et des données personnelles et notamment, des droits conférés par le RGPD. Ces objectifs se traduisent par la publication d'instruments dits « de droit souple » (référentiels, recommandations, lignes directrices, guides pratiques, etc.) et par la mise en ligne d'informations et bonnes pratiques disponibles sur son site web. Cet accompagnement se traduit, enfin, par la mise en oeuvre d'une collaboration avec des associations « têtes de réseaux », destinée à faciliter l'appropriation du RGPD par les professionnels d'un secteur : ces partenariats permettent la rédaction commune de guides pratiques, de codes de bonnes pratiques ou de mécanismes de certification.

Dans le domaine des données et des moyens de paiement, à partir des pistes de travail proposées par le présent Livre blanc, la CNIL souhaite se donner pour les années qui viennent une feuille de route fondée sur trois piliers : favoriser la bonne connaissance de la réglementation et des risques par les personnes, accompagner les professionnels dans leur conformité RGPD en utilisant le levier européen en tant que de besoin, favoriser l'interrégulation pour favoriser la cohérence de l'action publique. La CNIL souhaite construire cette feuille de route de manière partenariale, au plus près des besoins identifiés sur le terrain.

OUTILS PÉDAGOGIQUES SUR LES OPÉRATIONS DE PAIEMENT POUR LES ACTEURS DE TERRAIN

Parmi les publics auxquels s'adresse ce Livre blanc (grand public d'usagers, commerçants, professionnels du paiement, mais aussi régulateurs, investisseurs, etc), la CNIL souhaite améliorer la compréhension d'enjeux complexes et à forte technicité, afin de faire prendre conscience des risques pour la vie privée et les données personnelles et les droits et obligations qui y sont attachés (voir figure 15).

Pour les consommateurs

À l'issue du parcours d'achat d'un bien ou de la souscription d'un service, les moments de paiement sont traditionnellement un moment de « friction » au cours duquel les personnes concernées, consommateurs, s'interrogent sur leurs droits[90] et doivent également faire des choix concernant leurs données personnelles en toute connaissance de cause afin d'en garder le contrôle.

La CNIL se propose d'élaborer avec les associations de consommateurs de courtes fiches pédagogiques illustrant les principales questions à se poser par les consommateurs s'agissant des données et moyens de paiement, y compris la sécurité. L'objectif est que les parcours client très ergonomiques s'accompagnent d'une bonne conscience des enjeux de vie privée de protection des données personnelles associés, afin de favoriser une économie de la confiance.

Pour les commerçants

L'univers du commerce est très divers face à la question des données et moyens de paiement, que ce soit en termes de canal (e-commerce ou ventes physiques) ou de moyens (grands détaillants ou TPE). Mais quelle que soit la configuration, il doit être éclairé sur les enjeux de protection des données personnelles des données de ses clients, y compris dans leur dimension internationale, avant de proposer à ces derniers une solution de paiement.

La CNIL se propose de travailler avec les différentes fédérations de commerçants concernés à des fiches pratiques résumant les grandes questions que doit se poser un commerçant au moment de choisir son sous-traitant prestataire des services de paiement, trouver des ancrages de négociation avec lui et être capable éventuellement de mettre en avant auprès de sa clientèle les solutions plus protectrices de la vie privée et des données personnelles.

Pour les investisseurs

Pour un parcours innovant dans l'« *open banking* », la conformité RGPD, facteur de confiance pour le client est un point clé, notamment au stade de l'amorçage où les choix de protection des données dès la conception et par défaut (« *data protection by design and by default* ») doivent être faits. Mais les investisseurs ont besoin d'une grille de lecture pour pouvoir auditer la conformité RGPD des modèles d'affaires auxquels ils s'intéressent.

Dans le cadre de sa politique d'appui à l'innovation, la CNIL se propose d'élaborer un cadre d'évaluation des bénéfices et risques en matière vie privée et de protection des données personnelles, de manière partenariale avec des « têtes de pont » des écosystèmes innovants et des investisseurs d'amorçage. Ce cadre ne serait pas spécifique aux paiements mais les projets en matière de paiement y trouveraient des repères de conformité et de confiance.

