WHITE PAPER COLLECTION N°2

WHEN TRUST PAYS OFF

Today's and tomorrow's means of payment facing the challenge of data protection

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

WHITE PAPER COLLECTION **- N°2**

WHEN TRUST PAYS OFF:
Today's and tomorrow's means of payment facing the challenge of data protection

CONTENTS

September 2021

Director of publication: Gwendal Le Grand

Editor-in-Chief: Thomas Dautieu

Contributors to this White Paper: Aymeric Pontvianne (project manager), Antoine Courmont, Erevan Malroux, Gaston Gautreneau, Délia Rahal-Löfskog with the assistance of Valérie Bourriquen, Clément Commerçon, Viktorija Elenski, Pauline Faget, Estelle Hary, Antoine Planchot, Flora Sanchez and Clémence Scottez.

Graphic design: Agence Linéal - 03 20 41 40 76

Printing: DILA

Illustrations: Lakee MNP (Adobe Stock)

Translation: Technicis, November 2021

CONTENTS

EDITORIAL

Significant changes in means of payment are underway, especially since the start of the pandemic, with increased use of contactless payments, a decline in the use of cash and a boom in online shopping. These structural changes are accompanied by an increase in the use of new purely digital means of payment such as mobile payments, transfers between individuals and the use of digital wallets.

They are coupled with the development of FinTechs with the implementation of the second Payment Services Directive, opening up banking data to them.

The economic stakes are high. For instance, the American payment giant Square has announced its intention to buy Afterpay, the Australian specialist in split payments, for $29 billion, more than what Microsoft spent on the acquisition of LinkedIn. Ultimately, the payments sector will undergo even more profound transformations with new technical developments such as the rise of instant transfers, the digital euro project launched on 14 July 2021 by the European Central Bank and the European Payments Initiative (EPI) pan-European card network project, which will further modify the positioning of economic players.

However, payment data are personal data. Purchase data, financial data and contextual data concern many aspects of people's existence. They can be used to "track" their personal activities and identify their behaviour, but they can also be used to commit fraud. And what's more, the use of a given means of payment and, in particular, the possibilities of using cash also involve important issues of anonymity and protection of privacy. The CNIL needed to look at the privacy issues relating to payment data, and to circulation and protection thereof.

This White Paper is aimed at both the general public and professionals. It lays the groundwork for economic and legal analysis. It is backed by a public consultation on more specific compliance issues and defines a roadmap to support the various players for the years to come. This report is, in fact, only the first step in the dialogue that we are starting with stakeholders.

The aim is to achieve full compliance of the data processing by the various parties involved (banks and their service providers, but also merchants, e-commerce platforms and payment service providers), not only to protect individuals but also to strengthen the level playing field between all players on the French market. We still have a lot to learn from each other.

With the interest shown by the major digital players in payment methods, payment data have now become a matter of sovereignty, which raises even more acutely the privacy issues linked to international data transfers. The CNIL intends to contribute to this debate at national and European level. But because the subject is complex and not quite transparent, it is also our aim to inform individuals as much as possible about the risks and issues related to payment data and means of payment.

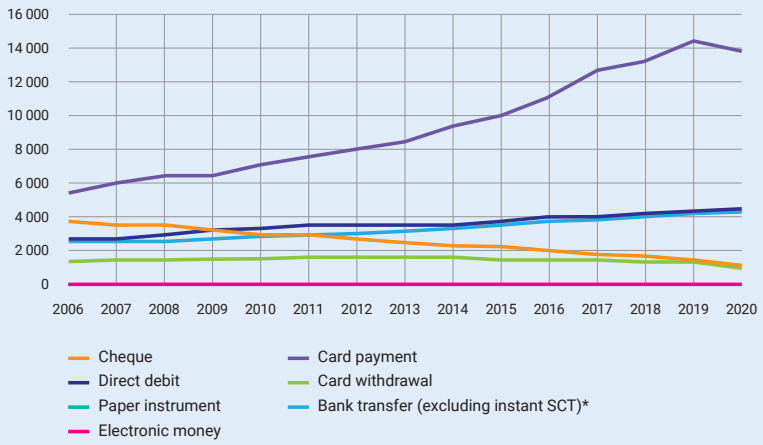
Finally, the digital economy feeds on trust between individuals and professionals. The new uses of payment data must not derogate from this reality. Surveys show that customers are sometimes reluctant to entrust their payment data to European start-ups and other FinTechs, as they are newcomers to this field. The CNIL would have achieved its objective if it contributes, at its own level, to ensuring that the protection of privacy is inseparable from the changes observed in payment services and a responsible innovation.

Marie-Laure Denis,
Chair of CNIL

KEY FIGURES

USE OF MEANS OF PAYMENT IN FRANCE 2006 TO 2020

IN MILLIONS OF TRANSACTIONS



* Instant SCT: SEPA instant credit transfer

Source: Observatory for the Security of Means of Payment (OSMP)

59%

OF POINT-OF-SALE PAYMENTS,

FOR 25%

OF THE AMOUNTS PAID, WERE MADE IN CASH IN FRANCE IN 2019

According to the ECB's 2019 SPACE survey

TRENDS IN MEANS OF PAYMENT IN FRANCE

68%

OF ONLINE SHOPPERS THINK THAT DATA SECURITY AND THE SECURITY OF TRANSACTIONS ON AN E-COMMERCE SITE REMAIN A SELECTION CRITERION

According to the quarterly barometer of the e-commerce audience in France Fevad -Médiamétrie (Q4 2020)

1

FRENCH PERSON OUT OF 10

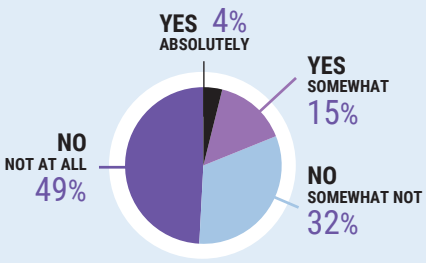
SAYS THEY USE A SMARTPHONE PAYMENT METHOD

According to the latest Global Consumer Survey conducted in summer 2020

81%

OF THOSE QUESTIONED DO NOT WANT TO SEE CASH DISAPPEAR IN FAVOUR OF DEMATERIALISED MEANS OF PAYMENT

According to the Ifop/Brink's 2019 observatory



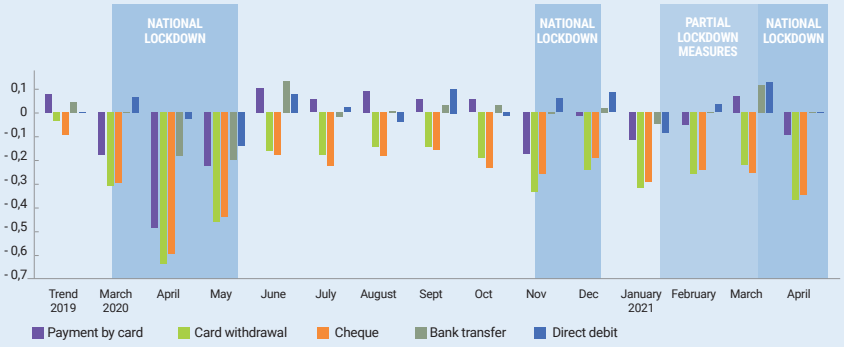
KEY FIGURES

COVID-19 CRISIS

A marked decline, especially during periods of lockdown, in means of payment involving physical contact, and an increase in contactless and online payments (cards, transfers, direct debits), reflecting an increased digitalisation of payments.

CHANGE IN PAYMENT FLOWS IN VOLUME COMPARED TO THE PRE-CRISIS BASIS PERIOD (MARCH 2019/FEBRUARY 2020) (%)

According to the 2020 OSMP report



COMPARED TO 2019

+ 37%

FOR CONTACTLESS PAYMENTS

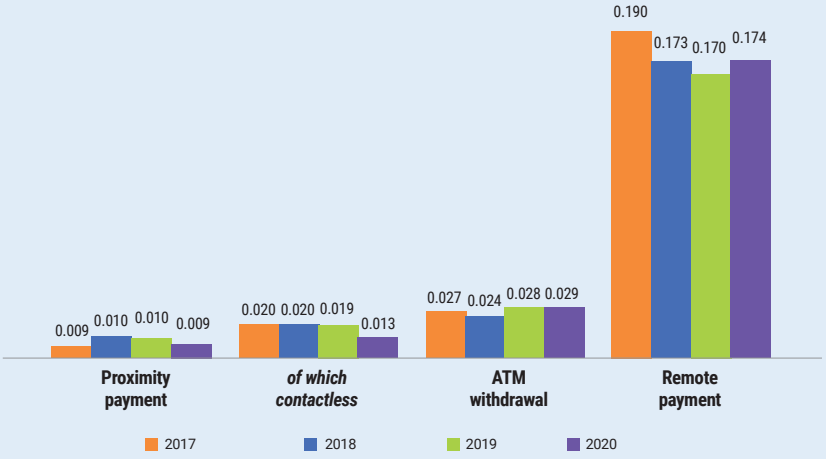
+ 13,2%

FOR ONLINE CARD PAYMENTS BY NUMBER OF TRANSACTIONS

FRAUD

COMPARISON OF FRAUD RATES ON NATIONAL TRANSACTIONS, BY TYPE OF TRANSACTION (%)

Source: Observatory for the Security of Means of Payment (OSMP)



ATM: automatic teller machine (cash machine)

2,825

NOTIFICATIONS OF DATA BREACHES RECEIVED BY THE CNIL IN 2020

OF WHICH

311

FOR FINANCIAL AND INSURANCE ACTIVITIES

+ 5%

IN 2020 COMPARED TO 2019

According to the 2020 CNIL annual report

PAYMENT DATA:
What are we talking about and why?

Payment operations, i.e. the payment of monetary compensation for the provision of goods or services, are of essential importance for economic and social life.

The speed and reliability of transaction settlement, whether between professionals (settlement-delivery of assets on the financial markets, for example), between professionals and individuals (retail purchases) or even between individuals (peer-to-peer payments) is a key factor for efficiency and level of trust in the economy.

The added value of the payments sector worldwide was estimated in 2019 at around $1.5 trillion[1] dollars, i.e. the equivalent of Spain's GDP, with a growth of around 7% per annum before the pandemic. Moreover, payment operations, which carry the full value of transactions within the economy, have a systemic character, which can become apparent in the event of breakdown or disruption of the systems used.

A payments revolution is under way: this term used since the 2012 Pauget-Constans report on the future of means of payment is no longer a metaphor. The field of payments is in fact today at the centre of three upheavals with cumulative effects:

A technological upheaval involving a change in usage patterns

The rise of online commerce and correlatively of online payments, the use of electronic money in wallets and smartphone payments have changed consumer behaviour and renewed the conditions for the operation of payments and circulation of the corresponding data.

A competitive upheaval and the arrival of innovative players

Faced with the traditional duo formed by banks and card networks, new players have emerged that provide payment services to e-commerce or new online services to consumers, a shift that has been accompanied by the sudden entrance of the big digital players in this field.

A regulatory upheaval in the access to data

European regulations have chosen "open banking" with the second Payment Services Directive (PSD2) of 2015, which implies supervised but compulsory access to bank account data by new FinTech players.

There is a great deal at stake for the French economy: employment in the payments industry was estimated at **72,000 direct jobs and 18,000 indirect jobs in 2014[2] with an added value of €6 to 7 billion euros,** half of which was outside the banking system.

Today, as the recent retail payments strategy of the European Commission reiterates, "once relegated to the back-office, payments have become strategically significant[3]" and are a matter of "Europe's economic and financial sovereignty". An economic, innovation and sovereignty issue, risks for privacy and personal data: **our payment data are no longer in the shadows of banking secrecy. This is why the CNIL has decided to broach the subject.** The views expressed in this White Paper will also enable it to play its full part in the European debate on these issues.

> ***Once relegated to the back-office, payments have become strategically significant***

1 - *Global Payments 2020, Fast forward into the future,* October 2020, bcg.com
2 - Mapping of the payments industry in France, April 2014, finance-innovation.org
3 - Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Retail Payments Strategy for the EU, 24 September 2020, eur-lex.europa.eu

WHAT IS PAYMENT DATA?

Payment transactions[4] bring into play fiat money, bank money and electronic money, means of payment (the technique allowing money to be used to perform the transaction), payment systems (the infrastructure used for the transfer of funds from the initiator to the recipient) and finally payment data.

They can be defined as all the data collected and processed during a payment operation, a potentially broad scope with increasingly strong links with other types of data (purchase history, customer knowledge data) as a result of the rise in online payments.

In practice, the data we are interested in here fall into three broad categories, the boundaries of which are more blurred for online payments than they are for physical payments:

• **Actual payment data:** including identifiers of the means of payment used, amount of the transaction, date and time of payment, identity of the merchant, identity of the beneficiary, IBAN, the customer's fraud prevention score, etc. These data depend on the means of payment and the payment system used and are traditionally historicised by banking operators.

• **Purchase or checkout data:** including characteristics of the products purchased, date and place of purchase, loyalty card details if applicable, etc. They are observed during the purchase and traditionally collected and historicised by merchants (traditional or online).

• **Contextual or behavioural data:** customer knowledge data, geolocation, characteristics of the terminal used for an online purchase, characteristics of the products explored prior to the purchase, the time spent browsing, etc. These data are easier to collect during an online purchase and are readily accessible to major digital players.

In the end, it is reasonable to define payment data as all the personal data used when a payment service is provided to a natural person, including ancillary data such as geolocation, contextual data or even, where applicable, the details of purchases. This definition is also the one adopted by the British Payment Systems Regulator[5] while the Payment Services Directive (PSD2) does not define this concept. In this White Paper, the CNIL focuses on personal data associated with payments involving individuals.

At this stage, it is important to remember that certain payments (in cash, below an amount of €1,000 in France for payments to a professional) do not generate associated personal data and today constitute an alternative available to all, as discussed later in this White Paper.

> ***"It is reasonable to define payment data as all the personal data used when a payment service is provided to a natural person"***

4 - A payment transaction is defined as an "action, initiated by the payer or on his behalf or by the beneficiary, consisting in paying, transferring or withdrawing funds, regardless of any underlying obligation between the payer and the beneficiary" (Article L.133-1 of the French Monetary and Financial Code).
5 - *"Discussion Paper: Data in the Payment Industry"*, 13 June 2018, psr.org.uk.

SPECIFIC ISSUES INVOLVED WITH PAYMENT DATA

These data are personal data, because they relate directly or indirectly to an identified or identifiable natural person (the customer). Some data are qualified as personal data when taken individually, some data because they are collected together with other data for identification purposes (e.g. browser characteristics) or because they can be cross-checked with other data for the purposes of inference about a person (e.g. the amount of a transaction).

In general, and taking into account their nature and the conditions under which they are collected, data will be considered as personal data unless they have been anonymised.

Payment data can relate to many aspects of people's lives. They are historicised and stored in bank accounts or electronic purses[6], beyond the transience of the transactions, sometimes over long periods. It is therefore reminiscent of what the Court of Justice of the European Union (CJEU) says about large-scale surveillance data: "Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them." [7]

What also makes payment data specific is that they can, in certain cases, concern third parties, not just the person who carried out a transaction. This is the case with payments where the beneficiary is another natural person, for example. These third parties are said to be "silent parties" because data concerning them are traced on the account of another person without the silent party being able to access them, which in certain cases raises particular issues in terms of personal data protection[8].

In addition, Article 9 of the General Data Protection Regulation (GDPR) particularly protects so-called "sensitive" data, i.e. data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, biometric data for the purpose of uniquely identifying a natural person, health data or data concerning a person's sex life or sexual orientation. While a simple transfer of funds is not intended to reveal such details, payment operations as a whole may result in the processing of sensitive data within the meaning of the GDPR, for example if a biometric authentication method is used.

Finally, the European Data Protection Board qualifies some of them as "highly personal data"[9] when they reveal geolocation or if they can be used to commit payment fraud. This is the case with card numbers and other payment identifiers, for example. There is obviously a great deal at stake in terms of security with these last data.

6 - Also known as e-wallets, see the definition of these terms in the glossary.
7 - Judgment of the CJEU, Grand Chamber, "Digital Rights Ireland Ltd" (case C 293/12), recital 27, 8 April 2014, eur-lex.europa.eu.
8 - "Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR" (PDF 308 KB), pp. 16 et seq., 15 December 2020, edpb.europa.eu.
9 - *Guidelines on the Data Protection Impact Assessment (DPIA) and how to determine whether processing is "likely to give rise to a high risk" for the purposes of Regulation (EU) 2016/67* (PDF, 1.4 MB), 4 October 2017, page 11.

SCOPE OF THE WORK: THE OUTLINE OF THE PAYMENT CHAIN

Like the payment operations themselves, payment data concern many important economic players:

- To start with, they concern the entire population. People carry out monetary transactions for all aspects of their existence. Household consumption expenditure thus represented €1,268 billion in France in 2019[10], that is, for 67 million inhabitants, around €18,650 per annum and per inhabitant.

- Then, payment data (excluding purchase data) are reflected by banks and card networks (CB, Visa, Mastercard, etc.): in France, the banking rate stands at 99% according to the French Banking Federation (FBF) and 25 billion payment transactions were processed by French banks in 2019. Similarly, there are 75 million payment cards in circulation in France, according to the ECB.

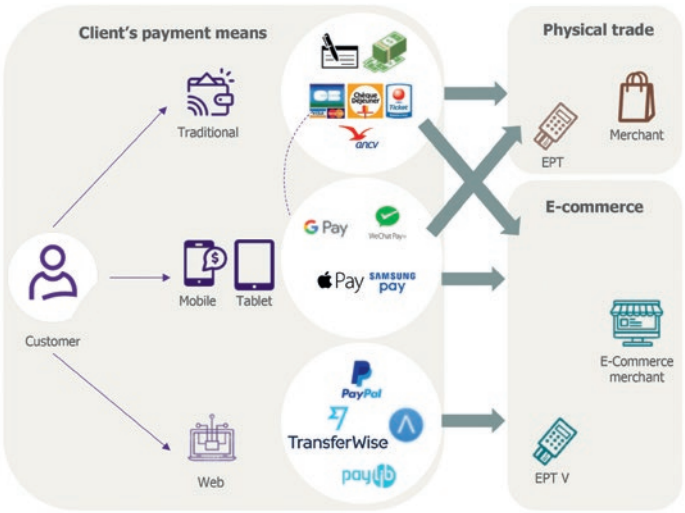
- Merchants and e-commerce merchants: the sector represented around 10% of the added value of the French economy in 2019[11] and 3.4 million jobs. Within this sector, the share of e-commerce is growing by more than 10% per annum and now represents around 10% of retail sales. In 2019, there were more than 200,000 active merchant sites in France according to the Fédération de la vente à distance (Fevad).

- And finally, payment service providers, whether they are physical (point-of-sale payment service providers) or digital (allowing a service to accept an online payment from a customer). So, at the start of 2021, France had 62 licensed payment institutions, 8 Account Information Service Providers (AISPs), 15 Payment Initiation Service Providers (PISPs) and 8,860 agents. Across the EU, there are 715 payment institutions, 65 AISPs and 165 PISPs (Source: websites of the French ACPR and the European Banking Authority).

Figure 1

Simplified diagram of the payment chain according to the terminal used.

Source: Wavestone study for the CNIL, December 2019



Payment data circulate along a fairly long chain which can take two main forms (See mapping on page 24). During a physical transaction, purchase data are collected by the checkout process and kept by the merchant, with financial data circulating along the electronic payment chain to the card network and to the banks where they are stored. During an online transaction, the process is less standardised. All of these players can access contextual data, some can even access purchase data. Security questions are raised by the flow of financial data before they reach the banking operator and the flow of data through online payment providers is based on diverse models and practices.

10 - INSEE, Annual national accounts, series 2.201 - Actual final consumption of households, May 2020, insee.fr
11 - INSEE, Value added by branch, annual data, June 2021, insee.fr

MAPPING OF MEANS OF PAYMENT IN FRANCE

The flow and use of payment data vary significantly depending on the means of payment used, hence why the dynamics of the different payment methods are of great importance for the work of CNIL. In particular, cash transactions do not in themselves result in the processing of personal data: they are anonymous. It is therefore the most protective means of payment in terms of privacy[12].

If we look at retail payments (related to individuals), the available statistics show that the two main means of payment are, both in France and elsewhere in Europe, cards and cash. In France, cash transactions are the most numerous but their average value is lower, while card transactions represent the majority in terms of amount.

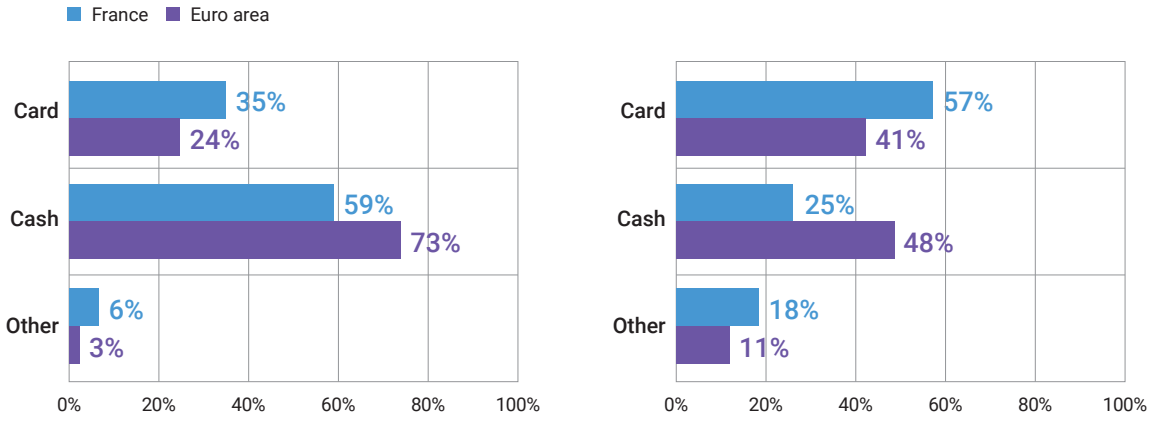
Apart from cash payments (in so-called central bank or fiat money), there are cashless or book payments or, as economists say, payments made in money issued by and under the control of the commercial banks.

In France, **card payments**, the values of which grow year on year, reached €578 billion in 2020[13]. Use fell slightly in 2020 (-4.3% in volume compared to 2019) due to the decline in proximity payments. **Bank transfers** between accounts, the second most widely used means of payment and increasingly popular during the pandemic, mainly concern payments with a professional counterpart (salaries, inter-company payments) rather than individuals. **Direct debits** (excluding cheques and cards) are the third most popular means of payment and can be used by individuals (direct debit mandate for example)[14]. These dematerialised means of payment are secured by the banking system.

Figure 2

Share of the different means of payment at point of sale and peer-to-peer, in France and in the euro area (left: in volume, right: in value).

Source: ECB SPACE survey, 2019 data, page 112



12 - A distinction is made between the protection of privacy (Article 7 of the European Charter of Fundamental Rights) and that of personal data (Article 8 of the Charter).
13 - 2020 Report of the Observatory for the Security of Means of Payment (OSMP), July 2021, banque-france.fr, (PDF) page 19.
14 - Bank transfer and direct debit are the two main payment options via bank accounts. Unlike bank transfers, which are initiated by the payer, the direct debit is launched by the payee, with the payer's agreement.

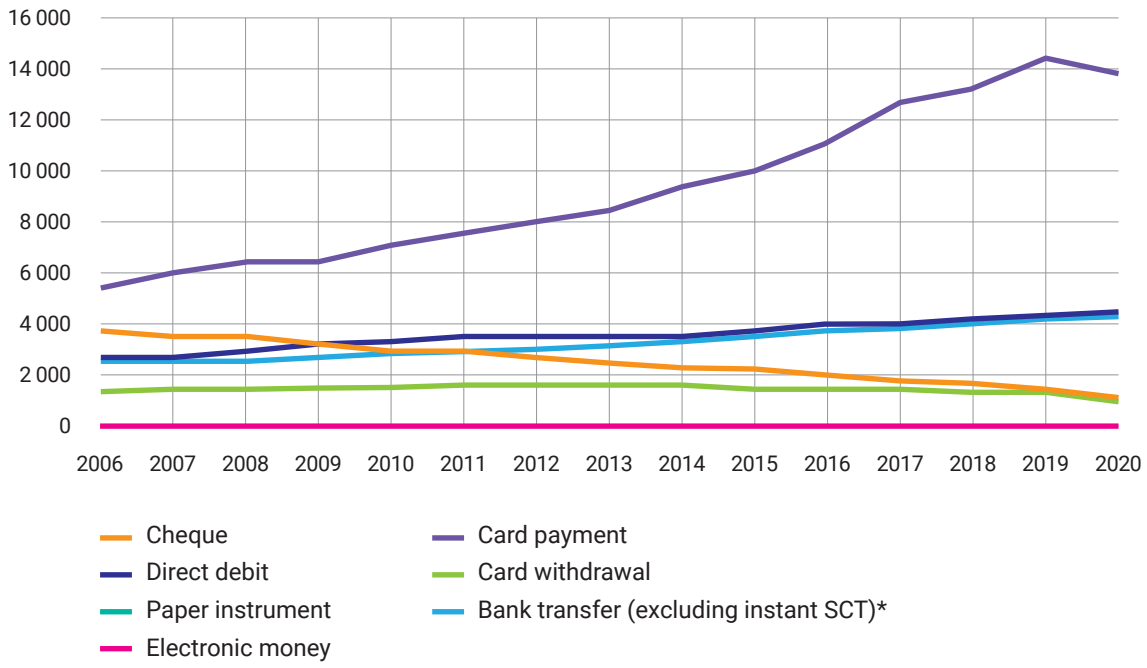
There has been a decline in the use of **cheques**, which remain established in the habits of individuals but which, despite the large amount of personal data they contain (name, address, account number, signature, etc.), are the most defrauded means of payment. We will not be looking at them in this work since they are not one of the new payment methods. **Electronic money,** finally, represents a marginal share of cashless transactions (less than 1% by both volume and value) but recorded an increase in total outstanding amount to €688 million (i.e. +22.6% compared to 2019).