Figure 13

Les points clés d'application du RGPD

Source : CNIL

90 - *Scènes de la vie numérique*, cahier IP n°8 (PDF, 5,1 Mo), p. 41, 13 avril 2021, cnil.fr

PLAN D'ACTION POUR L'ACCOMPAGNEMENT DES PROFESSIONNELS DANS LE DOMAINE DES PAIEMENTS

Les consultations menées par la CNIL ont démontré le besoin pour les professionnels du paiement, dans un cadre en évolution concurrentielle rapide, y compris avec de grands acteurs internationaux, d'un pacte de confiance avec leurs clients avec une proposition de valeur qui ne se réduise pas à des questions de coût ou d'expérience utilisateur mais qui s'étende au terrain de la vie privée et de la protection des données personnelles. Ce cadre de confiance pour le client, qui n'a à ce jour pas été posé dans toutes ses composantes, est également un cadre de référence pour les acteurs dans leur conformité RGPD. Une telle démarche est nécessaire afin de favoriser l'innovation et d'une manière générale un haut niveau de protection des données personnelles dans l'économie des paiements.
Dans cette optique, la CNIL compte décliner, dans les mois et années à venir, un plan d'action partenarial d'accompagnement à la conformité sur plusieurs points sur lesquels des besoins ont été exprimés.

Vers un code de conduite pour les prestataires de services de paiement, facteur de confiance pour les personnes

Un code de conduite est un outil de conformité sectoriel qui résulte d'une double démarche volontaire : la décision par l'organisation représentative du secteur d'élaborer un code et l'adhésion des professionnels concernés. C'est **un outil juridiquement contraignant** : il s'impose à ceux qui y adhèrent. Il oblige les adhérents, d'une part, à se conformer aux règles écrites au sein du code et d'autre part, à accepter qu'un organisme tiers désigné contrôle sa bonne application. Il peut concerner l'ensemble des points de conformité, y compris la sécurité ou les transferts.

Dans le domaine des paiements, un code de conduite serait l'équivalent pour la protection des données personnelles de la certification PCI-DSS vérifiée par le GIE Cartes bancaires pour la sécurité des paiements par carte. La CNIL propose aux associations professionnelles sectorielles d'être porteurs de ce projet (avec la participation, si nécessaire, des Fintechs et des banques). Une fois élaboré, le code de conduite peut être approuvé au plan européen pour des raisons d'égalité concurrentielle.

Des élaborations doctrinales sur certains points critiques de conformité

Compte tenu de la configuration du secteur, fortement intermédié, les données de paiement, portent généralement sur une multitude de bénéficiaires différents, et sont à ce titre susceptibles de révéler des informations relevant de la vie privée des personnes concernées, qu'elles soient collectées auprès de plusieurs responsables de traitements ou par un même acteur. Les enjeux en matière de protection des données sont d'autant plus importants lorsque ces données sont mutualisées afin d'être réutilisées après la réalisation du paiement. Ainsi, la CNIL envisage, dans le cadre de son programme de travail et en concertation avec les acteurs, d'élaborer une doctrine plus précise applicable aux traitements qui supposent une concentration, une mutualisation ou une réutilisation de données de paiement. En outre, ces développements seraient un atout de confiance pour l'ensemble des acteurs, notamment les acteurs innovants, qui n'ont pas les mêmes moyens à consacrer à la conformité que les grands groupes financiers.
Les travaux de la CNIL, permettront de clarifier les conditions dans lesquelles ces traitements peuvent être envisagés. Ils pourront notamment porter sur :

- **la qualification des acteurs :** en fonction de leur rôle dans cet environnement complexe, en raison du nombre d'intermédiaires et de la pluralité des réglementations qui leur sont applicables ;
- **le partage des données de paiement entre les acteurs :** qu'il s'agisse de la constitution de ces bases mutualisées ou de leur utilisation, chaque ouverture ou partage est un traitement soumis à l'ensemble des dispositions applicables en matière de protection des données ;
- **l'enrichissement des données de paiement réutilisées :** supposé par un nombre croissant d'usages, en matière de lutte contre la fraude ou à des fins commerciales, le traitement de données non strictement nécessaires à la réalisation du paiement pourrait contrevenir au principe de minimisation des données posé par le RGPD.

Des recommandations sur la sécurité : la tokenisation

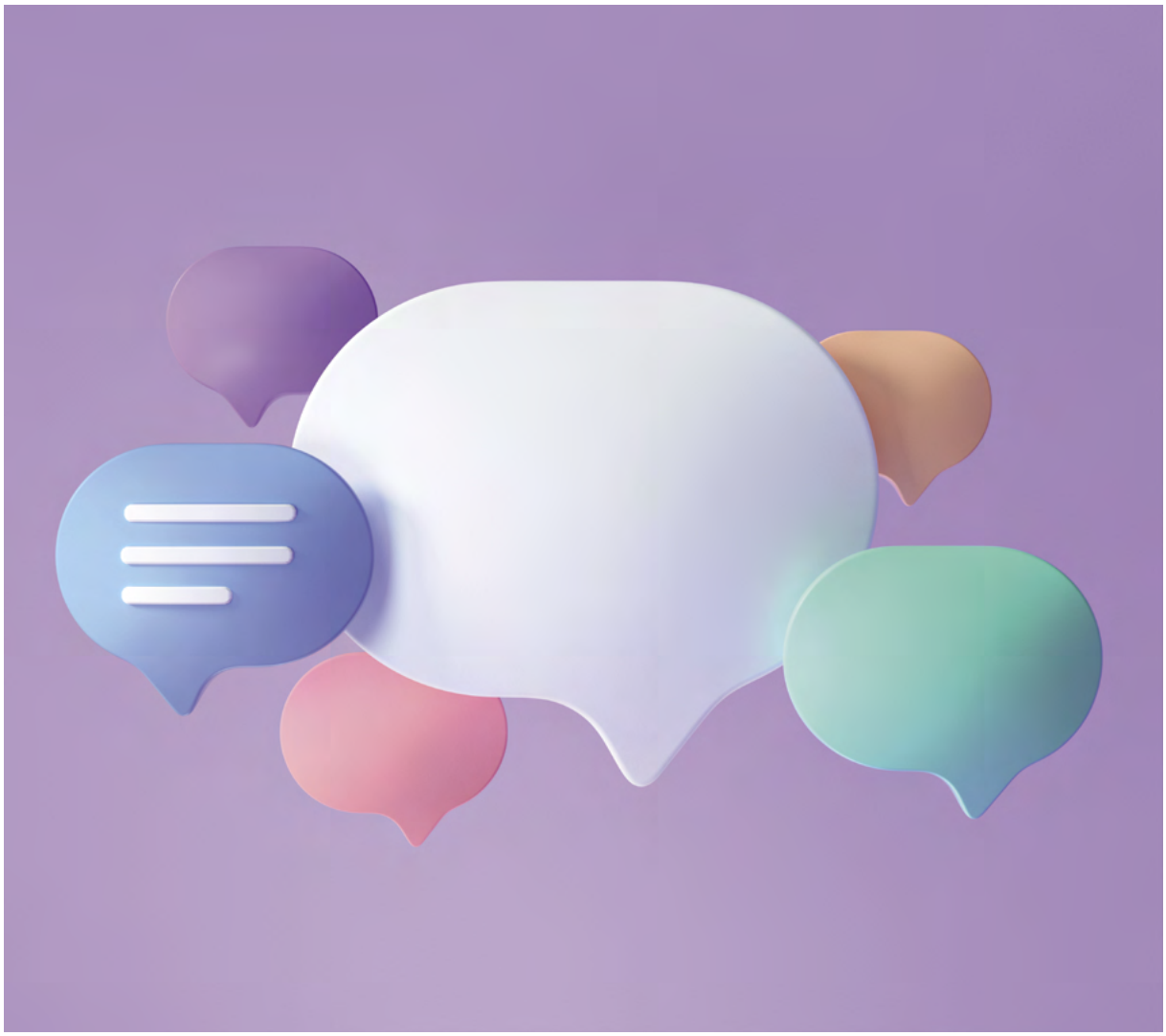
La CNIL se propose d'élaborer des recommandations pratiques en direction de l'écosystème et des régulateurs s'agissant notamment de la « tokenisation » (pseudonymisation) de ces données : champ des données concernées, techniques à utiliser, bonnes pratiques, etc.