Note that when payment is made remotely, there are fewer means of payment to choose from: the main ones used (card, transfer, direct debit) may require authentication that calls for a lot of personal data. The scope of "anonymity" is also much more limited (prepaid cards without a bank account, electronic money not widely used, with high fees and very low usage limits, which handicap these solutions, however suitable for small amounts). Online banks also make them available to their customers under better conditions than traditional banks.

Figure 3

Use of means of payment in France 2006 to 2020, in millions of operations.

Source: 2020 OSMP report, July 2021, page 22



* Instant SCT (SEPA instant credit transfer).

ACTIVITIES GOVERNED BY MULTIPLE REGULATIONS

The circulation and use of payment data are of course governed by the GDPR, but this regulation coexists with various other regulations, which the compliance departments of the players concerned keep a careful eye on.

The field of payments has long been well described by the distinction between fiat money (cash) issued by the central bank and made available to the general public through the 50,000 or so cash machines in mainland France and book money.

While cash is governed by a few simple rules such as discharge or legal tender, book money and the associated transactions are banking transactions and are traditionally governed by banking law, in France by the Monetary and Financial Code (CMF). Some of the important rules for payments include:

• **European rules** on the fight against money laundering and the financing of terrorism in Book 5 of the CMF[15], a risk to which payment transactions are particularly exposed since they are present both when entering into relationship with any professional and at the stage of vigilance on the transactions carried out;

• **national rules** governing the outsourcing of certain bank functions and in particular the French Order of 3 November 2014 relating to the internal control of companies in the banking sector, payment services and investment firms;

• **banking secrecy rules**, which are also national (Article L.511-33 of the CMF, see next page).

This banking matrix has gradually broken down into an electronic money transactions regime[16] (e.g. PayPal) and a specific payment transactions regime, from 2007, under the influence of European law and in the name of promoting innovation and competition through "open banking".

The latter regime aimed to ensure competition between banks and non-banking operators for payment services in order to move towards a single euro payments area, which was at that time very fragmented in Europe. This first Payment Services Directive of 2009, which established the status of payment institutions, was revised by the PSD2[17] of 2015, which allows third parties like FinTechs to access their clients' bank accounts for certain regulated transactions (payment initiations[18] or aggregated account information[19]) licensed by the national supervisor, in France the Prudential Supervision and Resolution Authority (ACPR), and under very secure conditions (in particular a strong authentication obligation via, for the sake of simplicity, the online banking application).

In addition, some national consumer standards have, over time, started to regulate the use of means of payment and proof of retail purchases but in a punctual manner, reflecting the lesser extent to which retail transactions are regulated compared to banking transactions (for example, Article D.112-3 of the Monetary and Financial Code on the ceiling for cash payments, the Decree of 3 October 1983 relating to the issuance of an invoice for any purchase greater than €25, etc.). With regard to online payments more specifically, consumers are also protected by national and European regulations governing distance selling and by the principle that the supplier of the payment instruments remains responsible for online fraud (protecting the customer in good faith).

15 - Transposing in particular the 5th Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and the 6th Directive (EU) 2018/843 of 30 May 2018 amending it. See also Regulation (EU) 2018/1672 of the European Parliament and of the Council of 23 October 2018 on controls on cash entering or leaving the Union.
16- Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions, revised in 2005 and in 2009.
17- Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market.
18- Payment Initiation Service Providers or PISPs.
19- Account Information Service Providers or AISPs.

This view would be incomplete without mentioning the European texts governing the payment systems themselves, which are subject to regulations within the area of competence of the European Central Bank, for example organising the overseeing of card schemes and their operations in Europe by central banks[20], as well as the important rules of the so-called "interchange" regulation, which falls under the ordinary European procedure and regulates the commissions of these schemes[21].

Finally, payment activities, in particular on points that are less regulated nationally, are governed by international standards drawn up by the private sector, in particular the large international card schemes: standards known as Europay Mastercard Visa or EMV, security standard PCI-DSS protecting in particular the transmission of card numbers in electronic payment infrastructures, and the 3DSecure standard for the fight against online payment fraud, in particular.

> ***Consumers are also protected by national and European regulations governing distance selling and by the principle that the supplier of the payment instruments remains responsible for online fraud***

FOCUS ON...

Banking secrecy and privacy

Provided for by law, banking secrecy is a form of relative professional secrecy, with exceptions and from which the obliged entity can be released by the person who benefits from it. It is required, by virtue of Articles L.511-33 and L.522-19 of the French Monetary and Financial Code, for credit institutions and finance companies but also payment institutions. It benefits both natural persons and legal entities. Violation thereof is penalised (one year of imprisonment, additional penalty of a professional ban).

According to a recent report from the High Legal Committee of the Paris Financial Centre, "the contours of this obligation, which has a very broad scope, remain difficult to grasp due to the multitude of exceptions scattered throughout the regulations and regular case law. Understanding the precise scope of application of banking secrecy remains a source of legal uncertainty, both for the persons protected and for the obliged entities (as well as natural persons bound to secrecy) who remain exposed to penal sanctions, which, although rarely delivered, are particularly severe.[22]"

While banking secrecy and the protection of personal data are in the same spirit, the legal constraints associated with banking secrecy seem, according to some, due to its very broad scope, to be greater than those resulting from the GDPR from an operational point of view.

20 - Regulation of the European Central Bank (EU) No 795/2014 on oversight requirements for systemically important payment systems.
21 - Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions.
22 - High Legal Committee of the Paris Financial Centre, Report on banking secrecy, 6 July 2020, banque-france.fr.

MEANS OF PAYMENT AND DATA: SOCIETAL AND PUBLIC FREEDOM ISSUES

Traceability

The issue with, and perhaps even the most obvious risk of the circulation of payment data is the potentially detailed knowledge of transactions by private entities, operating on a large scale and capable of reusing this knowledge for their own account. Payment data are based on a documentary system for keeping accounts, identifying customers and storing their debts, whether for account-keeping purposes (at banks) or for tax reasons (at point-of-sale). This historicisation of data increases their value and their attractiveness for the development of new services, mainly carried out by third parties, of various sizes, specialised in one type of analysis (fraud prevention, peer-to-peer payment, consolidated financial view, etc.). Thus, the longer the chain, the more players are likely to "capture" the data. Digitalisation of payments increases the possibilities of circulating these data and combining them with other data. Payment data are likely to fuel a "surveillance economy" like the data of Chinese internet giant Alibaba (via its AliExpress e-commerce and Ant Financial banking subsidiaries, using the Alipay payment solution) used to populate the Chinese social credit system.[23] The question also arises in Europe, even if the current regulations prevent such a scenario.

Anonymity

Another important issue concerns the anonymity of transactions, which is made possible by the use of cash and is at the heart of the current transformations of means of payment. The choice of a means of payment is in fact determined mainly by the characteristics of the transactions and the ease of use. While the use of cash is more frequent for populations with lower incomes, the main criterion for choosing the means of payment is the value of the transaction. In 2019, 92% of transactions under €5 were made in cash in the euro area[24], although the situation has since changed with the pandemic.

Cash is also preferred for in-store payments and was used in France before the pandemic for more than 50% of payments under €20.

Cash has advantages that make its total disappearance unlikely. At this stage, cash is the only means of payment universally accepted throughout the territory for any form of payment. In addition to the discharging effect, access to cash is easy and its use guarantees the anonymity of the transaction, hence its popularity with the general public. However, the risk is that, in the words of Tim Wu, a form of "tyranny of convenience" could appear[25]: by making the alternatives to cash sufficiently practical in everyday life, the share of cash could inexorably decrease. The use of cash thus has the potential to become quite marginal, which would have consequences in terms of social inclusion and the protection of privacy (see also the contribution of Marc Schwartz, page 19).

Several national economies have already gone cashless. In Sweden, for example, the Swish application, introduced in 2012 by six Scandinavian banks, is now used by more than 50% of the population for small-value transactions. In China, driven by Alipay and WeChat, 80% of payments were made via mobile in 2018 compared with less than 20% in 2013. From 2010 to 2016, Sweden went from 40% to 15% cash transactions in shops. Advocates of the "cashless" system point out the efficiency, the time and money savings, the security of this means of payment for customers and merchants, and the fight against fraud and terrorism. For French banks, the reduction in the proportion of cash and cheques, which are very expensive means of payment to maintain (€10 to 15,000 per year for a cash machine), represents a major profitability issue.

The disappearance of fiat money would also present important issues for privacy and freedoms. With cash, transactions between two people can be done without any third party knowing.

23 - See for example "The social credit system • How China assesses, rewards and punishes its people", July 2019, institut-thomas-more.org.
24 - ECB SPACE study, already cited, table 11 page 31, December 2020, ecb.europa.eu.
25 - "The tyranny of convenience", 24 March 2018, lemonde.fr.

Businesses cannot advertise based on transaction patterns or sources of income, or assign a credit score, governments cannot track these expenses, and a spouse with access to the joint account will not find out what gift they are going to get. The end of cash would mark the end of anonymous transactions. It would become possible to systematically track payments, to know what a person has bought, from whom, how often and at what price. This traceability would certainly facilitate, in our longitudes, the work of public administrations to identify tax fraud, but the price to pay in terms of privacy would perhaps be disproportionate.

Beyond payments, anonymity appears to be an essential condition for the functioning of democratic societies: it is through the defence of anonymity that several essential fundamental freedoms can be exercised (secret ballots, freedom of anonymous publication, anonymity of hospital care, professional secrecy, secrecy of correspondence, freedom to come and go anonymously, etc.). And if there is no right to pay anonymously, does this possibility not support a number of other rights and freedoms, given the links between payment data and the location, health or purchase data they contain or on the links between people? From this point of view, breaches of anonymity in payments should be accompanied by reflection on their proportionality and their necessity in a democratic society, to use the terms adopted by the case law of the CJEU.

Over to...
MARC SCHWARTZ

Marc Schwartz *has been CEO of the Monnaie de Paris since December 2018 and teaches economics of media and cultural industries at the École des affaires publiques de Sciences Po Paris. Starting out at the Court of Audits, before moving to the Treasury Department, France Télévisions and the Mazars firm, he was also director of the cabinet of the Minister of Culture (Françoise Nyssen) in 2017. He graduated from Sciences Po Paris, was a former student of ENA and holds a Master's degree in corporate finance and an Executive MBA.*

During the COVID-19 health crisis, contactless payment has grown significantly. The idea that our societies were gradually and inevitably moving towards a cashless future was relayed widely in the media. Wrongly, according to Marc Schwartz, CEO of the Monnaie de Paris.

In your study *"The great paradox - or why the reign of cash is far from over"* published by Terra Nova[26], you disagree with this alleged evidence. What is your analysis based on?

First of all, the numbers speak for themselves. There has never been so much cash in circulation around the world, and this amount has never stopped growing! The volume of dollars and euros in circulation has increased annually by 6 to 8% over the last twenty years. At the end of last year, there were over €1,400 billion in coins and banknotes in circulation. And in 2020, in the midst of the health crisis, there was even more of an increase: +11% for the euro and +15% for the dollar. If cash were disappearing, the reverse would be true.

I would also like to reiterate that cash is the only form of currency issued by central banks that is accessible to the general public and that it therefore constitutes one of the pillars of confidence in money. It is no coincidence that citizens refuse to give up cash. When asked, the vast majority of them say they are in favour of maintaining cash, proof of a real attachment to physical money. Eight out of ten households in France and seven out of ten households in the United States are opposed to the disappearance of cash; and 74% of the British believe that a world without cash would deprive them of their freedom of choice.

Finally, cash remains a popular payment method for individuals. The latest study published by the European Central Bank (ECB) establishes that in 2019, almost three-quarters of payments at points of sale in the euro area were made in cash, representing 48% of the total value of payments.

> ***It is no coincidence that citizens refuse to give up cash***

26 - *"Le grand paradoxe - ou pourquoi le règne du cash est loin de s'achever"* (The great paradox - or why the reign of cash is far from over), 8 January 2021, tnova.fr.

Contrary to popular belief, and even if its use is decreasing, cash therefore remains a popular method of payment for European consumers.

What are the advantages of cash that guarantee its long-term maintenance?

Cash is a universal, secure and completely free means of payment that individuals can use to pay for their expenses instantly. It is the only form of currency with legal tender status and immediate discharging effect, even if it is governed by regulations. Bank cards or payment apps do not have such a privilege and are far from universally accepted - and let's not get started on Bitcoin!

Cash enables those who do not have a bank account or card, or who are not sufficiently au fait with digital tools, to access a means of payment. Without cash, millions of people would be unable to purchase essential goods and would find themselves even more marginalised from society. In France, where the banking rate approaching saturation, 3 million people are nevertheless in a situation of financial exclusion.

Access to digital services is just as discriminating: INSEE considers that one in six French people suffers from "digital illiteracy". Financial inclusion is therefore a major reason for maintaining access to cash. The ECB also considers that the possibility of paying in cash "is important for certain groups who, for many legitimate reasons, prefer cash to other payment methods, or those who are not in a position to use digital technology".

In addition, cash is resilient: it does not need a power supply or an internet connection. Finally, it is also a savings vehicle, to which households, especially the poorest ones, turn in times of crisis. Like gold for the wealthiest households, cash is a safe haven, especially when interest rates are low or even negative. This hoarding role can help to explain the rebound in demand for cash worldwide in 2020.

Beyond the essential role that cash plays in the financial inclusion of the least advantaged households, how do you explain everyone's desire to maintain it?

This attachment to cash can be explained rationally, but also psychologically or symbolically.

First of all, the maintenance of cash stems from the protection of individual freedoms. The availability of a variety of payment methods allows you to choose between them, according to your preferences and according to the circumstances. This freedom of choice is the surest guarantee of confidence in money.

In addition, cash can be used to settle a transaction immediately and anonymously, and therefore protects individual data. And this anonymity is not, for the vast majority of households, a screen for illegal activities!

Card or online payments leave a trace that can be accessed by private companies, which can use them for advertising purposes This is what the Internet giants are doing, and it explains their recent attraction to the payments market. The data could also be used by governments with little concern for public freedoms. Warnings about the possible harmful uses of payment data are emerging from China, where some might be tempted to use social media, for example, to publicly humiliate individuals behind on debt payments.

In addition, and while it goes without saying that cash can be used for illegal purposes, its use is more strictly controlled nowadays: limits on payment in cash in shops or to pay taxes, bank investigations in the event of significant movements, etc. And it is worth noting that fraud with electronic means of payment is developing, for example in Africa with mobile phones or via cryptocurrencies. Finally, money is not only a disembodied means of payment, but also an institution that creates meaning and signals belonging to a community. As economist Jacques Mistral recently said: "money is not a thing, it is a social relationship".

Over-identification

Combined with these issues of anonymity of payments is the question of identification. The use of cashless payment methods requires the bank to know the identity of the debtor and the creditor, but this identity is increasingly required by other services using payment data, to avoid fraud, for example. The evolution of payments, in particular the growing share of remote payments, therefore generates a risk of "over-identification" of individuals, of disclosure of their identity attributes beyond what is necessary to provide the requested service, which can most of the time be provided on the basis of a declarative identifier or even a pseudonym.

In the name of the fight against financial crime, of all forms of fraud (payments, tax), and ultimately of a broadening of the points which need to be monitored, "the danger is that payment turns sanctimonious", in the words of a lawyer, and that the traditional principle according to which the payment operation is independent of the underlying transaction and does not have to know anything about it, is gradually lost sight as operations become digital. The general public does not want it, and is rather reluctant to use an official (or "sovereign") digital identity for financial purposes (online payments, online banking, credit applications, etc.), whereas the use of a sovereign digital identity is more accepted for administrative procedures, although not by the majority (see Figure 4). In the end, the public appears to be quite aware of the pros and cons of identification for each use case.

.

Figure 4

The need for a sovereign digital identity for the French depending on the situation.

Source: Ifop survey for Public Authorities/EY, March 2021

Inclusion

A fourth issue concerns financial and social inclusion. The evolution of means of payment towards increasingly digital solutions has mixed effects. On the one hand, the dematerialisation of payments raises the question of the "digital divide" and the accessibility of the corresponding solutions, particularly in France where, according to INSEE, one in six people do not use the Internet (more than half of people over 75 do not have Internet access) and more than one in three users lack basic digital skills[27]. A quarter of French people do not have a smartphone, because although almost 100% of the 18-40 age group have one, this is not the case for more than half of French people over 70, and also a quarter of the population does not have a computer, according to Crédoc[28].

Access to universal payment services for the population is therefore an issue, especially when authentication is required to use the service. Thus, the widespread reliance on strong authentication through the use of online banking apps following the full entry into force of the PSD2 Directive brings with it inclusion issues for people who do not have a smartphone. This is why tlicéité

he public authorities ask banking entities to offer alternatives, at least one of which should be free.

On the other hand, the development of alternative means of payment and solutions can promote financial inclusion, for example by lowering the cost of money transfers or by providing new cheque-cashing or online sales services to very small companies hitherto deprived of these options. According to the International Monetary Fund, these benefits can be observed in particular in developing countries[29], less so in a country like France.

State surveillance

As a consequence of their wealth for understanding the scope of individual acts and their high traceability in payment systems, payment data are of particular interest for detecting crimes and offences. The monitoring of transactions is thus one of the components of the obligations of financial entities in terms of the fight against money laundering, and we know that anonymous cash transactions involve more risks in this respect, as well as in the fight against tax fraud.

The subject of anti-money laundering and counter-terrorism financing (AML-CFT), one of the challenges of which is effective coordination with the GDPR and which is covered by other work being carried out by the CNIL and the European Data Protection Board[30], is not specific to payments and will therefore not be developed further in this White Paper. Of course, new digital technologies can give rise to new risks in this area as well as the possibilities of tracing transactions more closely to counter them. However, these issues generally concern crypto-assets, which are more stores of value used for speculative purposes than, to date, means of payment per se (see box on crypto payment on page 43). The same debate is under way with regard to the digital euro, which is expected to have the same characteristics as cash (see page 45 et seq.).

For the same reasons, payment data have also become, since the attacks of 11 September 2001, an issue for the intelligence services. In 2006, the European data protection authorities received complaints about the SWIFT interbank payments system, which provided data to US authorities without the knowledge of the data subjects. In 2013, the Snowden affair revealed that analysts at the US National Security Agency were using a so-called "follow the money" approach using financial data, credit card data in particular. According to the German weekly Der Spiegel, this surveillance was carried out mainly in the United States but extended to Europe, Africa and the Middle East, priority theatres of operations for all intelligence services.

From this perspective, there is no doubt that payment data, means and systems are subject to sovereignty issues both for European citizens and for European States, which have enacted rules for the protection of the personal data of their citizens (see page 70 et seq.).

27 - "The skills of the French in the EU average". One in six people do not use the Internet, more than one in three users lack basic digital skills, 30 October 2019, insee.fr.
28 - "2019 Digital Barometer", November 2019, credoc.fr.
29 - "Digital financial inclusion in the times of COVID-19", 1 July 2020, imf.org.
30 - "Statement on the protection of personal data processed in relation with the prevention of money laundering and terrorist financing" (PDF, 70 KB), adopted on 15 December 2020, edpb.europa.eu.

FOCUS ON...

AML-CFT and protection of personal data

As part of the ongoing review of European texts governing this area, the principles of personal data protection can help strengthen the effectiveness of the AML-CFT framework insofar as the data used by the latter, whether due to the obliged entities or their third-party sources, are accurate, relevant and up-to-date, in support of a targeted and proportionate risk assessment.

This is why the European Data Protection Board (EDPB) sent a position letter to the other European institutions in May 2021[31] reiterating the importance of striking the right balance between the prevention of AML-CFT risks and the protection of personal data, both in the interest of public freedoms and for the legal security of the operations of obliged data controllers in the fight against money laundering.

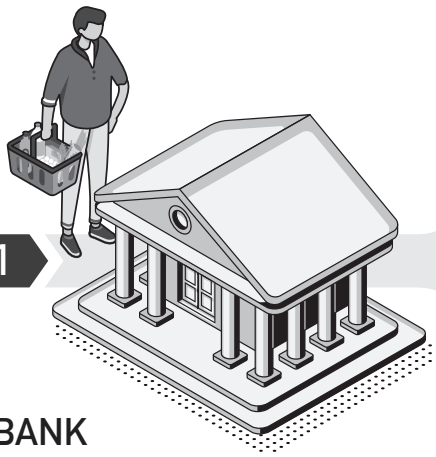
In this letter, the EDPB recommends in particular the adoption of a specific framework of lawfulness with regard to personal data provided by external sources, the definition of standards of proportionality based on a risk-based approach, and clarifications with regard to minimisation of the data collected. It recommends that the data used, both by obliged entities and by their external sources, be accurate, reliable and up-to-date, and that the retention periods for these data shall not be excessive. It stresses the need to adopt a specific legal framework, with suitable safeguards, to be able to process sensitive data or data relating to criminal convictions and offences. Finally, it calls for cooperation between supervisory authorities when drawing up guidelines, at both European and national level.

In general, the link between AML-CFT rules and the GDPR must be guided by the principles of necessity in a democratic society and proportionality of the breaches of the rights to privacy and to data protection enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.

31 - EDPB letter to the European Commission on the protection of personal data in the AML-CFT legislative proposals (PDF, 235 KB), 19 May 2021, edpb.europa.eu

FROM ACCOUNT TO ACCOUNT

Simplified mapping of means of payment and the key players involved.



1

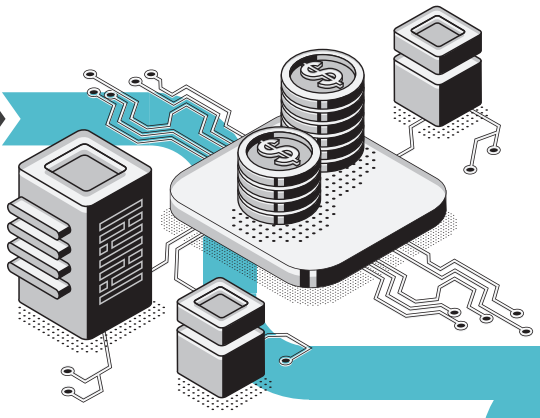
BANK

Provides banking services, such as a bank account or an online banking application.

HSBC

Fraud prevention, initiation, cashback

3



ELECTRONIC MONEY

Money stored electronically, independent of a bank account. Can be managed through an e-wallet.

Skrill PayPal payLib

PAYMENT CARD SCHEME

Defines the rules for their interoperability between banks, including abroad.

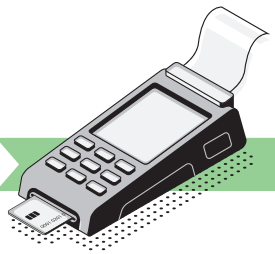
4

VISA

CB

mastercard

7



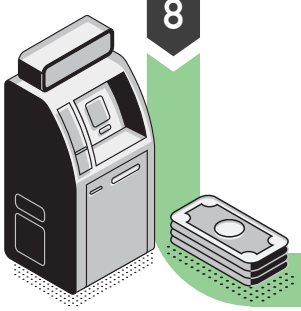
ELECTRONIC PAYMENT TERMINAL

Reads data from a card to authenticate and initiate a transaction with a merchant.

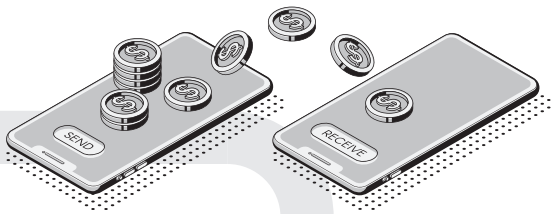
CASH

The most anonymous way to make purchases, cash can be withdrawn from a cash machine.

8



Online transactions
Point-of-sale transactions



2

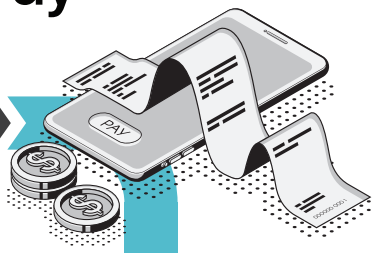
TRANSFERS

Transfer of sums directly from one account to another.