UN DIALOGUE À POURSUIVRE ENTRE LES DIFFÉRENTS RÉGULATEURS

Dans le domaine des paiements, et comme l'illustrent les contributions des autres régulateurs concernés à ce Livre blanc, les questions de protection de la vie privée et de protection des données personnelles interagissent avec d'autres réglementations, tant transversales que sectorielles. Il est important que les régulateurs échangent sur les solutions concrètes aux questions de conformité, mais aussi qu'ils coopèrent pour clarifier en tant que de besoin les points de droit découlant des différentes réglementations applicables.

La CNIL continuera d'entretenir un dialogue régulier (y compris pour travailler en réseau sur des points précis à la demande des professionnels concernés) avec les autres institutions concernées par cette interrégulation. Il s'agit, d'un point de vue sectoriel de l'ACPR, la Banque de France, la Direction générale du Trésor, mais aussi sur des aspects plus transversaux, de l'Autorité de la concurrence et Direction générale de la consommation, de la concurrence et de la répression des fraudes.

Enfin, la CNIL continuera à collaborer avec les autres régulateurs concernés et les institutions européennes pour contribuer aux débats réglementaires nationaux et européens actuels et à venir concernant les données et moyens de paiement.



CONCLUSION / REMERCIEMENTS

LE MOT DU COMMISSAIRE

Philippe-Pierre CABOURDIN
Membre du collège de la CNIL, conseiller maître à la Cour des comptes.

Au terme de ce parcours économique et juridique d'exploration des enjeux de vie privée et de protection des données personnelles attachés aux données et moyens de paiement, qui donne à voir toute la complexité de ces questions, trois réflexions me paraissent ressortir plus particulièrement.

La première constate que les moyens de paiement sont un bel exemple des liens forts qui mobilisent protection des données à caractère personnel, régulation de la concurrence, réglementation financière et protection du consommateur. Ces objectifs fondamentaux vers lesquels ce Livre blanc a jeté des ponts montrent que les régulateurs ne peuvent bien appréhender ces questions qu'en les abordant ensemble. Ce sujet justifie un haut niveau de coopération qui doit être maintenu et approfondi entre la CNIL et l'ACPR ou avec l'Autorité de la concurrence.

La deuxième porte sur le caractère diffus des flux de données de paiement et des données qui leur sont liées, à travers l'économie, en France comme à l'étranger. Les données de paiement hier définies strictement et cantonnées dans les systèmes bancaires sont aujourd'hui réutilisées, voire captées, et combinées avec d'autres et circulent à l'international même pour des transactions domestiques. Ceci plaide pour ne pas en faire seulement un objet de régulation financière ou de protection des données bancaires mais pour adopter une vision large de la régulation, allant de la responsabilité des commerçants à celle des grands acteurs de l'internet en passant par les enjeux émergents de politique monétaire. Une partie de ces débats ne peut évidemment être menée a minima qu'au plan européen.

La troisième postule que le paiement est un objet intrinsèquement politique, dont le débat public doit se saisir. Le citoyen doit pouvoir décider en toute connaissance de cause à qui il confie ses données de paiement, avec quels risques et pour quels usages. Il doit avoir des outils pour refuser les risques de traçage ou de compromission de ses données. Le maintien de moyens de paiement non traçables, y compris pour les monnaies numériques de banque centrale, et leur corollaire le libre choix du moyen de paiement en dessous d'un seuil à fixer, est essentiel pour les libertés publiques et pour nos libertés économiques. Enfin, le paiement est une question de souveraineté, des individus comme des États.

C'est pourquoi, le contrôle démocratique sur les enjeux des systèmes de paiement et les libertés qui y sont associées, est absolument essentiel. Puisse ce Livre blanc y contribuer !

Dans le cadre de la préparation du Livre blanc de la CNIL Quand la confiance paie : anciens et nouveaux moyens de paiement au défi de la protection des données, ont été consultées les entités suivantes :

- Wavestone
- Cabinet Racine
- Cabinet DLA Piper
- Me Pierre Storrer

- GIE Cartes bancaires
- Fédération bancaire française
- Natixis/BPCE
- Mastercard
- Association du paiement
- Worldline

- Mercatel
- Groupe Casino
- ACEDISE (représentant les systèmes d'encaissement)

- Association France FinTech
- Truffle capital
- Limonetik
- Lemonway
- Antelop
- Apple Pay
- Google Pay

La CNIL tient plus particulièrement à remercier ses partenaires :

- Association du paiement
- ACSEL (association de l'économie numérique)
- La mission numérique grands groupes

Glossaire

API (interface de programmation d'application ou *application programming interface*) : interface de programmation permettant à deux programmes ou logiciels d'interagir entre eux, en se connectant pour échanger des données, utilisée notamment dans le régime DPS2.

Authentification forte : dans le régime DSP2, procédure permettant au prestataire de services de paiement de vérifier l'identité d'un utilisateur de services de paiement, pour protéger la confidentialité de ses données, et reposant sur l'utilisation de deux éléments ou plus, indépendants, 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).

***Blockchain* :** registre (grande base de données) décentralisé (partagé simultanément) entre tous ses utilisateurs, tous également détenteurs de ce registre, et qui ont également tous la capacité d'y inscrire des données, selon des règles spécifiques fixées par un protocole informatique très sécurisé grâce à la cryptographie (en français : technologie de registre distribué).

Compensation : entre institutions financières, une transaction a toujours un débiteur et un créditeur. La compensation est matérialisée par le jeu d'écriture comptable qui retrace la transaction. On dit que le crédit sur le compte du créditeur compense le débit sur le compte du débiteur.

Cryptomonnaie : valeur monétaire représentée sous forme numérique et décentralisée, qui utilise des algorithmes cryptographiques et un protocole nommé *blockchain* pour assurer la fiabilité et la traçabilité des transactions.

Données hautement personnelles : selon le Comité européen pour la protection des données, données augmentant le risque possible pour les droits et libertés des personnes et dont la violation aurait clairement des incidences graves dans la vie quotidienne de la personne concernée (données financières susceptibles d'être utilisées pour des paiements frauduleux, par exemple).

Donnée personnelle : toute information relative à une personne physique susceptible d'être identifiée, directement ou indirectement.

Données relatives à la carte de paiement : pour la CNIL, les données nécessaires à la réalisation d'une transaction à distance par carte de paiement sont le numéro de la carte, la date d'expiration et le cryptogramme visuel.

Données sensibles : au sens du RGPD, donnée personnelle révélant la prétendue 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.

Donnée biométrique : donnée personnelle permettant d'identifier une personne physique de manière unique.

Monnaie de banque centrale : monnaie émise directement par une banque centrale sous forme de pièces et de billets (monnaie fiduciaire) et de sommes placées par les banques commerciales sur les comptes qu'elles détiennent auprès de la banque centrale, leur permettant non seulement de s'approvisionner en billets de banque, mais aussi d'assurer le maintien de sommes en réserve (les « réserves obligatoires »).

Monnaie scripturale : par opposition à la monnaie fiduciaire, forme de monnaie résultant des jeux d'écritures dans les comptes des entités financières privées et représentant une créance sur ces entités.

Monnaie numérique de banque centrale : élément de la base monétaire, échangeable au pair avec la monnaie fiduciaire et les réserves, disponible en permanence et dans des transactions de pair-à-pair et circulant sur des supports numériques (en anglais : *central bank digital currency* ou *CBDC*).