HUAWEI pay

Pay

SAMSUNG pay



5

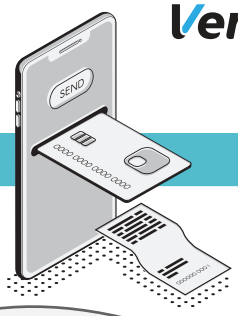
MOBILE PAYMENT

Allows payments to be made with a phone.
Usually associated with an e-wallet.

stripe

Square

Verifone

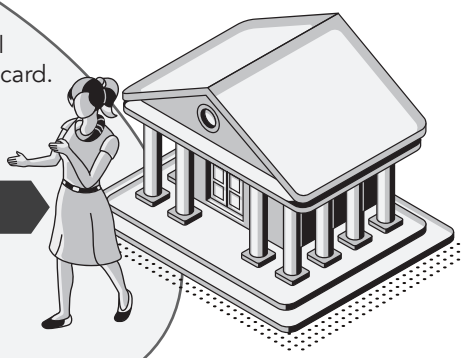


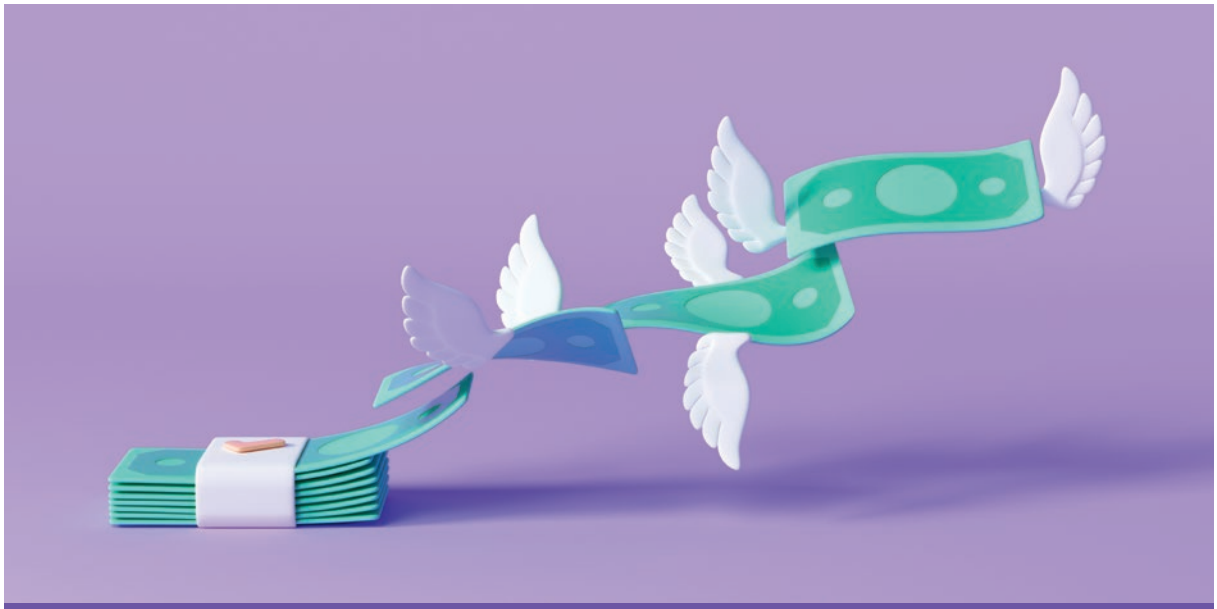
6

PAYMENT SERVICE PROVIDER

Allows merchants to accept physical or online payments, often made by card.

Scoring, billing, loyalty programme, split payment





OLD AND NEW MEANS OF PAYMENT: a complex ecosystem, new players

From an economic point of view, it is important that the payment operation, which is the counterpart to an underlying transaction (order of an item, provision of a service, delivery of a financial asset) and which results in a movement of funds, is settled with the right recipient, if possible quickly and at low cost. The operations that interest us here take place between a natural person and a professional, typically between a merchant and their customer. From the customer's point of view, the goal is fluidity and ease of use, but the techniques used to achieve this goal can be very complex. They are based on infrastructures developed by banks and purchased by merchants, which have two main aspects: a body of transaction management rules and a distribution of costs ("business model").

The main payment infrastructure in France for individuals is the physical electronic payment infrastructure of so-called "bank" cards, which accounted for 58% of cashless payments in 2019[32]. This infrastructure is very expensive since it represents, in France alone, several billion euros in commissions per annum[33], but it is also very efficient in terms of speed and ease of use. It is also not very sensitive to fraud (0.064% in 2019 according to the report of the Observatory for the Security of Means of Payment (OSMP)[34]). Its only real competitor is cash which, in 2019, represented 59% of the total number of transactions in France[35].

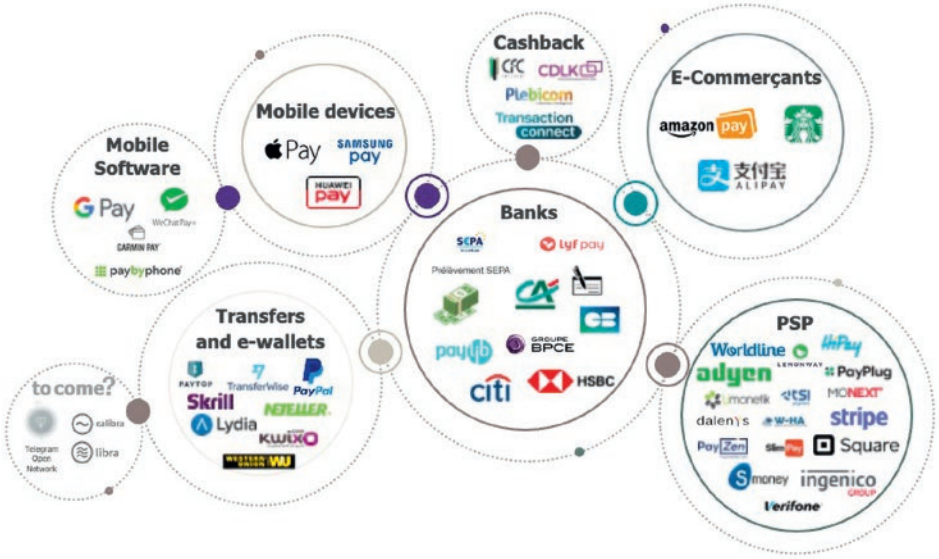
The payments industry is complex and the interests of the different players do not always converge: banks, card "schemes", merchants (large and small), physical (PSP) or online (e-PSP) payment service providers, some of which specialise in wire transfers, e-wallets, cashback solutions, but also e-commerce merchants, electronic money providers and mobile payment (X-pay) operators, which for the latter are purely digital players. Some are the result of an outsourcing of banking services (card schemes, PSPs), while others intermediate between the customer and the bank to capture the economic value which is often based on the corresponding data (e-PSPs, X-pay solutions). They often build on the existing payment infrastructure, where they bring about optimisations to reduce transaction times or costs or offer new services based on the analysis of transaction data.

For instance, the card system can be partially reused for e-commerce, for which **80% of turnover in France is via a card**[36]. But the challenges of online payments and the corresponding players differ greatly, with higher risks for data protection because, while the physical electronic payment circuit is closed by strict information management rules, the movement of data on the internet is by design open and inexpensive. The risk of fraud is therefore higher there (for cards, 0.17% compared with 0.01% at a physical point of sale).

Figure 5

Representation of the payments ecosystem.

Source: Wavestone study for the CNIL, December 2019



32 - Map of cashless means of payment, report of the 2020 collection (PDF, 2.2 MB), page 112, banque-france.fr.
33 - Between €1.2 and €1.8 billion per year payable by merchants (€600 billion in 2019 in France, amounts of card payments according to the Banque de France, between 0.2 and 0.3% interchange fee on these amounts); for cards €30 to €50 per annum and per card according to experts with 71 million cards in circulation in 2019, i.e. between €2 and €3.5 billion payable by cardholders. Note that the Pauget-Constans report estimated this amount at €2.6 billion in 2012 (Source: economie.gouv.fr).
34 - Observatory on the security of means of payment, 2019 annual report (PDF, 1.8 MB), page 19, banque-france.fr.
35 - Study on the payment attitudes of consumers in the euro area (SPACE), December 2020, ecb.europa.eu.
36 - Compared with 11.5% for e-wallets, 4% via consumer credit and only 1% for transfers or direct debits (Source: 2018 Fevad figures).

A HISTORY OF PAYMENT DATA AND MEANS OF PAYMENT IN THE 20TH CENTURY

The first of the modern-day means of payment, credit cards were introduced in the United States in the early 20th century. They serve as an interface between the customer's identity and account, ensuring a relationship of trust between the vendor and the buyer for a given transaction.

In 1914, Western Union, the main telegraph company in the United States at the time, issued its customers with paper cards that indicated their identity and allowed their accounts to be linked to their invoices. In many firms and department stores, systems started popping up to make the link between the customer's identity and their transaction history. These payment devices were not universal in that they were limited to each store (or chain of stores), but they also played the role of loyalty card. At that time, they were not associated with a bank account.

It was not until the 1950s and 1960s that universal credit card systems gradually emerged with the creation, through partnerships between banks, of large infrastructures that would become the American Express, Visa and Mastercard schemes. The rise of the major card schemes was gradual. At the time, the credit system was based on the transmission of carbon copies and their manual transcription, which was difficult to manage for both merchants and banks. As a result of these operational difficulties, little transactional data was kept by credit card companies on their customers. It was not until the 1970s, with the rise of IT and under the requirements of regulatory changes (aimed at greater transparency), that the first databases were created to keep a standardised history of transactions for each individual listing the date, amount, location and a brief description of each. There was still little data and what there was rather shallow, given the state of technology.

Controlling its entire infrastructure (unlike Visa and Mastercard, which were backed by a network of banks), American Express was one of the first operators to amass these transactional data and transform them into a marketing database. American Express customers are segmented and listings sold to businesses to deliver targeted advertising. For airlines, hotels, car manufacturers and other retailers, these partnerships provide access to valuable data on transactions completed by their customers.

The current desire of American Express to integrate receipts into its payment data must also be understood in this context[37].

The rapid growth of Visa, Mastercard and American Express universal credit cards led to merchants losing exclusivity to the information they held about their customers. Through their loyalty cards and their own credit cards, they had been able to gradually build up databases allowing them to better understand the purchasing behaviour of their customers, by associating purchases with a customer under all the brand's names. Loyalty cards make it possible to collect information such as the identity of the consumer, the date and time of the transaction as well as the products purchased. On the contrary, the current large card schemes rely on banking operators and the trust they generate, thereby reserving access to payment data to banks while reusing them for their own account in order to develop fraud prevention services, for example. This is also the case in France with the Cartes Bancaires economic interest group, a national network created in 1984, controlled by the French banks and which centralises the data of the vast majority of transactions, but backed by large global schemes, especially for international payments.

This history should, at a time when payment systems are being revolutionised by e-commerce, teach us that payment data and underlying customer knowledge are the subject of rivalry between banks and merchants, including through service providers, the outcome of which results from the state of the art and the configuration of the players and may result in intense exploitation.

37 - *"Digital Receipts feature from American Express helps Card Members identify, and remember, purchases and helps merchants reduce disputes"*, 18 February 2021, americanexpress.com

THE CARD AND THE "FOUR CORNERS" MODEL, A SECURE BUT COMPLEX MODEL

Today, the path of payment data in the most common scenario in France, that of a card transaction, is both complex and stabilised. It involves a traditional "four corners" model (payer-payer's bank-beneficiary's bank-beneficiary), which applies both at the physical point of sale and remotely:

- **On the customer's side,** a card comprising a pseudonymous identifier known as the PAN or Primary Account Number, the number appearing on the bank card, allowing it to be authenticated, with or without a PIN, with the account of its bank known as the "issuing bank", the bank that finally settles the payment.

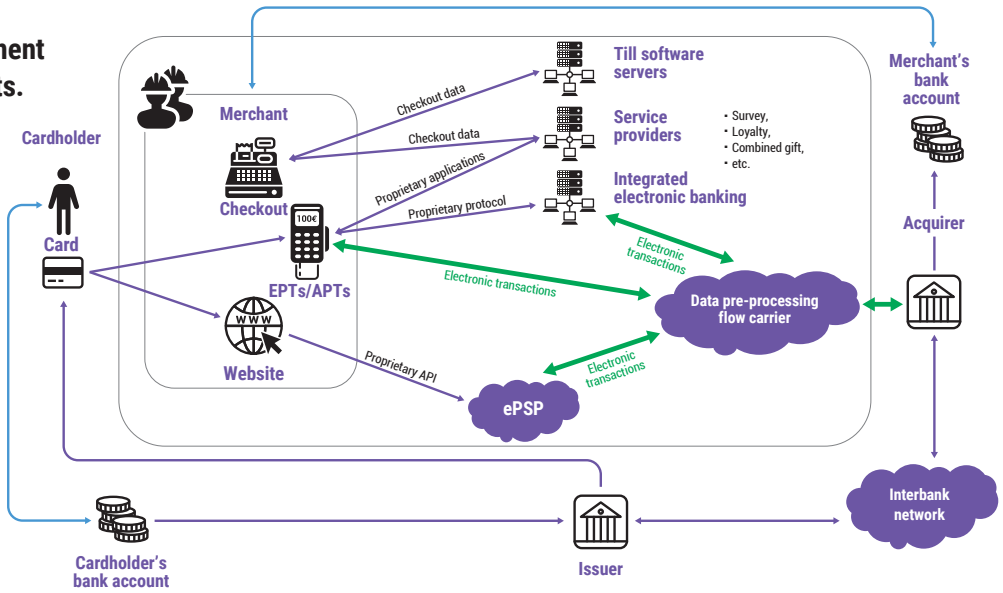
- **On the merchant's side,** equipped with an electronic payment terminal (EPT) at the point of sale or an online payment function (by SDK or external service provider), the data feeds into a double circuit: a payment "rail" on the one hand, allowing the merchant's bank or "acquiring bank" to request a direct debit authorisation from the issuing bank on the customer's account authenticated by their PAN and then to receive the corresponding authorisation; and a checkout circuit enabling local traceability of transactions, with more data (email, purchasing data, etc.) and possible interconnections with third-party services (loyalty, billing, reservations, etc.).

In this complex model, the quality of the rules followed by payment data is crucial, both for the security of transactions (protection of identifiers) and for the control of their data by the customer. Although the circulation of identifiers on the green arrows in Figure 6 is encrypted and standardised by the large international schemes (EMV standards, PCI-DSS standards, etc.), these rules are not mandatory and the proper protection of the checkout circuit depends on merchant behaviour and the quality of the till software.

From the point of view of security and data circulation, the "four corners" model works in a degraded mode for remote transactions, which, as the diagram shows, do not pass through the very secure infrastructures of the international schemes in the first stages of the transaction.

In addition, the distinction is less clear between payment data themselves and the ancillary data used by the e-PSP or the site itself for the purposes of fraud prevention, customer knowledge, targeted advertising, etc. without the data subject being aware of these operations and by which service providers they are carried out.

Figure 6
Circulation of payment data, card payments.
Source: Association du Paiement, January 2021



PAYMENT SERVICES, A TWO-SIDED MARKET

The four-corner model also illustrates the special nature of payment services, a prototype of a two-sided market[38], the operations of which bring together two different types of clientele: end consumers on the one hand and merchants on the other. These transactions assume that there are one or more intermediaries (card scheme, PSP, etc.) with, on one side of the market, the issuance of the payment instrument and, on the other side, the acquisition of the transaction.

Each player in this market has the possibility of balancing its business model, by varying the price to the consumer (for example by charging for issuance of the payment card, or the deposit of cheques) or by using a commission taken from the merchant, according to the willingness to pay of one or the other client. This type of market is also characterised by cross network effects: as the case of the card illustrates, a means of payment is all the more popular with consumers if it is often accepted by merchants, and vice versa.

This type of market has developed abundantly in the digital realm, where search engines or social networks offer their services free of charge to consumers and charge advertisers for advertising. Likewise, in the payments industry, American Express has chosen to offer very advantageous conditions to consumers (going so far as to offer it a form of remuneration in the form of "miles") but imposes a high commission rate on merchants.

Like digital players and as demonstrated above, the use of payment-related information is also one of the factors in the business model of these intermediaries, which can provide new sources of income in the form of targeted marketing or fraud prevention services. On this last point, the Banque de France itself insists on the necessary compliance with the GDPR of these processes as they involve growing data collection[39].

From a data protection point of view, the two-sided nature of this market puts payment operators in a position, at least in theory, to be able to collect personal data from both sides of the market (banking data on the one hand, purchasing or contextual data on the other) in order to enrich them, combine them and reuse them as they see fit to diversify their income. This type of player is encouraged to collect more data than the consumer would have spontaneously wished[40].

This is why, as the rest of this White Paper illustrates, there is a natural tendency in the payments market to collect "enriched" data in order to "create new services", and similarly this market tends to attract operators whose business models are based on combining and reusing data. However, due to the strength of the network effects, developments in the payments market are slow and new risks (both competitive and data protection risks) are only gradually unfolding[41].

38 - Rochet J.C., Tirole J., "Platform Competition in Two-Sided Markets", Journal of the European Economic Association, June 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", NBER Working Paper No. 28023, December 2020.
41 - Li B.G., McAndrews J., Wang Z., "Two-sided Market, R&D and Payments System Evolution", Journal of Monetary Economics Volume 115, November 2020, pages 180-199.

FOCUS ON...

The sector-specific inquiry of the *Autorité de la Concurrence* into FinTechs (April 2021)

In early 2020, the Autorité de la Concurrence (French Competition Authority) began to work on an own-initiative opinion on the competitive situation in the sector of the new technologies applied to financial activities and more specifically to payment activities. As well as looking at the industry from a competitive point of view, its opinion[42], to which the CNIL contributed, highlights the important role that personal data (and their regulation) can play in the articulation of payment-related business models.

The opinion distinguishes three groups of players with different strategies. Traditional banking players, on the one hand, adapt to changes in supply and demand by investing in FinTechs to create synergy or capture new markets, by forging partnership agreements with major digital players and by continuing to invest in customer experience and user-friendly services. FinTechs, with a wide variety of profiles and economic models (start-ups, online banks and even large retailers) are renewing the offer and are increasingly reliant on banks to benefit from their trust capital in terms of privacy, their distribution channels, their customer knowledge and their compliance function. The major digital players, finally, rely on their extensive community of users and above all have access to large volumes of data that they can use with their mastery of data processing technologies and artificial intelligence. Their marginal costs are lower than those of banks and they benefit from other sources of income that allow them to offer services presented as free to their users and favour the ergonomics of their solutions. The opinion thus emphasises these very significant competitive advantages.

The Autorité de la concurrence then raises several points of attention, some of which are particularly interesting from the point of view of the dialogue between regulators. First, it notes that payment tends to disappear as a stand-alone service, making it more difficult to define the relevant market. It then raises the subject of more competitive access to the NFC antenna of smartphones for the development of mobile payments, which reveals a trade-off between security and innovation. Finally, it revisits the competitive advantage that large digital platforms, or at least some of them, enjoy as a result of the combination and reuse of payment data (see page 20) in other business lines, and the effects of locking consumers into a given ecosystem that may be involved in the deployment of these solutions. "Payment data could, combined with the data collected in the context of their other activities, give these actors an unrivalled knowledge of the market and, consequently, an unparalleled competitive advantage that would be very difficult for a competitor to replicate. (...) For example, in the context of a merger, in view of the limits set by the General Data Protection Regulation, the ability of the companies concerned to combine different sets of data previously held separately raises questions" (p.110 of the opinion).

42 - "FinTech" sector-specific inquiry: the Autorité de la concurrence issues its opinion", 29 April 2021, autoritedelaconcurrence.fr

THE CENTRAL ROLE OF BANKING ENTITIES: THE TRUST ARGUMENT

Prior to the payments revolution we are now witnessing, the bank/card scheme pairing had pride of place, and in many still does today. Today, it is the commercial banks that manage risk and provide the interface between and with consumers, with a good level of consumer confidence.

According to a survey carried out by Ifop for the French Banking Federation[43], banks are trusted by 60% of respondents (35% disagree) and increasingly integrate new technologies for 85% of respondents (10% are of the opposite opinion), although 34% of respondents say they have not downloaded an online banking application (especially those over 50 and retirees). In fact, 70% of respondents trust banks to secure their personal data, compared with 35% who trust GAFA, for example.

Within banking services, innovations concerning means of payment are among the best known and the most commonly used, in particular contactless payment, payment by smartphone and even other forms of e-wallet used by 22% of respondents. Even if respondents' expectations are based more on security than innovation, payment is thus proving to be a relevant innovative strategy (and source of income diversification) for banks.

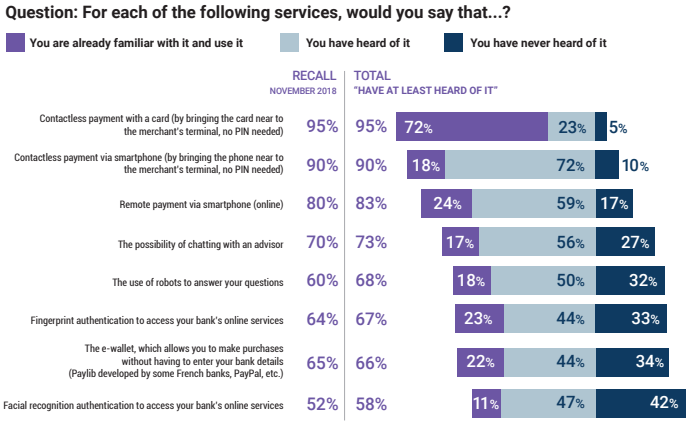
But the banking business model is itself evolving due to the now integrated digitalisation of services. According to the Deloitte survey on "The French and new financial services" at the beginning of 2020, 10% of French people said that they are customers of a mobile bank (e.g. Ma French Bank, Orange Bank, Revolut or N26), and 64% of them use it as their main account (+16 points in one year).

Thus, banks can provide access on their systems to services offered by third parties, such as identity verification, real estate searches, peer-to-peer loans, etc. According to the ACPR, "the role of online banks and neobanks in the race for innovation deserves to be highlighted. In the field of mobile phones or the innovative use of data for marketing purposes, these new players are particularly active. (...)

Figure 7

The new means of payment are the banking services best known to the French.

Source: Ifop/FBF, February 2021



For now, traditional banks continue to be favoured for traditional banking operations such as credit applications, but online banking appears to be a good compromise in terms of image and trust when it comes to simple transactions such as payments, while confidence in new players is lower. In this context, the "platformisation" strategies chosen by certain online banks, welcoming into their system new services developed by new independent players, taking advantage of the "natively digital" nature of their information systems, appear to be a credible alternative to the traditional banking model.

When they belong to already established banking groups, they can therefore play an innovation and experimentation laboratory role within them. In all cases, they have established themselves as essential players in the future transformations of retail banking"[44]. We can bet that this transformation of banking models will not make them lose their data protection compliance experience.

43 - *Les Français, leur banque, leurs attentes* (The French, their bank, their expectations), study no. 2, February 2021, fbf.fr.
44 - *Étude sur les modèles d'affaires des banques en ligne et des néobanques* (PDF, 723 KB), coll. Analyses et Synthèses, October 2018, acpr.banque-france.fr.

THE FINTECH WAVE: NEW CUSTOMER EXPECTATIONS, NEW PRACTICES

What we now call "FinTechs", a contraction of "finance" and "technology", were born out of the 2008 financial crisis in English-speaking countries. At that time, innovation shifted to start-up players, who were offering new services under preferential fluidity and consumer experience conditions, while the principle of "open banking" emerged alongside the development of online banking.

While the new FinTechs had no choice but to use their customers' account identifiers, under questionable security conditions, it seemed preferable to standardise their access to bank accounts in return for an obligation for banks to open them. FinTechs are present in a range of financial services but, in the field of payments, there are two main families: payment initiators, like the German Sofort, which needed visibility of the account balance to launch a payment transaction, and account aggregators, like the French firms Bankin, Budget Insight and Linxo, which provide consolidated information on all of a customer's bank accounts. This movement led to the adoption of the second European Payment Services Directive in 2015.
The implementation of the PSD2 has had several important consequences in terms of payment data:

- **it reinforced the rule provided for by the GDPR** according to which the customer and not the bank or the PSP has sovereignty over the use made of their data;

- **it broadened the scope of payment data** considerably without giving a precise definition, while allowing uses ancillary to payment services, which are not themselves defined;

- **it created a security standard on the market** with strong authentication and APIs, from which other services and uses will be able to draw inspiration in the future using this tendency of individuals to authenticate themselves.

From an economic point of view, the major danger of "open banking" for the banks is the risk of being intermediated and losing control of the customer relationship. They could risk being confined to a managerial role with low added value. But in reality, the relations between banks and FinTechs are more symbiotic. To stay in the game, banks must adapt and focus on customer experience and support, even if it means absorbing certain FinTechs to benefit from their experience or their service.

> ***"FinTechs are setting new banking standards by offering their customers cheaper and more personalised alternative solutions"***

Some FinTechs also offer services for banks to support them in their digital transformation process.

Finally, thanks to these new players, we are witnessing the development of services that complement the means of payment and which are intended for customers (loyalty cards, e-receipts, mobile banking services) or professionals (fraud management, customer data analysis, loyalty programme management), in addition to "bare payment" which is no longer considered an attractive business model. Another example is the development of so-called "split" or multi-instalment payments ("Buy Now, Pay Later"), half way between payment and credit, which requires assessment by the FinTech of the credit risk, with a significant amount of data being processed. In this way, electronic means of payment are often an entry point for reconsidering knowledge and customer relations. But these players are not exempt from financial risks either, as last year's Wirecard scandal[45] in Germany demonstrates, illustrating an investor bias overly favourable to online payments.

45 - This payment acquisition service provider, which operated under a banking licence and was listed on the Frankfurt Stock Exchange, specialised in online payment processing. It went bankrupt in 2020 after the discovery of fraudulent transactions in emerging or developing countries, disguised in its accounts.

In the end, the operational implementation of the PSD2 Directive is not expected to result in a disruption of the banks by FinTech players. Indeed, the latter need the collaboration of the banks to offer their customers a quality experience (as illustrated by the delicate implementation of data exchange interfaces or APIs, whereas the European Banking Authority recently called for national supervisors to remove such obstacles) and the tendency is rather for banking groups to take over FinTechs.

From the point of view of compliance, these changes do not constitute a weakening, even if determining factors other than simple commercial success now intervene in business models. We perhaps remember the rapid rise in the British market of the young start-up Pingit, launched by Barclays in 2012, but whose deployment was subsequently hampered by internal conflicts within the group.

These changes are by no means over, since the European Commission is due to launch the review process for the PSD2 directive at the end of 2021.

Finally, the issue of trust is crucial for these players. According to the Deloitte study on "The French and new financial services" (already cited), although FinTechs are seen as products of the future, a fairly marked perception of the risks associated with FinTechs by the public persists even if the services offered by the latter are increasingly well known. Only 40% of respondents would agree to entrust them with more personal data, for example, testifying to an important support stakes by the CNIL in this area.

FOCUS ON...

Portability of payment data

The question of the portability of payment data (sharing of data at a person's request) is not a simple one because it borders on two regulations, one sector-specific (PSD2) and the other general (GDPR). On 15 December 2020, the European Data Protection Board published guidelines to shed light on the relationship between these two texts[46]. These guidelines reiterate the distinction between contractual agreement within the meaning of the PSD2 and consent within the meaning of the GDPR. They specify that payment data within the scope of the PSD2 can only be reused with the customer's consent. Finally, they explain that it is not for the banks to assess the proportionality of the data collection by aggregators, the latter being fully responsible for the compliance of their processing.

In addition, the CNIL recently published a recommendation on the exercise of individuals' rights through an agent[47]. This recommendation specifies that an aggregator authorised by the ACPR is required, within the scope of the PSD2, to comply with the access and transmission rules provided for by this Directive, and cannot exercise for this purpose the rights provided for by the GDPR, such as the right to portability or the right of access, as an agent with regard to the service provider managing the account. On the other hand, it is possible for an agent, even when the latter is also an account information service provider, to exercise the right of access and the right to portability provided for by the GDPR, in its capacity as agent, with an account manager service provider, when the PSD2 is not intended to apply to this operation. This is the case, for example, if the data are accessed within the framework of the provision of a service not subject to the PSD2, or if the data accessed do not come from a payment account within the meaning of the PSD2.

In the latter case, the CNIL has adopted an approach favourable to innovation. It recommends that the data can be ported at regular intervals if the customer so requests, without such a request being regarded as excessive since the data are renewed quickly. In the case of a direct request for portability from one data controller to another, it recommends using the existing technical possibilities of the APIs already developed for the needs of the implementation of the PSD2, rather than extracting content via customer identifiers. The recommendation suggests safeguards to authenticate and secure these transactions.

46 - *Adopted guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR* (PDF, 308 KB), edpb.europa.eu
47 - *"Exercise of rights through a mandate: the CNIL publishes its recommendation"*, 25 June 2021, cnil.fr (in French)

Over to...

BERTRAND PEYRET

DEPUTY SECRETARY GENERAL OF THE ACPR

> ***It is important for authorities such as the ACPR and the CNIL to exercise vigilance and collaborate to ensure compliance with regulations***

Bertrand PEYRET *is Deputy Secretary General of the Prudential Supervision and Resolution Authority (ACPR), in charge of banking supervision and authorisations. Previously, he served as Inspector of the Banque de France, then Director of Banking Supervision and finally Director of Insurance Supervision at the ACPR. He has been a member of the Senior Supervisors Group, chaired the HubGovernance Group (Data Gaps Initiative) and participated in various sub-groups of the Financial Stability Board.*

What is data sharing in the financial sector?

These days, it mainly involves the possibility of sharing payment data (payment transactions, account balances, registered beneficiaries, etc.). Over the past ten years or so, new services have emerged, provided by new players, often FinTechs. They are reliant on access and use of this payment data. Since 2018 and the transposition of the second Payment Services Directive (PSD2), regulations have governed these activities by defining two new services: the payment initiation service, which, for example, makes it possible to transfer money to an online merchant on behalf of the customer, or the account information service which consists, among other things, in collecting data from one or more payment accounts.

How is data shared?

The regulations stipulate that payment service providers who manage payment accounts accessible online must furnish service providers authorised to provide the new payment initiation or account information services with an access interface that satisfies the requirements of the PSD2. This interface, which is often called "PSD2 API", is used to collect data or transmit payment orders, in compliance with the mandate given by the customer and under technical conditions intended to ensure the security and quality of the service.

Are new use cases emerging?

Absolutely. The account information service was originally designed to give users a consolidated view of all of their payment accounts managed by several payment service providers. Today, this vision is outdated. Account information service providers now offer services that go further and allow, for example, more active wealth management by offering investment opportunities or facilitating credit.

Do traditional banks also provide these services?

Historically, banks have had little to do with these account information or payment initiation services. The use of customer data was mainly limited to their use to meet legal obligations such as fraud prevention or the fight against money laundering and the financing of terrorism.

But things are changing. Banks are becoming more and more interested in this area, demonstrated by their entry into the capital of FinTechs and by the direct provision of services to customers relating to management of their payment data.

Do BigTechs provide services based on the use of financial data?

GAFA[48] and BATX[49] are increasingly active in the European payments market. Until now, these players have mainly invested in the payment solutions segment, i.e. applications that interface between a user and their bank to initiate payment transactions. These solutions such as Apple Pay or Google Pay are generally based on the use of payment card data issued by users' banks. In this case, the interest for BigTechs lies largely in the collection of user data, which allows them to develop their historical activities such as targeted advertising or the sale of their products. However, we are also witnessing the emergence of marketplace activities in which these BigTechs can gain possession of users' funds, which requires authorisation as a payment service provider to be obtained. These activities, as well as the economic weight of the BigTechs, which allows them to develop and roll out these new payment technologies on a large scale, justify the vigilance of the regulatory authorities in the financial sector. There should be no difference, in terms of control, in how these players and the FinTechs or banks are treated.

Can all data be shared?

No, not completely. For a start, it should be remembered that account information or payment initiation service providers can only access the accounts and information agreed with their customers.

Then, the PSD2 only processes data from payment accounts accessible online. Access to information relating to insurance contracts or to savings or securities accounts is, for example, not covered by the PSD2.

Is the sharing of financial data and open finance set to accelerate?

In the European Commission's digital finance action plan, published on 24 September 2020, one of the actions is to promote innovation by establishing a common space for financial data. The challenge involves facilitating access to these data by standardising them and providing for an electronic exchange format, promoting innovative solutions to facilitate regulatory reporting, and finally strengthening open finance.

Many users appreciate being able to benefit from innovative and tailor-made services, to better manage their assets, for example, or to facilitate access to other services. However, as long as these services are based on the use of financial and non-financial data, authorities such as the ACPR and the CNIL are justified in exercising vigilance and collaborating to ensure compliance with applicable regulations in this area.

What are the other potential uses of these technologies?

The possibilities offered by mass information processing via artificial intelligence and big data technologies are already partly exploited by institutions subject to ACPR controls. Using this information can help reduce risk in granting credit, but it can also be used to process insurance claims more quickly.

In addition, in certain areas such as the combat against fraud or anti money laundering, the use of innovative solutions based on such tools could help to identify high-risk situations more quickly and more reliably. In this area, too, the adoption of measures at European level to facilitate the exchange of data between establishments, while respecting the obligations relating in particular to professional secrecy and the protection of privacy, is desirable.

48 - US companies: Google, Amazon, Facebook, Apple
49 - Chinese operators: Baidu, Alibaba, Tencent, Xiaomi

PAYMENT, THE "TROJAN HORSE" OF THE BIG DIGITAL PLAYERS?

This wave of innovation in payments is also accompanied by the arrival in the sector of major digital economy operators. Although their point of entry today is payment, and mobile payment in particular (Google, Samsung Pay, Apple Pay), their wish, in the longer term, is to offer other financial services.

Mobile payment systems (X-pay solutions) are developing on the basis of the card infrastructure, which remains omnipresent in this system. Wallets (Apple Pay, Google Pay) are associated with the payment card. The card is saved on the phone, and the payment application is used to pay for purchases instead of the physical card. The rest of the processing of the financial flow is identical to that of the card. This strategy has made it possible to easily associate the banks, since nobody is a priori crowded out in this scheme, even if the partnerships signed with Apple are costly for the banks, who lose part of the commission taken from the merchant, but who anticipate that this model will develop.
However, there are two different strategies between phone manufacturers (Samsung, Apple) and service providers (Google). The former's business model is based on a commission charged on each transaction (the amount varies depending on the agreement negotiated between the banks and Apple or Samsung), as well as on an increase in phone sales as a result of enhanced functionality.

Conversely, the service provider model is based on the collection and use of data in return for a free service. Through these payment services, they seek to occupy a strategic place at the heart of the payment data chain and thus enrich their capital with data on each individual. This model, which banks are more reluctant to deploy, requires greater vigilance on the part of individuals, as the use of data goes beyond security purposes.
Amazon is pursuing a platform strategy similar to that of Alipay (see next page). The Amazon Pay button is available to any classic merchant site and allows it to position itself as a central player beyond the marketplace of its platform (since the customer uses their Amazon account to pay by connecting to it on their terminal). The company also markets (outside the EU) its JustWalkOut instant ayment technology implemented in its physical stores, which allows customers to be charged for their purchases without having to go to the checkout.

For Amazon, the challenge lies in predicting the purchase act by observing the history and contextual data, and targeting the recommendations, with the payment data resulting from the business model.

Whether payment is a source of profitability or data enrichment, it above all enables the major digital players to enter the financial services market in general, by joining forces with historical players for regulatory reasons. Amazon, Apple and Google have thus joined forces with JP Morgan, Goldman Sachs and Citigroup respectively to launch credit cards and consider the creation of current accounts. The development of other banking transactions provides an opportunity to collect additional information on individuals, based on which these companies will tomorrow be able to calculate risk scores and offer more complex products such as loans. They target in particular those excluded from the banking system, in a context where banks have had more difficulty in granting loans since the 2008 crisis, which raises ethical and legal issues. Amazon already offers financial services for merchants on its platform, just like Stripe and PayPal, which offer loans to small merchants.

It should be noted that these strategies designed and developed in the United States are not always transposable due to the obligations in force in Europe, and in particular what it would be possible to do while remaining compliant with the GDPR. These strategies still need to be consolidated on the European market, but they are already forcing traditional players to react. In the opinion of the research firm Xerfi, with the investigation launched by the European Commission in the summer of 2020 against Apple, who is restricting access to the NFC chip in the brand's phones to just the Apple Pay solution, only Amazon's model is a real threat to existing payment players[50], with 30 million users in France and the deployment of the Alexa voice assistant[51].

50 - "Les offensives sur le marché du paiement", Xerfi, February 2021
51 - See, on this subject, the CNIL White Paper on voice assistants, the recommendations of which also apply to payment data - On the record: Exploring the ethical, technical and legal issues of voice assistants, in French (PDF, 6.4 MB), September 2020, cnil.fr.

The Amazon Pay solution complements traditional PSPs: Amazon Pay, which already has the relevant data, executes the payment and offers the merchant transaction reporting, while the PSP acts as a simple gateway with the merchant's site.

Of course, the analysis reported here on the payments market cannot necessarily be transposed to other financial services (insurance, credit).

FOCUS ON...

Chinese players

Further afield, the example of the Chinese company Alibaba also testifies to these reconfigurations. Its Alipay payment service is used by more than a billion users (including two to five million users in France). It offers a mobile payment solution, bank transfers, fiduciary services and services to individuals (airline ticket reservations, asset management, order delivery, etc.). Above all, the system is fully integrated with the e-commerce platform. Alibaba therefore has full knowledge of the transactions carried out by each merchant and each customer.

According to Hubert Testard, former head of the French regional economic department in Beijing, "Alibaba and Tencent are not perceived as an immediate threat by European players in the payments industry. Their progress in Europe will probably be, as it is today in South-East Asia, mainly determined by the pace and size of the equity investments or acquisitions they make, with the obvious concern not to collide head-on with European regulators and policy makers". Even though Tencent has shares in the French company Lydia, for example, adapting to the GDPR is still "a real challenge for Chinese players, who are accustomed to a totally different regulatory framework in their own market.[52]".

In China, Alibaba and Tencent are seen by some analysts as the future players in the banking sector. Although they currently focus on payments, they are key players in the Chinese social scoring system, a mechanism that could be used in the future to determine the borrowing capacity of individuals. Their capacity to disrupt the banking system (via their online lending activity) is such that the public authorities felt the need to rein them in by interrupting last November the floating on the Shanghai stock exchange of Ant Group, a banking subsidiary of Alibaba, much to everyone's surprise.

52 - "Paiements en Europe : les géants de la FinTech chinoise à l'attaque", 20 December 2019, asiepacifique.fr.

Figure 8

Payment solutions offered in France by GAFA.

Source : Autorité de la concurrence

TOWARDS DIGITALISATION OF PAYMENTS: new challenges and changing privacy risks

THE GROWING DEMATERIALISATION OF PAYMENTS, A PHENOMENON AMPLIFIED BY THE COVID-19 PANDEMIC

Payment habits evolve slowly but tend to follow the buying habits of consumers on the one hand, and convenience and trust considerations on the other. Payment, when it involves the disclosure of personal data that may expose consumers to a fraud risk, constitutes a moment of "friction" during which people wonder about the risks, in particular the financial risks, involved.

Thus, the development of remote payments has long been hampered by the perceived risks of these situations, which are not without objective grounds (see page 27). But what is true for financial risks is also true for the risks of uncontrolled dissemination of personal data in general, since remote payment involves, for the very reason of combating fraud, additional checks and therefore the processing and combination of more data.

Today, however, online commerce seems to have become commonplace and the COVID-19 health crisis has only accelerated this trend. Thus, according to the quarterly barometer of the e-commerce audience in France Fevad - Médiamétrie (Q4 2020), nearly 4 in 10 online shoppers increased their online purchases in 2020, with 85% of them reporting spending more than usual. 85% of online shoppers say they prefer home delivery but "click and collect" attracted more than 4 out of 10 online shoppers last year. Online shopping on mobile phones, neglected for a certain time in 2020, has returned to the levels seen at the end of 2019. In addition, more than a quarter of online shoppers made their purchases online from their local businesses.

The pandemic has thus undoubtedly contributed to the blurring of the line between physical commerce and online commerce, perhaps irreversibly. That said, again according to this barometer, the security of data and transactions on an e-commerce site remains a selection criterion for 68% of online shoppers.

The health crisis has also escalated the use of "contactless" card payments with the use of the NFC (Near Field Communication) chip, of which the risks of misappropriation are greater than traditional authentication by presenting the card and entering a 4-digit code. This risk was weighed up last year against the health risk of entering this code, but also against the ease of use with the transaction limit being raised to €50 from 11 May 2020, on the recommendation of the European Banking Authority.

According to the aforementioned 2020 report from the Observatory for the Security of on payments, among these payments, last year there was a marked increase in the share of contactless payments, which rose from 9% in 2019 to 19% in 2020. Contactless payments accounted for 5.1 billion operations in 2020 (i.e. a 37% increase compared to 2019). Online card payments have benefited from the effects of the crisis, with a 13.2% increase in the number of transactions and a 9.3% increase by value.

Although there is still a risk with the NFC protocol, it should be put into perspective if we are to believe the OSMP report already cited: with a fraud rate of 0.013%, down in 2020 despite the increase in its use, contactless appears to be closer to point-of-sale payments with a PIN (0.009%) than it is to online payments (0.174%), which, for its part, increased slightly in 2020.

The growing dematerialisation of payments thus sustains the so-called "phygital" development strategies of large retailers, who imagine connected routes at the point of sale via a loyalty app that can then be used for payment via reduction coupons and, looking further ahead, the issuance of e-receipts with a customer experience that is as fluid as possible. While these strategies relate more to purchasing data than to payment data itself, dematerialisation has the potential to reduce or even eliminate the aforementioned "frictional" aspect of payment, which limits the opportunities for individuals to consider the risks that these transactions entail for the corresponding data.

In addition, while cash cannot be used for this type of payment, dematerialisation automatically feeds the decline in anonymity and the risks of over-identification of payments, at least as long as the central bank does not itself issue a digital currency (see page 45).

THE DIGITALISATION OF PAYMENTS: NEW CHALLENGES AND NEW RISKS

As a corollary of the development of e-commerce, online payments have given rise to the very rapid growth of e-PSP operators with competitive offers, such as the US player Stripe (created in 2006) or the Dutch firm Adyen (founded in 2011 and whose market capitalisation closely follows that of BNP), which in just a few years have become major players in online payments.

The development of electronic payments, as well as economies of scale impossible to achieve with physical commerce, also offers an opportunity for precise knowledge of consumer habits, through the analysis of data collected on the terminal used (desktop or mobile).

As they grow in size, these players aggregate other services and options around their initial model, in order to be able to offer merchant sites a comprehensive range of solutions like the Swedish company Klarna, which offers tokenisation[53], "wallets", prepaid cards and even a form of factoring (like the German Lastschrift). Payment data can then be used for multiple purposes: user experience, anti-fraud score, invoicing, credit score, etc., which assumes that the end user has been informed and is fully aware of it.

A sign of this dynamism of e-PSP operators relatively to traditional physical electronic payment PSPs, the sector is in a consolidation phase, with the takeover of Ingenico by Worldline for €7.8 billion in 2020, for example. Ingenico is the world leader in the physical payment terminals market and a major player in the electronic payments market. Worldline is the leading secure online payment provider. The objective of this buyout was to ensure the critical mass necessary for the investments related to new regulations and to develop value-added services by mastering all the tools in the payment chain. The strategy is similar for their competitors. In 2019, the US firms FIS and Global Payments acquired the British Worldplay, First Data and TSYS respectively. These movements seem essential in this industry, which has become international and where volumes are crucial.

In response to these integration phenomena and in order to maintain a direct link with their customers, certain mass retail players offer their own electronic payment services.

Until 2019, the Starbucks payment app had more users than Apple Pay. In France, Système U for example launched U Paiement in February 2019. It is an e-wallet application, which integrates a QR Code payment system and a loyalty programme (kitty, e-receipts, promotions). Carrefour, FNAC and Casino offer similar services on their apps, while some brands have pooled this service using the Lyf Pay application.

Digitalisation of payment solutions

The security of these applications is a central issue. It is not always up to banking security standards. Starbucks App has been hacked twice, and in both cases hackers were able to access credit card data and transfer money from users' bank accounts. In addition, the applications of large retailers often have access to a large amount of data about their users (transaction, device, location) that they can market to third parties, as Starbucks does. In both of these cases, the question of the compliance of these solutions with the GDPR arises, data security being one of the main principles of data protection, as is the control over who can or cannot access what data, with issues related in particular to transparency and information for individuals.

Another characteristic of current business models, which can give rise to overexposure of personal data, is their "multi-channel" nature. As the rise of "click and collect" solutions or the digitalisation of distribution illustrates, the same goods or services can be ordered online or in a store or agency, and be paid for remotely or on withdrawal. This interpenetration of online or point-of-sale routes, on different technical architectures, creates new possibilities for crossing payment data with terminal or geolocation data, with greater risks of re-identification and exploitation of data. In this context, the question of data reuse is central (see page 60 et seq.).

53 - See the definition of this term in the Glossary.

FOCUS ON...

Crypto payment: "cryptocurrencies" and Libra

The first large-scale virtual private currency, Bitcoin, was created in 2008. It is issued and circulates on a decentralised and public distributed ledger operating by consensus and ensuring the traceability of transactions, but also a very advanced pseudonymisation justifying the qualification of cryptocurrency. Since then, other virtual currencies have been created, still based on blockchain technology, but benefiting, thanks to a reserve mechanism, from a stabilised exchange rate against one of the major sovereign currencies, called "stablecoins", like the most widely used, Tether. The Libra association founded at the initiative of Facebook announced for its part a stablecoin project backed first by a currency basket, then faced with the resistance from central banks and regulators around the world, by parity with just the US dollar and on the basis of a so-called permissioned blockchain allowing control to be exercised over the validating "nodes" of transactions. This project, now known as Diem, would eventually be deployed from the United States, on the basis of cooperation with a bank specialising in crypto-assets.

These virtual currencies are now used more as a store of value (alternative investment asset) than as a medium of exchange that can give rise to payments. Their payment function has major limitations such as (i) the use of a completely new architecture, alongside the existing payment infrastructures organised by central banks around interbank payments, (ii) the lack of legal tender status of these private currencies, which are either very volatile or guaranteed by an issuer whose counterparty risk is disproportionate compared to a state issuer, making confidence in this currency entirely relative, and (iii) the significant transaction costs – for Bitcoin , in the range of several dollars, or even tens of dollars for Ethereum – making retail payment uses unsustainable.

However, the increasingly important holding of these currencies by economic agents (for the equivalent of several hundred billion dollars) could make their use attractive for payments. Tesla thus announced for a time acceptance of Bitcoins as payment for its products, followed by PayPal, which is allowing crypto payments at no cost in the coming months. Finally, Visa announced the integration of the USDC stablecoin into its scheme.

It is too early to predict the place that these alternative payment methods will eventually occupy for retail payments. It can be assumed that they will be used in certain areas such as crowdfunding or international remittances, due to the linkage with central bank digital currencies if they are launched (see page 45). The public authorities traditionally call on the public to exercise caution in the face of the financial risks, but also the security risks, of these means of payment, whereas the compliance of blockchain technology with the GDPR is currently under review by the European Data Protection Board[54].

Finally, the question of the impact on climate of these new payment solutions can also be asked, given the very energy-intensive nature of the Bitcoin system, for example. In terms of overall impact, traditional means of payment and new electronic means of payment are not necessarily equivalent.

54 - See also a preliminary approach of the CNIL on these questions: "Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data", 24 September 2018, cnil.fr (in French)

"CASHLESS SOCIETY", ANONYMITY AND FREE CHOICE BETWEEN MEANS OF PAYMENT

As we have seen, the digitalisation of payments and the development of electronic means of payment make payment transactions more data intensive, all other things being equal.

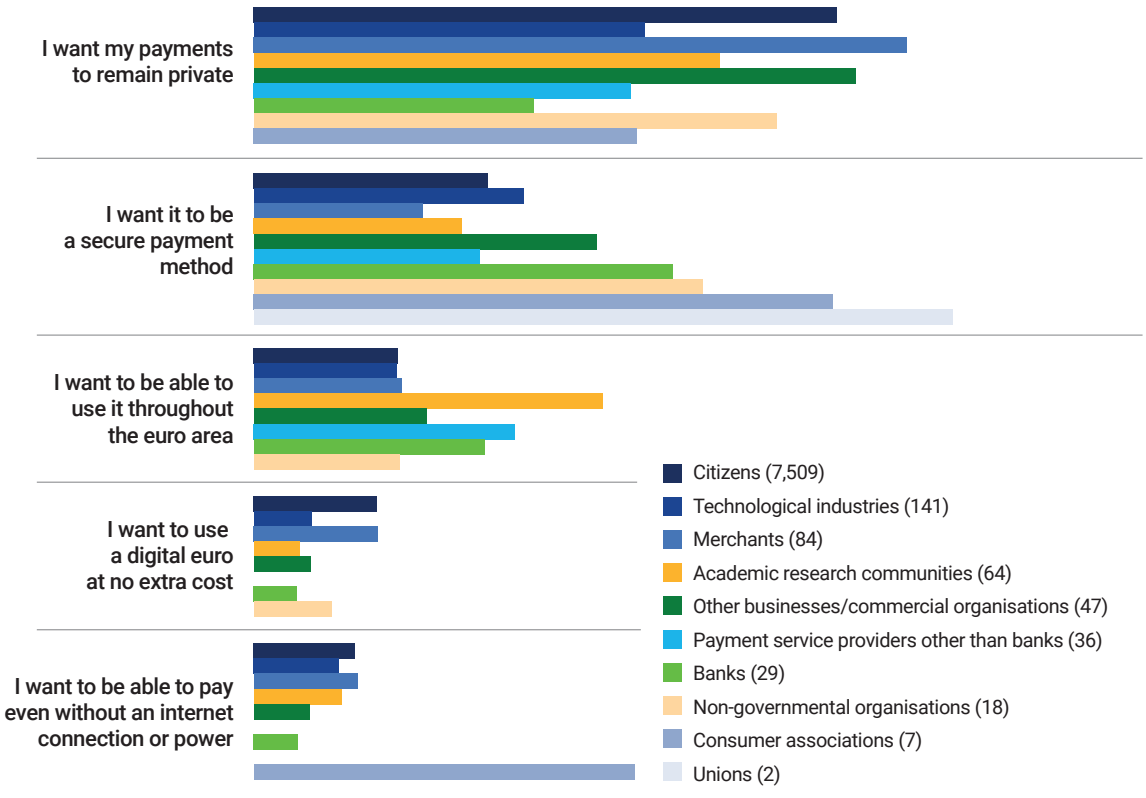
By increasing the scope of transactions for which some form of identification on a book money account is necessary, to the detriment of the simplicity and modestness of cash payment, it is automatically a factor in reducing anonymity in payments. However, the advent of a "cashless" society does not reflect the reality of tomorrow and in view of the demand expressed by citizens, the public authorities should take into account the objectives of maintaining the population's access to cash, for reasons of financial inclusion but also economic and social inclusion.

For example, from a technical point of view, e-wallets within the meaning of the 2009 Electronic Money Directive are likely to be anonymous insofar as sovereign identification is not technically required to open them and they are not necessarily linked to a bank account or a card. From this point of view, electronic money is assimilated to a bearer security as opposed to a registered debt security. However, anti-money laundering legislation almost completely eliminates these anonymity possibilities with a maximum stored monetary value of €150, the inability to refill via an unidentified source and monitoring of transactions from €50 (Article R.561-16-1 of the CMF). These limitations do not appear disproportionate given the risks, as soon as citizens also have sufficient access to cash.

Figure 9

Most important characteristic of a digital euro by type of respondent in the public consultation.

Source: ECB, April 2021.



A new complexion is put on the issue of protection of privacy in transactions in the debate surrounding the creation of central bank digital currencies. The objective of developing these monetary forms, and in particular a digital euro in Europe, is twofold:

- **Support innovation in retail payment** uses on a digital form of the sovereign currency, issued by the European system of central banks and acceptable as legal tender, instead of seeing it deployed outside the traditional banking system on the basis of private "cryptocurrencies".

- **Provide European citizens with a digital form of central bank currency** in online uses that are becoming a new norm, but without crowding out the use of cash. **To achieve its objectives and in particular to generate public confidence, given the potential risks of transaction monitoring, the digital euro shall have characteristics as close as possible to cash,** by allowing transactions that are close to anonymity (see box), which blockchain technology already allows, for example.

Another important aspect for the protection of rights and freedoms in the field of payments, convergent with consumer protection, is **the freedom to choose between several means of payment.**

From the point of view of the anonymity of transactions, the intensity of the collection of personal data or even from the point of view of digital inclusion, not all means of payment are equivalent. People should have physical alternatives to online payments where technically possible; for the same transaction, it is essential that they have the choice between several means of payment, including cash or a digital currency with similar characteristics, both for security reasons and so that they can themselves choose the level of personal data collection to which they are subject. Thus, the degree of protection of privacy and personal data deserves to constitute a factor of competitive distinction between the different means of payment.

FOCUS ON...

Central bank digital currencies

In October 2020, the ECB launched a public consultation on a possible digital euro with a view to creating this digital version of the euro by 2024. Many central banks are working on similar projects like the Royal Bank of Sweden, the US Federal Reserve or the People's Bank of China, which is well into the testing phase for a digital yuan. These projects were accelerated by the publication of the Libra/Diem project (2019/2020).

The consultation feedback published by the ECB last April shows that the protection of privacy in transactions is the number one concern of respondents, whether they are individuals, merchants, banks and PSPs, NGOs or even academics (see Figure 9), ahead of security, which is also related to this concern. In fact, the risks and implications of a retail digital euro in terms of privacy and the protection of personal data are massive, since a digital central bank currency has the potential, as the Chinese example illustrates, to trace transactions throughout the payment systems.

Many technological choices are still to be configured, in particular the choice between an account-based method or a bearer-based method, the degree of intermediation of the commercial banks, the possibility of using one's digital euro wallet without a internet connection or electricity and, finally, the applicable AML-CFT regime. The degree of anonymity of the digital euro and the minimisation of collection, identification and monitoring of transactions will be key to the success of the future digital euro. The requirement of data and privacy protection by design and by default shall be met.

The CNIL and the European Data Protection Board have initiated a dialogue with the Banque de France, with the ECB and other relevant European institutions on this important project[55], which was launched by the ECB on 14 July 2021 as a two-year experimental pilot phase.

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

Over to...

DAVID BOUNIE,

ECONOMIST SPECIALISING IN PAYMENTS

DAVID BOUNIE *is Professor and Director of the Department of Economic and Social Sciences at Télécom Paris, Institut Polytechnique de Paris, and Academic Fellow of the Institut Louis Bachelier. His research focuses on digital finance, and how digital technologies are transforming the finance industry in developed and developing countries. He is the co-founder of the Digital Finance Chair.*

You have been conducting research on digital finance for almost twenty years and working with businesses, banks and central banks in France and internationally. What do you think is the major technological innovation in digital payments?

Without a doubt, central bank digital currencies. Consumers and businesses are faced with multiple innovations in the field of digital means of payment, for making both face-to-face (contactless) payments and remote (online) payments. There are also many dedicated remote payment solutions offered by banks, digital platforms and major internet players, and the latter have also started to issue crypto-assets and private digital currencies (the Diem with Facebook for example).

> ***One solution for the digital euro would be to allow anonymity of payments below a certain threshold***

These innovations are taking off in a context where the pandemic has reinforced the use of cards to the detriment of cash. To cope with these developments, and to allow the entire population, including the most vulnerable, to have payment methods accepted throughout the country at their disposal, both offline and online, the central banks are considering the creation of digital cash. Digital cash is the equivalent of physical cash in that it is universally accepted and is legal tender throughout the country (including virtually). The cash is held in a wallet on a smartphone and is distributed by the central bank, banks or other payment providers. Users then credit their account and log in using different technologies. The wallet has an identifier, a current balance and a payment limit. The wallet offers a range of services including payment, person-to-person transfer and reimbursement of amounts borrowed on credit cards, and integrates programmable service options (smart contracts). The money transfer service between individuals can be used offline unlike other mobile payment services that only work on the internet.

In what way do you think central bank digital cash is a major innovation?

Its creation raises many questions. Beyond the issues of competition with other means of payment (cash and card) and its effects on the banking and monetary system, how can this new product be designed, for example, in relation to cash and card (e.g. pricing, remuneration)?

What services should be offered to consumers and businesses? Should anonymity be guaranteed in transactions like with coins and banknotes? And, in this case, how can we ensure control of payments in order to combat fraud, money laundering and terrorism?

We do not yet know exactly what form this new payment method will take in Europe, nor what services will be offered to users. But it is already clear that we are experiencing a revolution, different from the first generations of electronic money at the end of the last century. The reason is simple: the central banks have the possibility of direct contact with individuals and companies and of implementing programmable digital cash. This innovation is crucial because it offers the possibility for a central bank to conduct a monetary policy targeted at the individual (company) or at groups of individuals. For example, it will be possible to set up programmable loans, limited in time and space, to help certain individuals or businesses.

In terms of digital cash, should we not distinguish between a "European model" and a "Chinese model"?

In fact, to benefit from these innovative services, information on transactions, individuals and/or businesses is needed. China has proposed a first path. The Chinese authorities have chosen a two-tier infrastructure: the Central Bank issues the e-yuan and manages the payment infrastructures, and the banks/businesses distribute the e-yuan through dedicated accounts by providing the wallets directly. This way of working thus gives them perfect knowledge of all payment flows. Its motivations are numerous and contingent on the Chinese economy, which is marked in particular by the ban on cryptocurrencies, the control of capital flows and state control over the major internet platforms (Alibaba and Tencent). The dominant payment platforms on the Chinese market are indeed non-banking operators and are therefore not subject to banking regulations.

But this model is ill-suited to the European market, which is dominated by regulated private players and consumers concerned about the protection of their personal data. Coins and banknotes guarantee anonymity in transactions that consumers and businesses hold dear, and digital payments do not offer quite the same guarantees, in particular due to the regulatory constraints on bank obligations (the combat against fraud, money laundering and terrorism).

So what will the European Central Bank's digital cash proposal involve? One solution would be to allow anonymity of payments below a certain threshold. But this solution could be perceived as unfair competition, within the framework of existing means of payment such as cards, by the banks obliged with clear rules in terms of security and payment control.

In the context of these innovations, is there anything that market regulators need to look out for?

One major vigilance point concerns the use of individual payment data as a tool for targeting consumers by the major Internet platforms. Digital platforms typically use personal data to get to know consumers better, but they also resell these data to businesses that in turn want to identify consumers. Until now, digital platforms have had no knowledge of the purchases actually made by consumers, unless they enter into agreements with payment operators like the US card payment systems, for example. This partnership provides an almost 360° vision of consumers' lives, both online and offline.

Digital platforms could eventually distribute wallets and digital cash, just like banks. The line between markets - social networks/digital platforms/payments - could become increasingly thin, and increase the dominance of the digital platforms. This development would pose new competitive and innovative challenges for banks and regulators, ultimately modifying the whole of financial intermediation. It will become essential for competition authorities to ensure that they define the relevant markets, particularly in the context of the prospective analysis of merger and acquisition transactions in an increasingly fragmented payments market.

Finally, in addition to the doctrine of the relevant markets and consumer welfare based essentially on the price of services, the quality of digital services, in particular the protection of personal data, should also be taken into account. This development ultimately requires close collaboration between competition and data protection authorities, including in market concentration analyses

CURRENT TECHNOLOGICAL DEVELOPMENTS: THE "GAME CHANGERS" OF TOMORROW

The upheavals induced by regulations (PSD2) and the economic upheavals due to competition from large digital services are accompanied by changes caused by the deployment of new technologies, some not specific to payment (such as blockchain or cloud computing) that will not be commented on here, others that are specific to it. These include, but are not limited to, instant transfers, the *"request to pay"* and smartphone payments (mobile payments).

Instant transfer has been in existence in the SEPA zone since 2017 under the name SCT Inst but its use is not yet widespread. It consists of a transfer from bank account to bank account, made in less than 10 seconds and irrevocable given its speed. The instant payment business model has not yet been found: some banks are reluctant, emphasising the risk of fraud or the difficulty of carrying out anti-money laundering checks on amounts, or applying fees while classic SEPA transfers are free of charge. The European Central Bank recently[56] called on the retail banks to make this method more accessible, in particular because it constitutes an ergonomic and efficient alternative to the payment services intermediated by digital players.

Apart from peer-to-peer money transfers between individuals (like the US application Venmo, acquired by PayPal in 2018), few use cases have been established (think cashback), given how little the system has been deployed in the SEPA zone. The ECB has developed a settlement system dedicated to instant payments, called TIPS (Target Instant Payment Settlement), with optional membership but which the ECB wants to make compulsory for all banks by the end of the year. With 14 million transactions for a total amount of €7 billion in 2019, which is very low compared to the €28,658 billion value of transactions in 2019 (again according to the annual report of the OSMP), instant transfer is still very marginal.

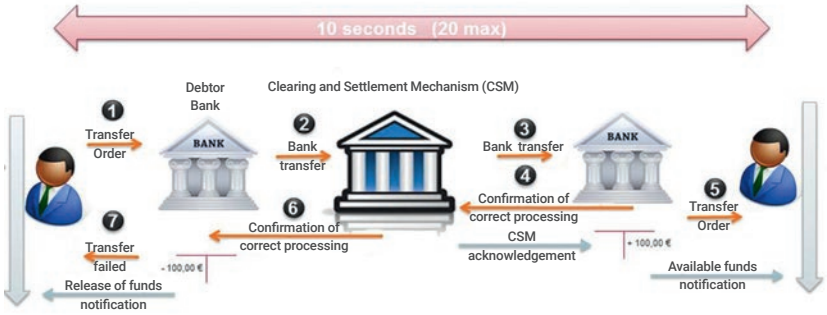
From the point of view of data circulation, the protocols designed by card schemes are not applicable to it and the "SCT Inst" specifications have been defined for broader circulation of data with a payment message size of 140 characters. These specifications involve, outside the payment solution with an SMS link as proposed by certain applications, the processing of the bank account number (IBAN) which has a certain sensitivity. Although the IBAN is not sensitive data within the meaning of the PSD2, its tokenisation within the framework of the "SCT Inst" protocol would undoubtedly be a progress in terms of security (see page 63).

Generally speaking, **a trend towards enrichment of payment data** is noticeable with the draft ISO 20022 standard, which is expected to be rolled out across Europe by the end of next year. This standard, operated by SWIFT, will allow larger messages to convey more data to allow additional services (reconciliation, automation of billing, facilitation of cross-border payments) but also to combat fraud, going beyond simple payment.

Figure 10

How SCT Inst instant transfer works

Source : Sébastien Chesnais.



56 - "Instant transfer: Europe asks banks to lower their fees rates", 24 May 2021, le monde.fr.

The European Payments Forum has also adopted the **"request to pay"** system. This consists of a messaging service in addition to the existing infrastructures that allows the payment transaction itself to be prepared by sending the payer a request asking them to authenticate themselves with their bank and sending the merchant confirmation that its request has been accepted. The payment is then settled between the payer's and the payee's banks, via an "SCT Inst" transfer. The goal is to provide consumers with a better prepared and frictionless payment experience with new billing, collection or peer-to-peer payment services. This project, which is set to be rolled out this year, is of interest to the banks, FinTechs and GAFA companies involved in the project.

In the specifications, the data message based on standard ISO 20022 will also be enriched to allow billing data in particular to be received, thus combining payment data and purchase data: the messages can include the invoice as an attachment as well as a payment reference (identification) in an "RTP Remittance information" field. This does not pose any difficulties for business-to-business invoicing but involves the movement of enriched data for retail use. This raises the question, in the specifications, of the pseudonymisation of directly identifying data such as the payer's reference (name, address) and the IBAN, instead of their decrypted circulation.

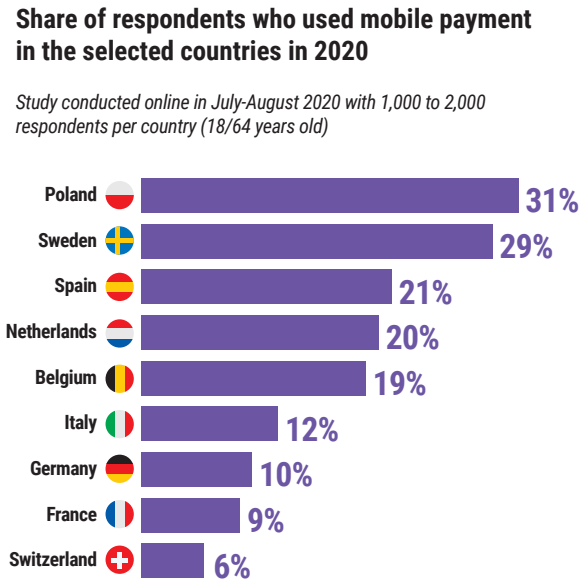
It is still a little early to know if these developments will be "game changers" for the field of payments. As already mentioned, look at what is going on currently for **mobile payments**. The penetration rate has remained very low in France until the current period. The most widespread solution on the market, Apple Pay, only arrived recently (2016) and its generalisation to all banks even more recently. According to the latest Global Consumer Survey carried out in the summer of 2020, only around one in ten French people surveyed said they used a smartphone payment method. This is one of the lowest adoption rates in Europe, with countries like Germany (10%) and Switzerland (6%). Other European countries such as Poland, Sweden, Spain and the Netherlands are already much more advanced in this area, with a share of users between 20% and 31% in summer 2020 (see Figure 11), and probably even more today due to the pandemic.

Still according to the Statista Global Consumer Survey, which compiles consumption data on more than 50 markets in 55 countries, the Paylib application is on the podium of the most popular mobile payment services in France.

Figure 11

Mobile payment has significant room for improvement in France.

Source : Statista



28% of users of this type of service said they had used this application to pay at a point of sale in the past year (March 2020 survey), compared with 35% and 41% respectively for the industry giants, Google Pay and Apple Pay. Among the other popular services in France, there are two other particularly promising French companies in this market, Lyf Pay (13%) and Lydia (9%). We should of course bear in mind that these figures are above all indicators of the reputation of these different services among French users and do not necessarily correspond to their market shares.

Payment by smartphone has great potential for widespread use in the long term, both because of its ease of use and its free access for the end customer (the very expensive commissions are paid by the banks) and its compatibility with card payment. From the point of view of personal data protection, there is a variety of business models, some more protective of privacy by committing to store payment data (but also to a certain extent purchase data) locally on the terminal, others resorting to more centralisation and combination of data, by combining payment cards and loyalty cards in the same wallet. Beyond security issues, future work by data protection authorities on this subject would undoubtedly be relevant.

INTERNET OF THINGS AND AUTONOMOUS PAYMENT

In the not too distant future, the development of the Internet of Things will be coupled with the technical capacity of these connected objects to make payments, with little or no human intervention (automaticity) and from object-to-object, without routing between a payer and a natural person payee (autonomy).

Payment professionals even imagine payment techniques using artificial intelligence that are invisible to the user. At present, Amazon is already experimenting with Amazon Go points of sale, with a first store opened in Europe in London in March 2021, where payments are made automatically, posing delicate questions about user recognition and tracing. Payments may be initiated autonomously, but are ultimately charged to the wallet or account of a user who is a natural person with financial capacity.

The scenarios are already imaginable today: pay-as-you-go timeshare services, vehicle parking, electric vehicle charging, orders placed by a smart refrigerator, micropayments by smartphone to access cultural or media content, etc. These use cases will raise questions beyond data protection, human trust in machines (auditability of algorithms and interpretability of results) and security (pseudonymisation of identifiers stored in objects and authentication of both the object itself and the user responsible for it).

The questions that will arise tomorrow for the CNIL on this subject are therefore not fundamentally different from those that arise today, but will be a digest of all their complexity, from the protection of personal data and security to the regulation of artificial intelligence (AI). The trust that people can place in a given payment universe will be at the heart of our concerns tomorrow as it is today.

The scenarios are already imaginable today: pay-as-you-go timeshare services, vehicle parking, electric vehicle charging, orders placed by a smart refrigerator, micropayments by smartphone to access cultural or media content

DESIRABLE FRICTIONS IN THE FUTURE OF PAYMENTS

As we have seen, the entire payment ecosystem, driven in particular by digital players, seeks to "streamline the payment experience" and "reduce the friction" that can keep consumers from making a payment.

Although the commercial interest of these initiatives is undeniable, the CNIL has, on the contrary, recommended for several years maintaining "desirable frictions", which put the collection of personal data in context and guarantee the correct information and the exercise of people's rights[57]. These frictions can also help strengthen authentication of the payer and improve the overall security of the transaction.

In this regard, the experience of the payment card, deployed on a massive scale from the 1980s, constitutes a model of balance between ergonomics, security and consumer empowerment. By adopting two-factor authentication (for example, owning the card and knowing the PIN code), which is used by almost the entire population, the banking system has taken an important security step, making it possible to maintain a very low level of fraud. At the same time, this daily transaction is fast, while remaining completely under the payer's control.

In the age of contactless – or even cashierless – payment, "desirable frictions" allowing everyone to keep control of the payments they make but also of the transfers of associated personal data must be redefined. These might take the form of regular reminders on the smartphone or notifications or new alerts about unusual spending (based, however, on advanced data analysis). The question of alternatives is also essential for protecting users' freedom of choice and avoiding the stigmatisation of less automatic practices.

The question of alternatives is also essential for protecting users' freedom of choice and avoiding the stigmatisation of less automatic practices

57 - *The form of choices, personal data, design and desirable frictions* (PDF, 1.4 MB), March 2019, cnil.fr (in French).

GUARANTEEING THE PROTECTION OF DATA AND PRIVACY IN THE FIELD OF PAYMENTS: points of vigilance

THE PROTECTION OF RIGHTS IN A FRAGMENTED ECOSYSTEM

As the introductory remarks demonstrate, the payments ecosystem involves a lot of players acting to varying degrees on the purpose and means of the data processing carried out using the transactions and their ancillary data. Each of these players processes personal data in this context. As such, their level of responsibility with regard to this processing must be clear, in order to determine their obligations under the GDPR and vis-à-vis data subjects.

The status of payment operators in light of the GDPR

The GDPR provides for three possible qualifications. Any professional processing personal data acts either as a controller, or as a processor, or as a joint controller. It is essential for each player to know its role since this determines the nature of the obligations under this status.

Data controller

The controller is the person, public authority, company or body initiating the processing, who decides on its implementation by determining both its aim ("purpose") and its modalities ("essential means", such as the type of personal data processed or the duration of their processing, or the determination of the recipients of the data)[58].

The data controller, because of their decisive influence on data processing, has a duty to ensure compliance with the essential principles of the GDPR.
This qualification is relatively easy when an entity is the only one processing a file, on its own behalf. This is particularly the case of a customer file set up by a merchant. However, when it comes to payment, several parties have to be present. Indeed, apart from cash payments, it is almost impossible for a single party to process payment data, since the beneficiary of the payment itself has an account manager, who is generally different from the manager of the payment account used by the payer, and is also likely to use several intermediaries, such as a payment gateway, a flow carrier, a card scheme, a payment service provider, etc.

This specificity of the field makes it necessary to consider joint controllership or processor status.

Data processor

Unlike the data controller, the processor does not process the data on its own behalf, but on behalf and under the authority of a data controller. A very wide variety of service providers qualify as data processors in the legal sense of the term, particularly in the payments sector. However, data processors should not be confused with solution providers who do not have access to and do not process personal data, such as software publishers or hardware manufacturers, who are not concerned by this qualification.
An entity can only process data in its capacity as a processor on the documented instruction of the data controller, which consequently excludes any own reuse of the data without the consent of the data controller.

In practice, the analysis of a set of indices on a case-by-case basis is necessary to determine whether an entity is a processor or a controller. Thus, the level of instruction given, the degree of control over performance of the service, the added value provided by the service provider or the degree of transparency about the use of a service provider can be taken into account. One of the specificities of the payments field is the limited number of players in direct contact with the data subjects (such as banks, merchants, or providers of payment services for individuals).

While the absence of a direct relationship between a professional and the data subjects is not decisive in terms of qualification, it must be taken into account and may lead to the conclusion that many service providers process data as a data processor.

58 - EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, July 2021, edpb.europa.eu

This seems to be the case in particular when the service in question is intended for merchants or banks and the data is not reused on their own account or on behalf of other counterpart data controllers. The clear separation (logical or physical) of the databases of each counterpart of the service is a relevant criterion in this regard in order to ensure that the data processor only processes the data on behalf of a given data controller and does not reuse the data transmitted by its professional counterparts on its own behalf or to offer other value-added services (for example to improve its services or to establish profiles or even statistics from these data, with a view to selling them).

Joint data controllers

Finally, there are situations in which several players are responsible for control and for which they jointly define the purpose and the essential means. This is particularly the case when two bodies process data for the same purpose (such as making payment) and determine the categories of data processed or their recipients. This situation may result from joint decision-making or a plurality of separate but converging decisions without which the processing would not take place.

Joint data controllers are required to determine, in a transparent manner, their respective obligations under the GDPR. An agreement must then be entered into between the latter to reflect this distribution of roles, and the essential points of this agreement must be made accessible to the data subjects, who can however exercise their rights (such as the right of access to their data) with each joint controller.

As regards payments, it seems possible to retain the concept of joint responsibility, since a certain number of players in the processing chain are likely to intervene for the same purpose (such as making the payment) and potentially jointly determine the means of this processing.

Service providers presenting themselves as data processors cannot reuse the data for their own account without changing their status and becoming data controllers.

In the payments industry, a large number of service providers present themselves as data processors. It is therefore decisive for these players to be aware that this qualification does not authorise them to process the data entrusted to them, beyond the instructions given by the data controller, on their own behalf and on their own initiative.

Indeed, being required to process data only on documented instruction from its data controller, the processor must be authorised in writing by the latter in order to be able to consider processing the data on its own behalf. It would then become data controller for these processing operations. This authorisation must result from the real freedom of the data controller to grant it and cannot result from a clause inserted by the data processor into its standard contracts. Such reuse is also subject to verification, by the initial data controller, of the compatibility of these new purposes specific to the initial data processor with the purpose for which the data were initially collected.

To ensure this compatibility (detailed below), the initial data controller must take into account various factors listed in Article 6(4) of the GDPR, including the possible existence of a link between purposes, the possible consequences of the intended further processing for data subjects and the nature of the data, which in this case call for particular vigilance and a relatively strict assessment of what could be **a compatible purpose**. The initial data controller is also required to inform the data subjects concerned (or this category of data subjects concerned) in the event that it grants such authorisation.

Finally, in addition to obtaining this written authorisation from the initial controller, all the provisions of the GDPR must be applied by the new controller, which includes in particular **the information of data subjects** on the purpose of the processing and the identity of the data controller as well as the establishment of mechanisms allowing the exercise of their rights. Likewise, if the processing carried out can only be based on the consent of individuals, the data processor who has become data controller for this processing must provide a means of obtaining this agreement directly from the data subjects, for example through its counterpart if they are in direct contact with the individuals in question.

Management of the risks presented by processing

One of the essential principles of the GDPR is the obligation for professionals to implement internal mechanisms and procedures to demonstrate compliance with data protection rules. This principle, often referred to by the term "accountability", manifests itself through several obligations of the GDPR, in particular that of keeping a register of processing operations, or that of carrying out **data protection impact assessments** (often designated by the acronym DPIA or PIA for Privacy Impact Assessment) when processing is likely to create a high risk for the rights and freedoms of natural persons.

This assessment must be carried out before the intended processing is implemented and be updated throughout the life cycle of the processing to allow the controller to assess the risks that may be generated by data processing and to put in place safeguards to reduce and manage these risks.

And yet, this assessment is often necessary as regards payment data. Indeed, to determine whether such an assessment is necessary, it should be verified whether the processing in question meets at least two of the nine criteria of the G29 guidelines[59]. While the specific nature of payment data is not subject to a ban on processing in principle, it calls for particular vigilance on the part of data controllers, in that it fulfils one of the criteria making it possible to determine whether a DPIA is required, due to their "highly personal" nature. In addition, an impact assessment will be necessary as soon as the envisaged processing meets another criterion, such as evaluation or scoring (including profiling), the existence of an automated decision having a significant effect on the data subjects, the large-scale collection of personal data, the cross-referencing of data, or the presence of innovative technology.

The CNIL has published[60] a list of processing operations for which the performance of a data protection impact assessment is mandatory. For example, it includes profiling processing using data from external sources, which may concern the payments field, in particular for commercial or fraud prevention purposes.

59 - Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation (EU) 2016/679 (PDF, 1.4 MB), 4 April 2017, cnil.fr.
60 - "Deliberation No. 2018-327 on the adoption of the list of processing operations for which a data protection impact assessment (DPIA) is required", 11 October 2018, legifrance.fr (in French)

PROPORTIONALITY AND MINIMISATION

Purpose of processing and principle of data minimisation

Among the main principles of the GDPR, mentioned in Article 5 of the Regulation, the principle of purpose of the processing and that of data minimisation are of particular relevance as regards payment. The regulation require all data controllers to ensure that the purpose of each processing operation is determined, legitimate and explicit. The purpose covers the aim or objective pursued by the processing. It must in particular be recorded in the register to be kept by the data controller, but must above all be brought to the attention of the data subjects within the context of transparency obligations. This obligation is not neutral in a complex ecosystem such as that of payments, because it assumes that each player who decides to use data on their own behalf makes themselves known, through direct information easily accessible to the data subjects, so that these data subjects can trace the use of their data and exercise, if they wish, the rights they are guaranteed by the GDPR.

In addition, precisely determining the purpose of the processing is essential to define the data that can be processed. Indeed, the principle of minimisation requires that personal data be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. It is therefore prohibited and unlawful to collect or even accumulate data without a valid purpose, for the sole reason that these data could prove useful in the future. For example, the purpose cannot be reduced to the simple desire to centralise data from companies in the same group, without a specific objective, nor can it be limited to the desire to accumulate enough data to anticipate deriving meaning from them in the future or developing a new service based on them.

The same applies to the cross-checking of payment data with other categories of data, such as behavioural data, precise data on purchases made or even location data. The enrichment of payment data, in particular by adding contextual data, does not constitute a purpose in itself. This does not mean that these processing operations are by nature impossible and illegal, but that the **centralisation, cross-referencing or enrichment of data are not in themselves valid purposes.**

For example, the main purpose in relation to payment is **the completion of a transaction**. In this regard, the CNIL considers that with regard to remote card payments for goods or services, the card number, the expiry date and the security code are the only data strictly necessary to make the payment. Conversely, the cardholder's title, the contents of the basket and the delivery address do not appear to be strictly necessary to make the payment. In any case, the bank details and the card number are data for which it would be difficult to envisage processing to be for any purpose other than making the payment. Their processing is not prohibited in principle in that they are not by nature special categories of data subject to Article 9 of the GDPR, but the highly personal nature of these data and the principle of minimisation call for increased vigilance.

One trend in the online payments sector, observed with several operators, involves offering online payment solutions allowing frictionless ergonomics for the user, which implies different personal data processing operations before the purchase is validated. It should be noted that such processing has a purpose distinct from completion of the transaction, one that resides more in the optimisation of the payment process. It follows that if these additional data could prove to be necessary for this purpose distinct from the purpose of making the payment, they must then meet different conditions (in particular with regard to the legal bases of this processing, developed below).

Data protection by design and by default

The principle of minimisation should be brought together with the requirement for data protection by design and by default, which requires the data controller to implement, both when determining the means of processing and for the processing itself, technical and organisational measures (such as pseudonymisation, consisting in transforming data so that it can no longer be attributed to a specific data subject without resorting to additional information, for example by replacing directly identifying data such as card names and numbers with random values).

For example, for statistical analyses for the purpose of improving payment services, it should first be considered whether the processing of personal data is necessary (i.e. whether the processing of anonymous data would not suffice, in particular the use of aggregated statistics which do not allow a data subject to be identified). In this regard, it should be noted that the anonymisation of payment data can prove to be extremely complex due to their highly identifying nature. If the processing of anonymous data is not sufficient, consideration should be given to pseudonymising the data, whenever possible.

In the field of payments, these principles are essentially reflected in measures relating to pseudonymisation, minimisation of the data collected, the duration for which data is retained and the recipients. However, the implementation of these principles may also result from measures allowing data subjects to control the processing of their data, such as the implementation of a prior right of opposition, which does not have to be reasoned, with regard to certain processing operations, in particular for the purposes of marketing.

IDENTIFICATION AND AUTHENTICATION

As we have seen, payment operations, particularly remote ones, require identification of the payer and the payee so that the funds can be legitimately debited from the right person and reach the right recipient. In addition, the issuer of a payment instrument (typically a credit institution, a payment institution or an electronic money institution) is subject to anti-money laundering rules which involve sovereign identification of the customer and monitoring of the transactions carried out. However, this identification requirement only concerns the issuer of the payment instruments. As the example of the card illustrates, it is not necessary for the recipient of the payment, for example the merchant, to have access to the sovereign identity of the payer: it is enough for it to be certain that the trusted third party will pay it the funds via the use of a pseudonymous identifier that guarantees that its customer has successfully authenticated themselves with the issuer of the payment instrument. Even in the context of the combat against fraud, there is therefore no equivalence between payment and "digital identity".

There should be a clear distinction between **identification** (phase which consists in establishing the user's identity to answer the question "Who are you?" via a unique identifier) and **authentication** (phase which allows the user to provide proof that they are identified in order to answer the question "Are you really this person?" through the use of an authenticator that only they know or have). For the trusted third party of the payer, authentication consists of disclosing that it has correctly identified the payer. It does not imply the person's registration on an account held by the merchant, even if the latter may wish to do so for customer management reasons, for example.

Consequently, the PSD2 established a standard of strong authentication for payments, known as two-factor authentication, with two factors to be chosen from among three elements (see Figure 12), giving access to the customer's bank account: inherence (something you are), knowledge (something you know) and possession (something you have).

Figure 12
Strong authentication in the PSD2 Directive..
Source : SIA Partners

These three categories are not, however, equivalent from the point of view of the GDPR, since the "inherence" category mostly falls under the qualification of biometric data, protected by Article 9 of the GDPR. Strong authentication is not mandatory when the transaction is low risk (anti-fraud score, as calculated by the payment service provider, below a certain threshold), when it is below €30 or is the result of a subscription, in particular. The regulations clearly distinguish, conceptually, between authentication and anti-fraud, which are two different things. The 3DSv2 standard developed by the major card schemes to combat online fraud, and which also uses an enriched data set[61], is another illustration of this. These two concepts are therefore not subject to the same analysis with regard to the protection of privacy, including because strong authentication creates a moment of "friction" for people, while invasive and "passive" anti-fraud diligence for individuals do not have the same effect.

In addition, thereby reflecting the polysemy of the term "identity", there are **several levels of identification**, ranging from the anonymity of using cash to the sovereign identity certified by the public authorities, involving the declarative or pseudonymous identity via a login and password. In most payment acts under a contract, the use of a declarative identifier with the merchant or the subscribed service is sufficient and "sovereign over-identification" for authentication purposes would not be desirable. **Since the identity attribute is personal data, its disclosure must be required in compliance with the GDPR**, respecting the principles of necessity, minimisation and proportionality of collection described above.

FOCUS ON...

Uses of biometrics worth assessing

Biometric data is sensitive data within the meaning of the GDPR and as such is specifically protected. They can only be processed for specifically justified purposes. They cannot, in particular, be processed on the basis of performance of a contract or on the basis of the legitimate interests of the data controller, but only, for a commercial interest, on the basis of consent. For the reasons described above, the CNIL more easily accepts the processing of biometric data for authentication purposes, rather than for identification of individuals.

In the context of the increasingly widespread use of biometric authentication mechanisms on smartphones, particularly used within the context of payment, the CNIL reiterated that individuals must keep control of their biometric template by storing it locally[62]. In this scenario, the processing carried out, at the initiative and under the sole control of the data subject, may be covered by the domestic exemption mentioned in point (c) of Article 2(2) of the GDPR. This excludes any imposed or "passive" biometric authentication (of which the data subject would not be aware). This also implies that application providers offer an alternative authentication mode to biometrics (for example entering a code), without additional constraints. Finally, the device must include high security guarantees by default.

In the context of the current trend in "behavioural biometrics", previously static biometric methods (fingerprint, retinal scan, face) are becoming dynamic (typing, gait, way of holding an object) and, combined with each other and with the aid of artificial intelligence, could result in a high level of unique identification of individuals. The use cases concerned extend to the detection of fraud. The relevance of collecting consent, which can then be withdrawn at any time, for the purposes of obtaining an anti-fraud assessment, obviously raises questions from the point of view of the controller, as well as that of the proportionality of the use of biometric identifiers for this purpose, from the regulator's point of view. These difficulties are doubled by those relating to the collection of tracer-type data on a terminal, on the basis of Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, known as the "ePrivacy" Directive.

61 - Device ID, IP address, cardholder identity, delivery address, telephone number, since some fields are not mandatory but strongly recommended: see the "EMV 3-D Secure" specifications on emvco.com.
62 - "Biométrie dans les smartphones des particuliers : application du cadre de protection des données", 24 July 2018, cnil.fr.

CIRCULATION, REUSE AND RETENTION

Collection, use and circulation of payment data

The payments field is characterised by a large number of players in a complex processing chain. As much as it allows, it calls for the circulation of certain payment data for the completion of transactions. This is also the first characteristic of the three corners payment model, which seems to be the most minimalist scheme and consists of an exchange of information between the cardholder, the beneficiary of the payment (a merchant for example) and the bank when the latter is both that of the beneficiary and of the cardholder. Although the collection, circulation, transfer and sharing of payment data are not the subject of a specific framework governed by the GDPR, they constitute personal data processing operations and must therefore meet all the requirements of this Regulation.

As with any processing of personal data, such processing implies in particular the need to pursue a specific, explicit and legitimate purpose, but also the requirement of a valid **legal basis**. As with the application of the principle of minimisation, it is the purpose that makes it possible to determine the legal basis applicable to the processing.

Indeed, to be lawful, processing must be based on one of the grounds mentioned in Article 6 of the GDPR. In terms of payment data, the most frequent legal bases are performance of a contract to which the data subject is party, legitimate interests, the consent of the data subjects or compliance with a legal obligation to which the controller is subject. In addition to the specific conditions of validity, the legal bases retained by the data controller shall determine, where applicable, the requirement for additional safeguards (see box).

FOCUS ON...

The possible legal bases[63] for processing of payment data

Among the various possible legal bases provided for by Article 6 of the GDPR, the processing of personal data in the field of payments can be based on four of them:

Performance of a contract:
https://www.cnil.fr/fr/le-contrat-dans-quels-cas-fonder-un-traitement-sur-cette-base-legale.

This may be processing pursuing the purpose of making a payment within the framework of a sales contract between a merchant and its customer. Please note, the objective assessment of the condition of necessity means that it is not sufficient for the contract in question to provide for this processing in order to be considered as necessary for performance of the contract. Thus, for example, processing for marketing purposes does not appear to be necessary for the performance of a sales contract.

continued on page 60 >

63 - « Les bases légales », cnil.fr

Legitimate interests:
cnil.fr/fr/les-bases-legales/interet-legitime

It may first and foremost concern processing aimed at guaranteeing the security of the network and information, implemented for the purposes of fraud prevention, or necessary for direct marketing to a company's customers. In view of the complexity of the payments field and the opacity of its operation from the point of view of data subjects, the reasonable expectations of individuals should be interpreted with caution, particularly with regard to players that do not have a direct relationship with them. The particular sensitivity of payment data makes much of their processing particularly intrusive, especially when they involve profiling or cross-referencing with other data, which has the effect of limiting the possibility of using legitimate interests as the legal basis. As part of the compensatory measures, provision may be made, for processing of the profiling of the online purchasing behaviour of individuals, for an unconditional right of opposition, above all one that can be exercised before processing takes place, for the benefit of individuals, to allow them to stop the profiling to which they are subject.

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

It may be the basis for processing relating to payment data. Please note that refusal to consent to processing that is not necessary for the performance of the contract should not have any consequences on performance of that contract or on the provision of the service (in accordance with Article 7(4) of the GDPR). For example, a data controller providing a payment system intended for data subjects collects the consent of its customers for the use of their transaction data for the purposes of personalising advertising. Consent could be considered freely given if the data subject's potential refusal does not impact use of its payment system. The same would apply to a bank, which can validly obtain the consent of its customers to receive personalised offers from commercial partners, linked to the use of their payment card, when refusal has no impact on the provision of the current account and card.

Finally, certain processing operations may be necessary for the controller to comply with legal obligations related to them.
cnil.fr/fr/les-bases-legales/obligation-legale
particularly in anti-money laundering and counter-terrorism financing.

Reuse of payment data

When a data controller plans to process personal data for a purpose other than that for which it was collected, the GDPR specifically regulates any such further processing. The principle, laid down by Article 6(4) of the GDPR, is that the data subject's consent must be obtained for this processing to be lawful, unless this processing is necessary to comply with a legal obligation or if it concerns a purpose compatible with the purpose for which the data were initially collected.

In order to ascertain whether a purpose of further processing is compatible, several factors should be taken into account, such as any link between the purposes, the context in which the data were collected, the nature of the data, the possible consequences of the intended further processing for data subjects, and the existence of appropriate safeguards such as encryption or pseudonymisation.

As regards payments, the compatible purposes should therefore be assessed very strictly, taking into account the particular sensitivity of the data in question. Thus, it could be considered that further processing of payment data in order to produce statistical analyses to help improve the payment system implemented by a data controller

is a compatible purpose that does not require the data subject's consent when suitable safeguards are in place.

Conversely, the reuse by a card scheme of a transaction history to determine the person's consumption habits and resell these data to a credit institution wanting to enrich the profiles of its future borrowers does not appear to be a compatible purpose, given the consequences for the data subject and the excessive nature of the operation with regard to its supposed reasonable expectations vis-à-vis the merchant. The data subject's consent would therefore be required in order to be able to envisage any such further processing.

In terms of data reuse, certain sector-specific regulations may impose limitations in addition to the criteria laid down by the GDPR. This is particularly the case with the PSD2, which states (in particular in Articles 66 and 67 thereof) that any purpose other than the provision of an account information service or a payment initiation service is not a compatible purpose for the providers of these services. The merchant must therefore obtain the data subject's consent to process these data for other purposes (unless such further processing results from Union or Member State law, in accordance with Article 6(4) of the GDPR).

Storage of payment data

Pursuant to the principle of storage limitation, any personal data must be kept only for a period of time necessary for the purposes for which they are processed. It is therefore important to reason by purpose (point (e) of Article 5(1) of the GDPR). A controller must define and respect a retention period proportionate to the purpose of the processing implemented. An appropriate retention period helps to limit the considerable impact on the data subjects in the event of theft of banking data, or of credit card fraud.

As regards payments, a distinction should be made between the storage of data justified by **the performance of the payment** and storage for **other purposes**, such as proof of transactions completed or billing.

For example, the CNIL has already had the opportunity to comment on certain retention periods for remote payments by card in its recently amended Deliberation No. 2018-303[64] :

- Thus, the CNIL estimates that to **make a single payment**, the retention of payment data may be justified until full payment or until receipt of the goods or performance of the service (or even until the end of the withdrawal period provided for the sale of goods and provision of remote services). In the event of a subscription with tacit renewal, the data may be kept until the last payment deadline.

- For **claims management**, payment data may be kept for 13 months following the debit date or 15 months in the case of deferred debit payment cards. The data thus kept for proof purposes must be kept in an intermediate archive and only be used if the transaction is disputed. More generally, intermediate archiving should be considered whenever possible, by any data controller. This process is indeed a technical measure contributing to ensuring the security of the data processed.

- Conversely, certain data should not be kept after the transaction has been completed. This is the case with the security code of a payment card, retention of which is not justified.

Finally, as **e-receipts** are regularly envisaged by players in the payments industry, it should be noted that such dematerialisation cannot have the effect of justifying a longer retention period or the implementation of other processing operations for other purposes, in particular marketing. This processing should in any event respect the conditions of lawfulness described above, in particular as regards further processing. For example, an email address collected for the purpose of sending a receipt cannot be used for marketing purposes without respecting the principles in this area (namely the collection of the data subject's consent, or the information and the possibility of objecting prior to collection for marketing of products or services similar to those already supplied by the company), since the marketing purpose and the purpose of sending electronic receipts are two fully distinct purposes.

On this subject, the CNIL will contribute to discussions on the decree implementing Article 49 of Law No. 2020-105 of 10 February 2020 on the fight against waste and the circular economy, which plans to bring to an end the systematic printing of receipts from 1 January 2023 in France.

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

FOCUS ON...

Retention of card data to facilitate subsequent purchases

The principle of purpose limitation provided for in point (b) of Article 5(1) of the GDPR generally requires the data controller not to use the data processed and collected for purposes other than those initially intended. In principle, merchants must therefore obtain the consent of their customers to retain their banking data beyond a transaction to facilitate their subsequent purchases. This consent is not presumed and must take the form of an unambiguous act of will, for example by means of a checkbox. It must also be possible for the data subject to withdraw it at any time.

However, in certain cases, an additional subscription can testify to the customer's desire to enter into a regular commercial relationship with the merchant by frequently purchasing on its website. In this case, these merchants may consider keeping by default the bank data entered by customers who take out these additional subscriptions, on the basis of their legitimate interests. The conditions of this default retention are detailed in the CNIL's deliberation on this subject[65] and involve in particular sufficiently complete prior information to the data subjects, the possibility of easily objecting to this collection or storage at any time, as well as the implementation of appropriate security measures.

PAYMENT DATA SECURITY

From the point of view of data security, practices (and business models) appear heterogeneous, especially for online payments where the unencrypted circulation of payment data presents risks for individuals.

In addition, security issues are amplified with the increasingly important digitalisation trends, which is materialised by the desire to find solutions compatible with a multitude of terminals, whether today's mobile terminals or tomorrow's connected objects capable of initiating payments.

Thus, regardless of the security levels made mandatory in payment environments located closest to financial institutions, it is essential that each player take the right measure of the **need for security** of payment data or purchase data.

Indeed, all players must face major developments in attacks, in particular through ransomware. In addition to these criminal attacks, the main purpose of which is to extort a financial sum from the targeted organisation or to carry out blackmail, there is now often an exfiltration of data in order to achieve a leverage effect in obtaining the sums requested in exchange for a decryption key for the data made unavailable. The indirect purpose of this data exfiltration is to allow cybercriminals to resell said data, if applicable.

65 - "Remote payment by bank card", 28 February 2019, cnil.fr (in French). See also the "Cdiscount" judgement of the Conseil d'Etat, 10/9 CHR of 10 December 2020, No. 429571.

At the same time, the proliferation of payment media can lead to new attack patterns based on poor management of the security of players new to the payments market. Thus, over the past two years, the CNIL has observed the development of "credential stuffing" attacks, which consist in trying to connect to an account with username/password pairs that have previously been the subject of data leaks . This technique allows certain attackers to connect to retailers "jackpots" and retrieve the tens or hundreds of euros stored there. More broadly, the CNIL received 2,825 notifications of data breaches in 2020, including 311 for financial and insurance activities, up 5% in 2020 compared to 2019 (24% for all notifications). Today's solutions, like those of tomorrow, must be designed in a context of high digital crime patterns, which are constantly increasing and adapting. In this sense, it is important to integrate security issues as early as possible in projects and throughout the data life cycle. One example is connected objects, which have often been found to have insufficient security levels, in particular for reasons of cost reduction.

Customer expectations that call for more speed in the execution of the service or its provision, and the desire for a simplified customer journey are not expectations incompatible with an adequate level of security. Thus, as already mentioned in this White Paper, the CNIL questions the impacts of using the unencrypted customer's IBAN and distributing it in order to allow instant payment within the framework of the SCT Inst. Indeed, as is the case with certain contactless mobile payment solutions today, the tokenisation of card numbers in order to make a payment seems more likely to meet security challenges. To this tokenisation is added a limited lifespan of the data, limiting subsequent use in the event of hacking of a merchant's environments, for example.

The practice of tokenisation therefore appears capable of offering better protection for payment and security data. It also provides undeniable protection for cardholders. Indeed, in the event of unfortunate hacking of a player in the processing chain, which needs to be taken into account in the risk analysis, this number is no longer usable and offers pseudonymisation by making the link with the cardholder more complex. This solution thus provides the cardholder with financial security, while protecting them from the point of view of their privacy.

It also protects the payment institution by limiting the risk of fraudulent payment and of reuse of a card number that can be reused several times without the cardholder's knowledge.

The CNIL will develop practical recommendations for the ecosystem and regulators with regard to the tokenisation of these data: scope of the data concerned, techniques to use, good practices, etc. (see page 84).

Tokenisation

Tokenisation refers to techniques consisting of replacing sensitive payment data, such as an account (IBAN) or card (PAN) number, with randomly generated disposable data called a token, the use of which is restricted to a single use and which can be limited in time.

"It is essential that each player take full measure of the need to secure payment data or purchase data"

66 - "La violation du trimestre : attaque par credential stuffing sur un site web", 12 January 2021, cnil.fr

Over to...
VALÉRIE FASQUELLE,
BANQUE DE FRANCE

Valérie FASQUELLE, *a graduate of the Institut d'Études Politiques de Paris and the Université de Paris-Dauphine, has been Director of Infrastructures, Innovation and Payments at the Banque de France. In the various positions she has held, Valérie Fasquelle has been at the heart of the major infrastructure projects carried out by the Eurosystem between 2004 and 2015 such as Target 2 and Target 2 Securities. The Banque de France has a particular interest in the field of currency and payments. In particular, it has a mandate to oversee the security of cashless means of payment, which has been conferred by law.*

Beyond aspects relating to the protection of citizens' privacy, payment data raises obvious issues of the combat against fraud, but also of sovereignty. Valérie Fasquelle, former Director of Infrastructures, Innovation and Payments at the Banque de France, presents the challenges currently faced by the regulator.

> ***Users must be made aware of the risks associated with disclosing their bank details***

What is sensitive payment data and where is it found in our daily lives?

Sensitive payment data are data "which could be used to commit fraud" according to the PSD2. However, the proliferation of digital uses and the promises of an increasingly fluid payment experience have contributed to the dissemination of this payment data (for example, saving of payment data in a web browser, a mobile application or on merchant sites). In addition, payment operators like the FinTechs are increasingly seeking to harness the potential of transaction data to offer their customers more innovative and more tailored services. The dissemination of payment data to a multitude of players is therefore a defining trend in the payments industry. This in turn contributes to the continuous search for vulnerabilities by cyber-fraudsters who are deploying increasingly sophisticated methods to steal sensitive payment data.

How can use of this payment data to commit fraud be prevented?

The combat against fraud relies in part on the ability to protect sensitive payment data at all levels. Security standards and regulations on payment services (in particular the GDPR and the PSD2 respectively) govern professionals and activities related to payment and define all the requirements necessary for the protection, processing and exchange of these data.

Nevertheless, it is absolutely necessary to make users aware of the risks associated with the disclosure of their data or the use of websites and applications from unreliable sources so that they become the first line of defence in the combat against fraud.

In practice, what does the PSD2 contribute in terms of data security for consumers?

The PSD2 has helped to strengthen the security of access to users' payment accounts in the same way as it has strengthened the security of payments in the broad sense: by introducing an obligation for the cardholder to use strong authentication. Where a simple static password was previously sufficient to log in to online or mobile banking, regulations now provide for the use of a second authentication factor, for example a password sent by text message or unlocking by biometric fingerprint. However, the regulations take into account the need to find the right balance between simplicity and security: for access to accounts, strong authentication is only required once every 90 days, since the risks are much lower than in the context of payment operations, which are by definition more sensitive to fraud and therefore subject to strong authentication almost systematically.

The PSD2 also made it possible to regulate the practices of access to payment accounts by third parties, known as account aggregators, which offer presentation services for statements of accounts and expenditure generally accompanied by value-added offers in terms of budget management advice (for example alerts, suggestions for more appropriate banking or credit offers, etc.). These players previously operated outside any regulatory framework using so-called web scraping techniques: they would collect their customers' bank identifiers and use them to connect to their customers' online banking to retrieve account or transaction statements. The PSD2 now requires these players to register with the banking authorities (the ACPR in France), and provides that the banks set up dedicated interfaces (or APIs) to allow access to their customers' data without using web scraping techniques.

Thus, the PSD2 helped to both restore the strictly personal character of account holders' login credentials, while supporting the development of a new activity based on the use of data within a secure framework, with security requirements and well-defined rules and responsibilities.

You also mention sovereignty issues concerning the management of payment data: can you tell us more?

The completion of a payment operation in Europe is increasingly dependent on the participation of third parties (e.g. Visa, Apple Pay, Google Cloud, etc.) often established outside the European Union. In a context of continuous growth in the use of cashless means of payment, this can constitute a vulnerability for the strategic autonomy of the European economy, with regard to the risk of continuity, but also in the event of threats of retaliation or unjustified transfers of data to a third party (for example in the context of intelligence operations or criminal investigations). Moreover, beyond the strict supervisory mandate of the central banks, dependence on non-European players makes the correct implementation of European personal data protection rules (including for payment data) more uncertain. Finally, in the context of the digital revolution, payment activities provide two strategic assets (data and a daily customer relationship) essential to maintaining European competitiveness.

What solutions do you recommend in order to better take the European sovereignty dimension into account in the retention, processing and exchange of payment data?

There is growing interest in the issue of data processing and retention, and rightly so. We are closely monitoring the projects of the European Commission within the framework of its data strategy, several initiatives of which must be specified in 2021. In France, the National Cashless Payments Committee (CNPS) – chaired by the Banque de France – has echoed the fears of the French market, and is promoting implementation of a policy for localising payment data in Europe, as recommended by a report from the Conseil general de l'économie submitted to the Minister of the Economy in February 2020[67].

67 - Lemery S. and Steiner R., "Mise en œuvre d'une politique de localisation des données critiques de paiement en Europe", Report No. 2019/16/CGE/SG, 2020, economie.gouv.fr.

PREVENTING FRAUD

In the payments industry, and more specifically for online payments, processing for the purposes of combating fraud is the focus of many of the vigilance points previously mentioned in terms of personal data protection.

First of all, with regard to the qualification of organisations, it seems that several players in the chain are technically able to process payment data for this purpose. These include the merchant, the payment gateway, the payment service providers, the card scheme and the account manager.

The combat against fraud then raises the question of data minimisation. In fact, only the data necessary for these operations can be processed, which implies a case-by-case analysis of the data likely to be processed, in view of the context of the fraud, the data already available and other mechanisms already in place to prevent such fraud (e.g. enhanced authentication). A balance must therefore be found between the proportionality of the processing and the effectiveness of the systems. In general, the CNIL favours systems that rely on securing means of payment or authentication rather than processing seeking to increase the amount of data collected to assess the risk of fraud. It is indeed much more difficult to comply with its information obligations and the rights granted to individuals in the event of mass data collection.

> ***A balance must therefore be found between the proportionality of the processing and the effectiveness of the systems***

In this regard, in the field of online payments, particular attention must be paid to the possible application of the ePrivacy Directive, and in particular transposition thereof into Article 82 of the French Act "Informatique et Libertés", which calls for the user's consent to allow the action to access, by electronic transmission, information already stored in their electronic communications terminal equipment, or to enter information in this equipment. In other words, the use of **a tracker on the terminal** of a data subject to collect data requires the data subject's consent, regardless of the legal basis used for subsequent processing of the personal data thus collected.

This obligation to collect consent concerns in particular so-called contextual scoring services, based on data related to the context of the transaction such as the IP address, location data, data from the browser used, etc., but also **behavioural biometrics** scoring, i.e. scoring based on data on keystroke dynamics, mouse movements, terminal usage habits, or the use of touch screens.

As we have seen, this second type of scoring may also be subject to the specific framework for biometric data governed by the GDPR (Article 9), when it concerns the processing of behavioural characteristics specific to the data subject to contribute to their unique identification. The explicit consent of the data subject, or the adoption of a model regulation by the CNIL, could prove necessary to allow such processing to be performed.

Moreover, with regard to the legal basis of this processing, whereas it seems difficult to consider that the anti-fraud processing operations are necessary for the payment to be made, legitimate interests seem to be the most relevant legal basis for this processing, provided that its validity conditions, as described above, are met. However, it assumes that this processing falls within the reasonable expectations of the data subjects and that a certain number of safeguards aimed at protecting the interests, rights and freedoms of data subjects are put in place.

Another difficulty in payment fraud prevention stems from the sharing of data between different data controllers, or even the use of tools based on the pooling of data. **This sharing of data** raises several questions in terms of data protection, starting with the qualification of the players. It seems that the entity pooling the data should in principle be qualified as data controller, since the latter generally determines the data it pools, for what purposes and by what means (thus determining the purpose and the means of the processing). The question of the distribution of roles between the entities contributing to this database, and the players taking advantage of it (in particular by querying the pooled database), is also essential. Where several players contribute to determining the means of processing (by a joint decision or convergent decisions) and pursue the same purpose (such as that of combating fraud), joint controllership must be considered and governed under the conditions laid down in Article 26 of the GDPR.

For example, when it comes to establishing a list of people presenting a fraud risk, the CNIL generally considers that two levels of **information** are relevant:

- General information for data subjects on the existence of a fraud prevention mechanism that could lead to them being registered on a list of persons presenting a fraud risk.

- If an anomaly, an inconsistency or a flag that may be the result of fraud is detected, the data controller has the option of adding an individual to a list of individuals presenting a fraud risk. The data subject, who could be included on this list, may be contacted, depending on the type of suspected fraud (internal or external), to provide additional information. At the end of the investigations, if a decision is taken that produces legal effects (such as the refusal to proceed to payment or to enter into a sales contract), written and individual information must be sent, specifying the measures taken by the controller and giving the individual the opportunity to present its observations, without prejudice to the applicable legal provisions.

In terms of a pooled database, it appears that both the transmission of data to constitute and supply this database and the use of the result of this pooling must be brought to the attention of the data subjects. For example, in a deliberation authorising the implementation of a shared database for the purpose of combating fraud in online sales[68], the CNIL had retained that the information was provided on the collection forms of the e-commerce merchants using (and supplying) this processing.

Compliance with the conditions governing subsequent data processing described above, as well as the exercise of the rights of data subjects, is also of particular importance in the combat against fraud. In this regard, it appears essential for data controllers to provide appropriate means to ensure the effectiveness of the exercise of rights, in particular by clarifying the respective roles of the players, when they find themselves in a data processor (in accordance with Article 28 of the GDPR) or joint controllership (Article 26 of the GDPR) situation.

Finally, Article 22 of the GDPR regulates any **fully automated decision** taken on the sole basis of processing, a concept which could be illustrated, for example, by the practice of refusing a transaction solely on the basis of a score established automatically and without human intervention. In this regard, the GDPR imposes a series of conditions to be applied on a case-by-case basis, and in particular the right, for the individuals concerned, not to be the subject of a decision based solely on automated processing and producing legal effects concerning them or similarly significantly affecting them.

68 - "Deliberation No. 2013-367 authorising the company ONEY TECH to implement automated processing of personal data for the purpose of combating the risks of payment fraud on the Internet", 28 November 2013, legifrance.fr (in French).

FOCUS ON...

Exemptions to strong authentication for electronic payments with a risk of fraud

One of the objectives of PSD2 is to strengthen payment security. In this regard, it establishes (in Article 97 thereof) an obligation of strong authentication of electronic payments initiated by the payer. This obligation falls on payment service providers, and strong authentication is defined as relying on the use of two or more elements belonging to the categories "knowledge" (something only the user knows), "possession" (something only the user has) and "inherence" (something the user is).

However, Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 responsible for specifying security and authentication requirements provides for several exceptions to the strong authentication obligation, one of which involves a certain number of personal data processing operations. More specifically, it provides (in Article 18 thereof) that payment service providers are allowed not to apply strong customer authentication where the payer initiates a remote electronic payment transaction identified by the payment service provider as posing a low level of risk. This level of risk is determined by scoring, which involves considering a certain number of personal data relating to the payment in question and more generally to the payer. This concerns in particular the possible abnormal location of the payer or the payee, the payer's previous payment spending habits, the history of their payment operations and the identification of abnormal payment behaviour in relation to the payment operation history.

In accordance with Article 94 of the PSD2, the processing of personal data carried out for the purposes of this directive, such as that implemented within the framework of the 3D Secure protocol[69] (see Figure 13), is subject to data protection regulations. It is therefore wise to reiterate a few attention points in this matter. First of all, this processing must have a legal basis. In addition to the existence of certain specific legal obligations, it seems that legitimate interests should be considered as being the most appropriate legal basis for such processing, since its purpose is to prevent the risk of fraud in order to allow facilitation of payments by lifting the authentication obligation.

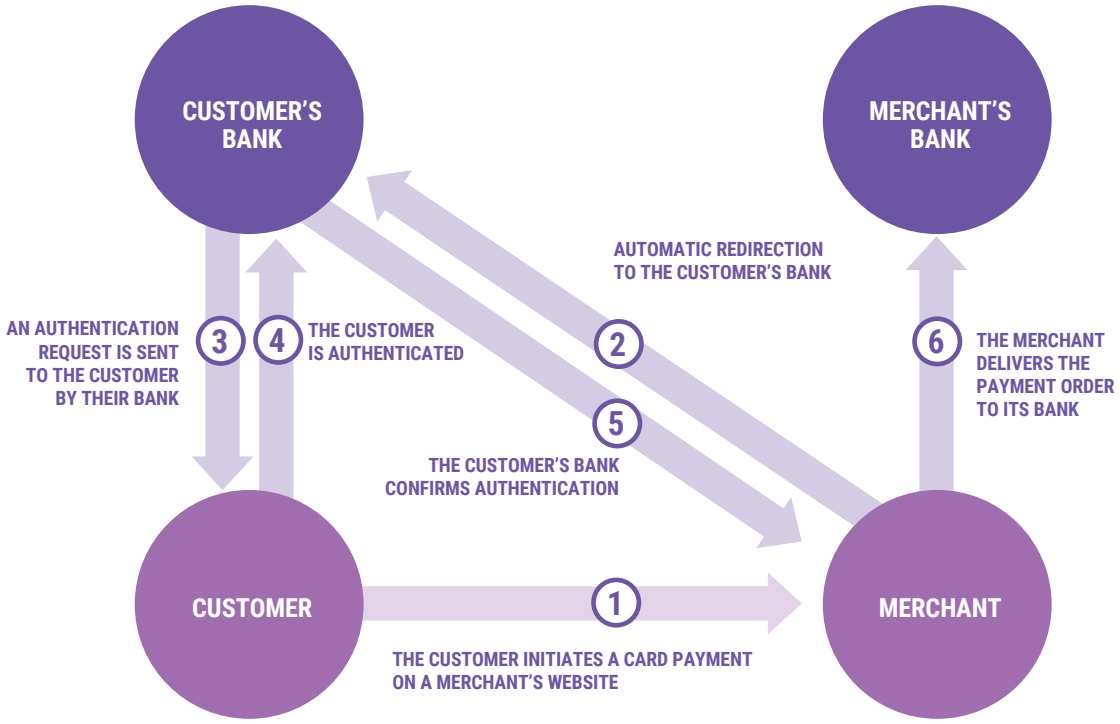
Each data controller carrying out this processing therefore has an obligation to ensure, and to be able to prove, compliance with the principle of minimisation and balancing of the interests of the data subjects, whether concerning the collection of data, their transmission to another controller, or their retention period. Data subjects must be informed of the existence of this processing, and be able, if necessary, to exercise their rights over the data, such as their right of access or possibly their right of opposition. In this regard, leaving it up to the data subjects to authenticate themselves for each electronic payment could be a relevant and protective means which would also allow the exercise of a prior right of opposition, since the processing operations relating to the derogation of the low risk would no longer be necessary.

69 - This is a protocol for security, authentication and fraud prevention in online transactions, the specifications of which are determined by the EMVco consortium.

Figure 13

Operation of the "3D Secure" protocol.

Source: Banque de France, "Paiements et infrastructures de marché à l'ère digitale" (Payments and market infrastructures in the digital age), January 2021, page 57



TRANSFERS AND INTERNATIONAL CIRCULATION OF PAYMENT DATA:
a sovereignty issue for the European framework of trust?

Payment data are susceptible to global circulation, due to the global nature of certain players such as the large card networks or e-commerce giants, the weight of international payments in a globalised economy (millions of transactions per day worth trillions of dollars in the SWIFT clearing system) and the rise of online commerce, of which the operations are more globalised than in physical commerce.

Thus, according to the United Nations Conference on Trade and Development (UNCTAD), cross-border retail e-commerce amounted to some 440 billion dollars in 2019, an increase of 9% compared to 2018. The share of online shoppers making cross-border purchases increased from 20% in 2017 to 25% in 2019. The weight of cross-border transactions in online commerce has also justified the launch, in 2019, of specific negotiations on this subject within the framework of the World Trade Organization. In Europe, in 2019, the share of cross-border online sales accounted for 23.5% of total online sales and while most cross-border trade in Europe (55%) was generated by players in the European Union, 45% were made by players from third countries[70].

The issue of protecting the payment data of European citizens thus has undeniable geopolitical implications and is at the heart of sovereignty issues, in several ways. These include the sovereignty of states, in the sense of their non-submission to other states, in the classic legal sense. They also include the sovereignty of individuals over their data, according to the principle of "informational autonomy" which underlies the GDPR.

With what we can call **data sovereignty**, these two perspectives come together: it is by giving themselves the means to effectively protect the personal data of their nationals (from access by foreign authorities, from the economic exploitation of private third parties, etc.) and to invoke European values that European states avoid dependence (technological, economic and political) on other states.

Data sovereignty thus joins digital sovereignty, according to lawyer Pauline Türk: "The notion of digital sovereignty is therefore not limited to the strict classical legal perspective, attached to the power of states. It refers in its broadest sense to command and the right to self-determination in a digital world. (...) Against the logic of patrimonialization of personal data, the consecration of a right to informational self-determination would make it possible to guarantee the right of individuals to control the use and future of the personal data provided, as well as the "traces" left by the digital activity. Certain rights derived from it have already been enshrined, in particular at European level, by the General Data Protection Regulation (GDPR), which entered into force in 2018, or by the Court of Justice of the European Union (right to be forgotten, de-listing, data portability, consent, information and rectification, etc.)." [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", 4 July 2020, cbcommerce.eu.
71 - P. Türk, professor of public law at the University of Côte d'Azur, "Definition and challenges of digital sovereignty", Les Cahiers français, No. 415, May-June 2020 (in French).

THE LONG-STANDING QUESTION OF ACCESS BY FOREIGN AUTHORITIES

This subject is not a new one for payment data. It was, for example, illustrated in the early 2000s by the fears expressed about a programme to monitor international banking transactions set up by the United States in 2001. This was based on an interbank financial transaction service under Belgian law (SWIFT[72]), initially in order to track the financing of terrorist networks but which was then accused of having quickly become a tool for monitoring the financial transactions of individuals and companies leading, in particular, the G29[73] to express its serious concerns.

Thus, in an opinion of 22 November 2006, it considered that in the absence of transparency and effective supervision mechanisms, the data thus transferred from Europe to SWIFT's branch in the United States, then from there to the US authorities, violated European personal data protection rules.

The proper functioning of the international interbank clearing system led Europe to enter into an agreement with the United States in 2010, after a first version rejected by the European Parliament, to legalise the data transfers in question[74]. This agreement was deemed insufficient by the G29, which wrote to the US government in June 2011 deploring in particular the lack of information for individuals and the lack of effectiveness of the agreement.

However, the misuse of the SWIFT system by the United States, alleged at the time, resulted in the development of local financial communications protocols in Europe such as EBICS[75].

In the SWIFT case, just like almost 15 years later in the Schrems II case, the territorial applicability of US law within payment systems conflicts with the territorial scope of European personal data law, as soon as individuals located in Europe are affected. To understand this, we must first examine under what conditions personal data can be transferred outside of Europe.

> ***The territorial applicability of US law within payment systems conflicts with the territorial scope of European personal data law***

72 - Society for Worldwide Interbank Financial Telecommunication.
73 - Former group of European data protection authorities, forerunner of the EDPB.
74 - "Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program", Official Journal No. L 195 of 27 July 2010, eur-lex.europa.eu.
75 - Electronic Banking Internet Communication Standard.

OUTSIDE THE EU, PROTECTION OF PERSONAL DATA THROUGH THE "BUBBLE OF TRUST"

**Trust is crucial when it comes to personal data.
Within Europe, a principle of free movement applies to these data.
On the other hand, when they need to be exported outside the European Union or the European Economic Area, special rules apply.**

Following the example of Directive 95/46/EC and the French Data Protection Act of 6 January 1978 as amended, the GDPR organises the conditions for the transfer of personal data outside the European Union so that it continues to benefit from its protection, once transferred to third countries.

As such, the GDPR establishes the principle that transfers to a third country are in principle prohibited (Article 44), unless the third country has been recognised as offering an adequate level of protection by a decision of the European Commission, known as an "adequacy decision" (Article 45), or in the absence of an adequacy decision, when the transfer is subject to "appropriate safeguards" (Article 46).

In the absence of an adequacy decision or appropriate safeguards, data may in certain specific situations, exhaustively listed and strictly interpreted by the European Data Protection Board, be transferred on the basis of derogations expressly listed by the GDPR (Article 49).

In addition, since May 2018, the GDPR has broadened the range of legal tools used to regulate transfers. They can now be used by both data controllers and processors. In addition, it also concerns onward transfers: those relating to transfers of data from the European Union to a third country, for example, then to another third country or an international organisation.

Finally, the data subject must be informed when their data are collected of the possibility of them being transferred outside the EU. This indication generally appears in the confidentiality policies of the subscribed service.

International transfers: the GDPR toolbox

The adequacy decision is a facilitating tool. It allows the free movement of data to third countries or international organisations and does not require the data exporter to take any other steps (other transfer tools or obtaining authorisation from the CNIL).

The purpose of the adequacy assessment should be to analyse that the level of protection of personal data is essentially equivalent to that guaranteed in the European Union. This analysis must be carried out with regard to a list of criteria, in particular: respect for human rights and fundamental freedoms, the relevant legislation relating to the protection of personal data, both general and sector-specific, including with regard to public security, defence, national security and criminal law and the access of public authorities to personal data, effective and enforceable rights as well as the remedies available to the data subjects and the existence and effective functioning of an independent supervisory authority (Art. 45-2).

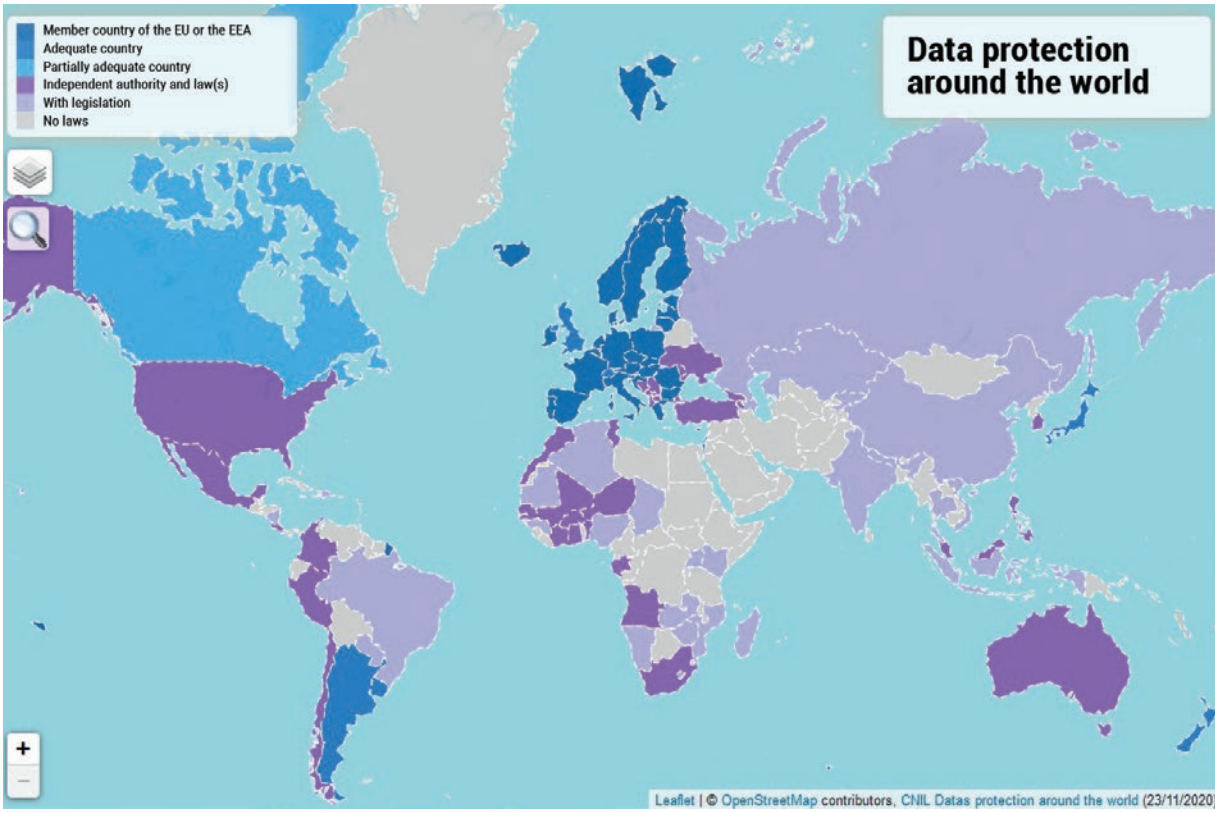
Thus, a payment service provider controlling or processing data in Switzerland or Japan, for example, is covered by this principle of adequacy (see Figure 14). Please note that the country where data is processed is not necessarily the country where the service provider's headquarters are based, generally in the EU if it wants to be able to carry out payment transactions in Europe by virtue of the applicable sector-specific rules.

Adequacy decisions must be subject to periodic review, at least every four years, by the European Commission in order to take into account all relevant developments in the third country or international organisation concerned. In addition, independently of the periodic review, the Commission must continuously monitor developments which may affect and call into question its adequacy decisions.

Figure 14

Map of adequate countries in summer 2021.

Source : CNIL



In the absence of an adequacy decision, it is necessary to rely on one of the eight other legal instruments governing international transfers provided for by Article 46 of the GDPR. Among these, the organisation must make its choice with regard to its nature, size, internal organisation, maturity in terms of data protection, its competitive market, etc.

The transfer tools anticipated include the **Binding Corporate Rules** (BCR), which are highly attractive to the international groups for which they are mainly intended. In this way, large international banks and large US card schemes, whose data are transferred to the United States, can use it. In addition, the approved national or European certification mechanisms (which have not yet found a way to apply to payment data) mainly target SMEs and constitute a differentiating factor allowing them to win contracts.

The codes of conduct provided for in Articles 40 and 41 of the GDPR also constitute compliance tools that allow a business sector to support the compliance of professionals through practical and operational recommendations while harmonising practices at sector level. The use of codes of conduct as transfer tools, adopted at European level by the EDPB, could represent a valuable tool in the payments industry where the management of transfers can be complex. In fact, payment services are often reliant on a chain of players, whose respective roles are complex to grasp, some of which are global in size, sometimes with the presence of further processing, even though the risk of access not complying with European rules for this type of data is higher (see page 22).

Standard contractual clauses (SCCs) are another transfer tool that could be used. These are template contractual clauses adopted by the European Commission to regulate transfers of personal data made by data controllers to recipients located outside the European Union. They aim to simplify the task of data controllers in the implementation of transfer contracts.

There are two types of clauses adapted to each situation: transfers from controller to controller and transfers from controller to processor.

The European Commission recently adopted revised clauses[76] following the CJEU's "Schrems II" judgment in July 2020 (see box).

FOCUS ON...

The Schrems II judgment

In its judgment of 16 July 2020, the Court of Justice of the European Union (CJEU) invalidated the so-called "Privacy Shield", adopted in 2016 by the European Commission following the invalidation of the "Safe Harbor", which allowed data to be transferred between the European Union and US operators adhering to its data protection principles without any further formalities. The Court held that US law relating to access to data by intelligence services (in particular Section 702 of the Foreign Intelligence Surveillance Act (FISA) applicable to electronic communications operators and Executive Order 12333 applicable to underwater cables) does not ensure an essentially equivalent level of protection[77] to Europe, in particular in the absence of effective redress mechanisms available to European citizens.

The Court also clarified that, as a general rule, standard contractual clauses can always be used to transfer data to a third country (whether it is the United States or another third country). However, the CJEU underlined that it is then up to the data exporter and importer to assess in practice whether the legislation of the third country allows the level of protection required by EU law and the safeguards required by the SCCs.

If this level cannot be achieved, companies must take additional measures[78] to guarantee a level of protection essentially equivalent to that provided for in the European Economic Area and they must ensure that the third country's legislation does not interfere with these additional measures in such a way as to deprive them of their effectiveness.

In practice, for those exporting personal data to the United States (or any other third country), the continuation of transfers on the basis of SCCs will therefore depend on any additional technical and organisational measures that they could put in place (e.g. end-to-end encryption without holding the encryption keys, split or multi-party processing, access minimisation, etc.). The whole formed by the additional measures and the SCCs, after analysis on a case-by-case basis of the circumstances surrounding the transfer, will have to ensure that the legislation of the country to which the data are exported does not compromise the adequate level of protection that the clauses and these measures should guarantee. Otherwise, they are required to suspend or end the transfer of personal data. In the field of payments, analysis of the sector-specific legislation of the third country may be essential for economic players.

This major judgment on the protection of personal data has particularly significant repercussions. Indeed, it strengthens the accountability provided for by the GDPR by emphasising the need for data controllers or processors to ensure compliance with fundamental rights, as protected within the European Union, of the legislation in countries to which data are transferred and the effective guarantee of the rights of individuals. In this sense, the judgment contributes to data sovereignty.

76 - See "European Commission adopts new tools for safe exchanges of personal data", June 2021, ec.europa.eu.
77 - See in particular recital 145 of the judgment of the Court, clause 4(g) of Commission Decision 2010/87/EU, clause 5 (a) of Commission Decision 2001/497/EC and Annex II (c) of Commission Decision 2004/915/EC.
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. See also, on the CNIL website, the section "Data controllers: how to identify and process data transfers outside the EU?" (https://www.cnil.fr/fr/responsables-de-traitement-comment-identifier-et-traiter-des-transferts-de-donnees-hors-ue).

EUROPEAN LOCALISATION OF PAYMENT DATA: FROM PROTECTION TO SOVEREIGNTY?

The GDPR pursues a dual objective of protecting personal data and the free movement of such data within a virtuous scope. As such, it is part of an open vision of sovereignty: players from third countries who wish to process Europeans' data can do so, but according to European rules and values. Where foreign law makes this impossible, the data must be processed in Europe. For payment data, which presents particular challenges in terms of privacy, should we go further and impose their systematic localisation in Europe? This is what a recent report from the Conseil général de l'économie proposed (see box on next page).

The CNIL recently followed a similar reasoning with regard to health data. "Due to the sensitivity and the volume of data intended to be hosted within the Health Data Hub, for which the highest level of technical but also legal protection must be ensured, including in terms of direct access by the authorities of third countries, the CNIL has expressed its wish for its hosting and the services linked to its management to be reserved for entities falling exclusively under the jurisdictions of the European Union.[79]"

The data security obligation of banking and payment institutions does not stem only from the GDPR. As they operate in a closely regulated sector, banking and payment institutions also appear on the list of operators of essential services (OESs) that have to implement the NIS Directive[80], which provides, in particular[81], for the obligation to apply specific security rules to essential information systems, to notify ANSSI[82] of security incidents occurring on these systems and to submit to its control.

In this context, the localisation of payment data in European territory could, it is true, lead to a solution that combines sovereignty and security, while offering citizens greater control over their data, and the data protection authorities greater control over the corresponding processing.

However, it is neither a necessary condition, as we have seen, nor a sufficient condition to guarantee effective protection of the payment data of Europeans.

For example, the US CLOUD Act of 2018 applies to American entities that process data in Europe, as long as they have access to these data[83]. However, the European Data Protection Board noted in this regard that, unless there is an international agreement establishing safeguards, "the lawfulness of such transfers of personal data cannot be confirmed, without prejudice to exceptional circumstances in which the processing is necessary to protect the vital interests of data subjects"[84].

Moreover, the recommendations of the European Banking Authority on cloud outsourcing tend to favour the storage of data in Europe. They ask banking institutions to "take special precautions when entering into and managing outsourcing agreements agreed outside the EEA, because of the potential risks for data protection and for effective control by the supervisory authority"[85].

All of these questions must therefore be examined with the greatest attention by data controllers and processors having recourse or likely to have recourse to international transfers of payment data. A case-by-case analysis, the prerequisite of which is the proper identification of transfers taking place in the field and the analysis of legislation in the destination country, is necessary.

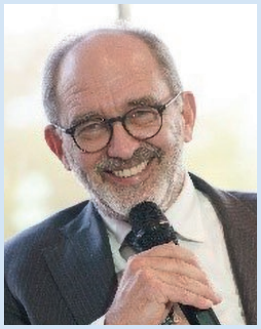
It is desirable for these players to then question themselves, in particular, about the issue of knowing whether the transfers are indeed necessary for performance of the services and, if the transfer appears to be more of a choice, to think about alternatives, in order to minimise the risk of access that does not comply with European rules.

79 - "La Plateforme des données de santé (Health Data Hub)", 9 February 2021, cnil.fr.
80 - Directive (EU) 2016/1148 of the European Parliament and of the Council specifying the elements to be taken into consideration by digital service providers in order to manage the risks which threaten the security of networks and information systems, as well as the parameters making it possible to determine if an incident has a significant impact.
81 - See Decree No. 2018-384 of 23 May 2018 relating to the security of the networks and information systems of essential service operators and digital service supplies.
82 - Agence nationale de la sécurité des systèmes d'information (French National Cyber Security Agency).
83 - It is in this context that 13 European banks recently joined the "European Cloud User Coalition" (ECUC), an initiative launched by the German banking group Commerzbank in 2019 to implement a safe European cloud solution.
84 - "EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection", 10 July 2019, edps.europa.eu.
85 - "Recommendations on outsourcing to cloud service providers" (PDF, 138 KB), 28 March 2018, eba.europa.eu.

Over to...

RÉMI STEINER AND SANDRINE LÉMERY,

CONSEIL GÉNÉRAL DE L'ÉCONOMIE



RÉMI STEINER
has held a variety of positions in various banking institutions, notably as Director and Deputy CEO of the banks Hervet and UBP (Union de Banques à Paris), whose merger with CCF led to the creation of HSBC France.
In 2011, Rémi Steiner joined the Conseil général de l'économie, when the field of expertise of this entity, chaired by the Minister of the Economy and Finance, was extended to all financial services and related activities.

SANDRINE LÉMERY
Professor at the Conservatoire national des arts et métiers (National Conservatory of Arts and Crafts) and holder of the actuarial chair, Sandrine Lémery is also Vice-President of the Institute of Actuaries and President of the Supervisory Board of the French Pension Reserve Fund. She has alternated between 17 years within the authority in charge of insurance supervision and 10 years of administrative roles on economic and social subjects. She was notably the first Secretary General of the Prudential Supervision and Resolution Authority (ACPR) from 2013 to 2018.

> ***There is a close connection between our recommended obligation to localise payment data and the GDPR***

The French National Cashless Payments Committee (CNPS) is a forum for exchange and discussion, where representatives of the payments industry and public stakeholders interested in the development of this activity meet. In its coordination and guidance role, on 18 February 2019, the CNPS approved a new national retail payments strategy for 2019 to 2024[86].

Within the framework of the implementation of this strategy, the French Minister of the Economy and Finance entrusted the Conseil general de l'économie, on 19 June 2019, with a mission to study the implementation of a policy for localising payment data in Europe.

We were invited to assess "the importance and sensitivity of extra-European processing of critical payment data, as well as the sovereignty issues" associated with this processing, in light of changes in the payment services offer, as well as the entry into force of the General Data Protection Regulation (GDPR) and the Second Payment Services Directive (PSD2). In the light of past events, we have examined the potential threats to the use of payment data and auditioned a large number of players representative of the payment chain and active in France: public bodies, professional organisations, banks and payment institutions retail companies, service providers specialising in the field of payment, etc.

86 - "La stratégie nationale des moyens de paiement scripturaux 2019-2024", published by the Banque de France in February 2019

The report we produced was published on the website of the Conseil général de l'économie[87].

The recommendations we made are not limited to the sole question of data localisation. It seemed difficult to isolate them from other questions related to the conditions of European independence in terms of payment. All are framed in the perspective of proposals likely to be brought by France for inclusion in European regulations.

In the course of our interviews, we were genuinely surprised to note that the idea of a data localisation obligation gathered broad support among those we spoke to, even within very international companies, provided of course that this obligation does not apply at the level of France but for the whole of the European Union. Only a very small number of international players opposed it, and their objections did not seem to us to stand in the way of our endorsement of the principle of payment data localisation in Europe.

We considered that there should be a close connection between the localisation obligation that we recommended and the GDPR: the payment data that we proposed submitting to this obligation are those relating to intra-European payments made by natural persons or for the benefit of natural persons, therefore personal data within the meaning of the GDPR. We assessed that the CNIL and the data protection officers in the companies concerned were best placed to ensure that this rule was respected.

It is already clear that the GDPR constitutes a valuable shield against the inappropriate use of payment data. But this protection is not always sufficient. The identification of the responsibilities defined by the GDPR (controller, joint controller or processor) and their relationship are often not clear when personal data passes from hand to hand between a series of players, often very numerous, in the processing of a payment operation.

It is common for an intermediary in this payment chain not to have a direct relationship with the originator or with the beneficiary of a payment, and not to be able through its own means to identify either of them. However, it is not justified in considering that the data are anonymous, that they are not bound by the rules on personal data protection or that it can use them as it wishes.

Moreover, even if the GDPR is in principle applicable to all, there are undoubtedly profound differences with regard to the possibility of assessing the compliance of a processing operation, of imposing sanctions and of ensuring the recovery of a fine, depending on whether the processing results from the activity of "an establishment, a controller or a processor in the territory of the Union" or that of a non-European player.

At this stage, the services of the European Commission have not explicitly taken a stand in favour of localising payment data in Europe. But the sovereignty concerns that underlie this idea remain all the more acute, as demonstrated by the invalidation in July 2020 by the Court of Justice of the European Union of the "Privacy shield"[88] adequacy decision, the Franco-German initiative GAIA-X, the ECB's commitment to SCT Inst instant payment, or the launch by the major European banks of the EPI (European Payments Initiative) project.

87 - Lemery S. and Steiner R., "Mise en œuvre d'une politique de localisation des données critiques de paiement en Europe", Report No. 2019/16/CGE/SG, 2020, economie.gouv.fr.
88 - *Judgment of the CJEU in case C-311/18 Data Protection Commissioner / Maximilian Schrems and Facebook Ireland* (PDF, 344 KB), 16 July 2020, curia.europa.eu.

PAYMENT IN EUROPE: A STRATEGIC ACTIVITY

In September 2020, the European Commission published a European strategy for retail payments[89]. For the Commission, "once relegated to the back-office, payments have become strategically significant. They are the lifeblood of the European economy".

The Commission notes that some of the important changes described in this White Paper could call into question European autonomy in relation to payments, and supports the creation of the future European EPI card scheme (see box on page 81).

As part of this strategy, it supports the widespread use of instant payment as a new standard, advocates the European standardisation of QR codes to enable the development of mobile payment, and emphasises the SEPA "Lookup proxy" standard which allows to transfer money without exposing one's IBAN.

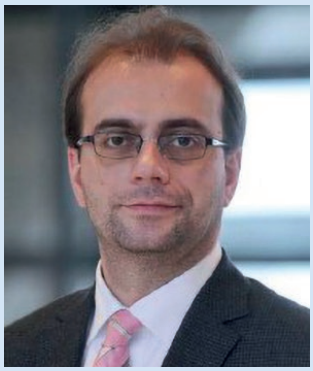
It wants to strengthen electronic billing and promote the acceptance of digital payments, but also maintain the availability of central bank money in cash. It supports the development of a digital euro and will launch, at the end of 2021, the review of the PSD2 directive, in particular on aspects of fraud prevention and on entities exempt from PSD2 authorisation. It also indicates that it wants to make the recipient, place and date of the payment more transparent. It wants to guarantee a right of access, under fair, reasonable and non-discriminatory conditions, to the technical infrastructures deemed necessary to support the provision of payment services (e.g. NFC chip).

89 - "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Retail Payments Strategy for the EU", 24 September 2020, ec.europa.eu; citation page 2.

Over to...

SÉBASTIEN RASPILLER

HEAD OF THE FINANCIAL SECTOR DEPARTMENT OF THE DIRECTORATE GENERAL OF THE TREASURY



SÉBASTIEN RASPILLER

Assistant Secretary, Head of the financial sector department of the Directorate-General of the Treasury. A graduate of the École Polytechnique. Former economist at INSEE. He then became a member of the fiscal policy office of the German Federal Ministry of Finance, before holding various positions at the Directorate General of the Treasury, notably as head of the sub-directorate for financial markets.

> ***Payment data: several key sovereignty issues***

Control of payment data, which brings together all the information essential for carrying out payment transactions and the context of transactions, is a major issue for States, with several key sovereignty issues:
(i) an issue of economic sovereignty, against the backdrop of the critical risk of a sudden cessation of activity by third parties in the payment chain;
(ii) an issue of financial sovereignty, with the increasing monetisation of payment data,
(iii) a central sovereignty issue, linked to the ability to protect individual payment data and because of the challenges involved in the fight against money laundering and the financing of terrorism;
(iv) a technological sovereignty issue, since control of payment data goes hand in hand with an innovative ecosystem and innovative services.

The 2019-2024 French national retail payments strategy has thus identified the control of payment data as a key issue, in terms of generation, processing and storage of this data. This choice is not unique in the world: several countries (Japan, Malaysia, China, Russia and India) have already decided, in light of these sovereignty issues, to assign very strict obligations within the framework of data (re)localisation policies, with in particular the obligation for players to establish their IT infrastructures processing payment data on the soil of the jurisdictions concerned.

Characterised by partly extra-European processing of critical payment data, Europe is lagging behind. The public report submitted by the Conseil général de l'économie on 15 February 2020 confirms this observation and the threats to European sovereignty linked to the current context, with many risks: political dependence, limited mutual legal assistance, espionage, lack of effectiveness of the GDPR, violation of the level playing field. In addition, the emergence of new payment solutions by the major technological players only reinforces the fear of disordered exploitation of payment data by third parties.

Within this context, France is determined to promote a truly independent Europe in terms of payment data. It therefore supports the European Payment Initiative, which should make it possible to both strengthen the European approach to payment data (by creating a pan-European scheme) and strengthen their processing for transactions as part of a pan-European payments solution.

In addition, France is actively participating in the work of the future crypto-assets regulation (known as "MiCA"), which aims, among other things, to subject private digital payment asset projects to a demanding European licensing regime, linked to an obligation for crypto-asset issuers to be established on European soil, which would require them to comply with European standards including with the GDPR.

Finally, in the context of drafting of the texts of the new digital strategy, France is endeavouring to convince its partners of the need to further explore the most promising avenues outlined by the aforementioned report of the Conseil général de l'économie : this would particularly involve deepening the separation introduced by the interchange regulation between the entity that provides governance (definition of standards) and that in charge of carrying out processing (interbank processing), by requiring them to locate their data centres (storage, place of processing, back-up) in Europe, like other foreign jurisdictions.

FOCUS ON...

The EPI (European Payments Initiative) project and its GDPR compliance challenges

Last July, a consortium of 16 European banks from 5 euro-zone countries launched a pan-European card scheme project aiming at competing with the American Visa and Mastercard schemes. The new proposal aiming at competing to offer classic direct debits but also instant (SCT Inst) transfers and a digital wallet for mobile payments. The project faces two challenges: the unification of the European payments market and European sovereignty in terms of payments (US sanctions may imply suspension of the operations of the card schemes). It ultimately aims for global coverage, via co-branding with the global schemes for international payments.

A provisional company was founded in Belgium and a call for new participants launched for the end of 2021. The launch of the peer-to-peer payment solution is scheduled for the first half of 2022, the e-wallet for the second half of 2022, followed by card-related projects planned by 2024 with a phase for migration from the existing infrastructure. The implementation of the system would involve significant investments and the updating of existing electronic payment infrastructures, which means convincing merchants and consumers of the added value of the project. Although the inclusion of instant transfers raises the question of the economic model of the project and possible revision of the 2015 "interchange" regulation, EPI has yet to decide whether to adopt the "request to pay" technique, whether to host the digital euro or even crypto-currencies as PayPal does.

To foster credibility to EPI's offer in the context of payments, the protection of privacy and GDPR compliance of the new solution will play a key role. EPI has every interest in making data protection a competitive differentiator and an element of its communication, including towards public authorities. EPI can now work towards this goal:

- by integrating the "privacy by design" rule (Article 25 of the GDPR) upstream in the conduct of its project, in particular, of the technological and organisational choices it will have to make, to avoid any irreversibility and based on a solid impact assessment;
- by seeking full compliance with the Schrems II judgment through an appropriate policy of outsourcing its cloud and servers that avoids any submission to US law;
- by seeking, if necessary, the advice of a European national data protection authority during the structuring phase on the most complex points of application of the GDPR.

Beyond that, it will be necessary to prevent the implementation of the EPI project from leading to the disappearance of the security promotion role currently performed by the approval of the GIE CB economic interest group in the ecosystem in France.

ROADMAP FOR SUPPORT AND EDUCATIONAL SOLUTIONS

As part of its missions, the CNIL aims to provide professionals with precision and predictability in its regulation, and legal certainty when necessary. It also wishes to provide the public with a better understanding of the issues of protection of privacy and personal data and in particular of the rights conferred by the GDPR. These objectives are reflected in the publication of so-called "soft law" instruments (repositories, recommendations, guidelines, practical guides, etc.) and in the posting of information and good practices on its website. This support is reflected, finally, in the implementation of a collaboration with "heads of network" associations, intended to facilitate appropriation of the GDPR by the professionals in a sector. These partnerships allow the joint writing of practical guides, codes of good practice or certification mechanisms.

In the field of payment data and means, on the basis of the avenues of work proposed by this White Paper, the CNIL intends to adopt a roadmap for the coming years based on three pillars: encourage good knowledge of the regulations and risks by individuals, support professionals in their GDPR compliance by using the European level as necessary, and promote inter-regulation to encourage the consistency of public action. The CNIL wishes to build this roadmap in partnership, as close as possible to the needs identified on the ground.

EDUCATIONAL TOOLS ON PAYMENT OPERATIONS FOR PLAYERS ON THE GROUND

The CNIL intends to improve the understanding of complex and highly technical issues among the audiences to which this White Paper is addressed (general public users, merchants, payment professionals, but also regulators, investors, etc.), in order to raise awareness of the risks to privacy and personal data and the rights and obligations attached to them (see Figure 15).

For consumers

At the end of the process to purchase goods or subscribe to a service, the moment at which payment is made traditionally creates a moment of "friction" when the data subject, the consumer, wonders about their rights[90] and also has to make informed choices about their personal data in order to keep control of them.

The CNIL intends to develop, with consumer associations, short educational sheets illustrating the main questions consumers should ask with regard to data and means of payment, including security. The aim is for highly ergonomic customer journeys to be accompanied by a good awareness of the privacy issues of the associated personal data protection, in order to promote an economy of trust.

For merchants

The world of commerce is very diverse when it comes to the question of payment data and means, whether in terms of channel (e-commerce or physical sales) or means (large retailers or very small businesses). But whatever the configuration, it must be informed about the challenges of protecting the personal data of its customers, including their international dimension, before offering them a payment solution.

The CNIL plans to work with the various relevant merchants' federations on fact sheets summarising the major questions that a merchant must ask itself when choosing a data processor for payment services, find anchors for negotiation with it and potentially be able to highlight to its customers solutions that are more protective of privacy and personal data.

For investors

For an innovative course in "open banking", GDPR compliance, a factor of trust for the customer is a key point, especially at the initiation stage where the choices of data protection by design and by default must be made. But investors need a framework to be able to audit the GDPR compliance of the business models in which they are interested.

As part of its innovation support policy, the CNIL intends to develop a framework for assessing the benefits and risks in matters of privacy and the protection of personal data, in partnership with leaders of the innovative ecosystems and seed investors. This framework would not be specific to payments, but payment projects would find in it benchmarks for compliance and trust.

Figure 13

Key points of application of the GDPR

Source : CNIL

90 - *Scenes from digital life, IP booklet no. 8* (PDF, 5.1 MB), in French, p. 41, 13 April 2021, cnil.fr

ACTION PLAN FOR SUPPORTING PROFESSIONALS IN THE FIELD OF PAYMENTS

The consultations carried out by the CNIL demonstrated the need for payment professionals, in a rapidly changing competitive environment, including with major international players, for a pact of trust with their customers with a value proposition that cannot be reduced to questions of cost or user experience, but which extends to the field of privacy and the protection of personal data. This framework of trust for the customer, which has not yet been established in all its components, is also a reference framework for operators in their GDPR compliance. Such an approach is necessary in order to promote innovation and in general a high level of protection of personal data in the payment economy.

With this in mind, the CNIL intends to develop, in the months and years to come, a partnership action plan to support compliance on several points on which needs have been expressed.

Towards a code of conduct for payment service providers, a factor of trust for individuals

A code of conduct is a sector-specific compliance tool resulting from a two-fold voluntary process: the decision by the organisation representing the sector to establish a code and the support of the professionals concerned. It is **a legally binding tool**, binding on those who adhere to it. It obliges adherents, on the one hand, to comply with the rules written within the code and, on the other hand, to accept that a designated third-party body controls its correct application. It may concern all compliance points, including security or transfers.

In the field of payments, a code of conduct would be the equivalent for the protection of personal data of the PCI-DSS certification verified by the Cartes Bancaires economic interest group for the security of card payments. The CNIL suggests that sector-specific professional associations lead the way in this project (with the participation, if necessary, of FinTechs and banks). Once drawn up, the code of conduct can be approved at European level for reasons of level playing field.

Doctrinal developments on certain critical points of compliance

Given the configuration of the sector, which is highly intermediated, payment data generally relate to a multitude of different beneficiaries, and as such is likely to reveal information relating to the private life of the data subjects, whether it is collected from several data controllers or by just one operator. The issues in terms of data protection are all the more important when these data are shared in order to be reused after the payment has been made. Thus, the CNIL intends, as part of its work programme and in consultation with the players, to develop a more precise doctrine applicable to processing operations which involve the concentration, pooling or reuse of payment data. In addition, these developments would be a trusted asset for all players, especially innovative players, who do not have the same resources to devote to compliance as large financial groups.

The work of the CNIL will clarify the conditions under which this processing can be considered. They may relate in particular to:

- **the qualification of the players:** according to their role in this complex environment, due to the number of intermediaries and the many regulations applicable to them;
- **the sharing of payment data between players:** whether it concerns the constitution of these shared databases or their use, each opening or sharing is a process subject to all the applicable data protection provisions;
- **enrichment of reused payment data:** assumed by a growing number of uses, in terms of the combat against fraud or for commercial purposes, the processing of data not strictly necessary to make the payment could contravene the principle of data minimisation laid down by the GDPR.

Security recommendations: tokenisation

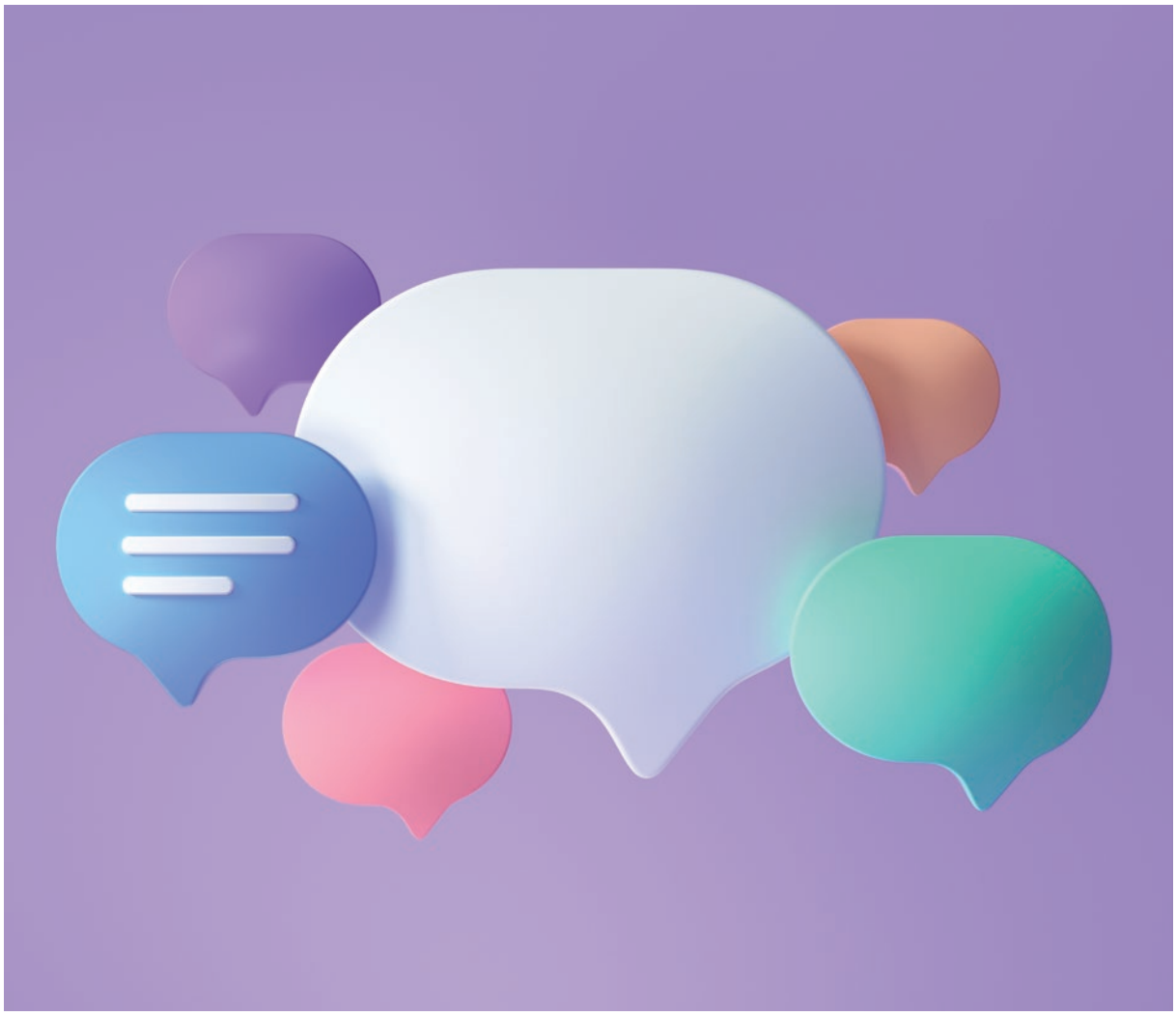
The CNIL intends to develop practical recommendations for the ecosystem and regulators, particularly with regard to the "tokenisation" (pseudonymisation) of these data: scope of the data concerned, techniques to use, good practices, etc.

A DIALOGUE TO BE MAINTAINED BETWEEN THE DIFFERENT REGULATORS

In the field of payments, and as illustrated by the contributions of the other regulators concerned to this White Paper, the issues of privacy protection and personal data protection interact with other regulations, both cross-sectoral and sector-specific. It is important that regulators exchange views on concrete solutions to compliance issues, but also that they cooperate to clarify as necessary the points of law arising from the various applicable regulations.

The CNIL will continue to maintain regular dialogue (including networking on specific points at the request of the professionals concerned) with the other institutions concerned by this inter-regulation. From a sector-specific point of view, this concerns the ACPR, the Banque de France and the Directorate General of the Treasury, but also on more cross-sectoral aspects, the Autorité de la concurrence and the Directorate General for Competition Policy, Consumer Affairs and Fraud Control (DGCCRF).

Finally, the CNIL will continue to collaborate with the other regulators concerned and the European institutions to