Monnaie électronique : valeur monétaire stockée sous une forme électronique, y compris magnétique, représentant une créance sur l'émetteur, qui est émise contre la remise de fonds aux fins d'opérations de paiement et qui est acceptée par une personne physique ou morale autre que l'émetteur de monnaie électronique.

Glossaire

Monnaie fiduciaire : billets et pièces émis par les autorités publiques et ayant cours légal.

Moyen de paiement : tout instrument qui permet à une personne de transférer des fonds, quel que soit le support ou le procédé technique utilisé.

Moyens de paiements scripturaux : les cartes de paiement, les chèques, les virements, les prélèvements, les effets de commerce et la monnaie électronique

Opération de paiement : action initiée par le payeur, ou pour son compte, ou par le bénéficiaire, consistant à verser, à transférer ou à retirer des fonds, indépendamment de toute obligation sous-jacente entre le payeur et le bénéficiaire (définition de la DSP2).

Paiement (selon le Code civil) : exécution volontaire de la prestation due qui libère le débiteur à l'égard du créancier et éteint la dette.

Paiement instantané : solution de paiement électronique disponible en permanence résultant d'une compensation interbancaire immédiate ou quasi immédiate de l'opération.

Porte-monnaie électronique ou encore Portefeuille numérique : solution permettant à un utilisateur de confier à un tiers, jugé de confiance, des instruments et données de paiement, sans recours à un compte bancaire.

Prestataire de services de paiement gestionnaire de comptes : dans le régime DSP2, prestataire de services de paiement qui fournit et gère des comptes de paiement pour des payeurs (en anglais : *account servicing payment service provider* ou *ASPSP*).

Protocole 3D-Secure : protocole mettant en relation le payeur avec la banque émettrice de la carte bancaire afin d'authentifier celui-ci pour un paiement en ligne.
SCT Inst : paiement instantané transfrontalier de la zone euro, également appelé le SEPA Instant Credit Transfer.

SDK ou Software Development Kit : outil de développement permettant la création d'une fonctionnalité sur une plateforme.

SEPA (EU) : système interbancaire de paiement de détail reposant sur une infrastructure fonctionnant sur la base d'une compensation multilatérale avec un règlement différé intervenant une fois par jour en monnaie banque centrale.

Services d'initiation de paiement : dans le régime DSP2, services qui permettent à une personne physique ou morale d'ordonner l'exécution d'opérations de paiement, par exemple des virements, à partir d'une interface (site internet et/ou application mobile) qui n'est pas forcément celle de la banque dans laquelle son compte (ou ses comptes) est (sont) détenu(s) (en anglais : *payment initiation service provider* ou *PISP*).

Services d'information sur les comptes : dans le régime DSP2, services qui permettent à une personne physique ou morale de regrouper sur une seule interface les informations sur un ou plusieurs de ses comptes de paiement (en anglais : account information service provider ou AISP).

Système de paiement : type d'infrastructure de marché assurant le règlement interbancaire des paiements de détail de la clientèle des banques ou des paiements de montant élevé entre institutions financières.

Technologie de communication sans contact NFC (« near field communication ») : technologie permettant à deux terminaux situés à proximité équipés d'une telle technologie, un ordiphone et un terminal de paiement par exemple, d'échanger très rapidement des données et des instructions.

Tokenisation : procédé de sécurité informatique permettant de remplacer une donnée critique par un élément équivalent qui n'aura aucune valeur intrinsèque ou signification exploitable une fois sorti du système. Pour présenter un niveau de sécurité satisfaisant, un *token* (ou jeton) doit être irréversible et généré de manière aléatoire.

Transfert international de données : toute communication, copie ou déplacement de données personnelles ayant vocation à être traitées dans un pays tiers à l'Union européenne.

Commission nationale de l'informatique et des libertés
3 place de Fontenoy
TSA 80715
75334 PARIS CEDEX 07
Tél. +33 (0)1 53 73 22 22

cnil.fr
educnum.fr
linc.cnil.fr

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS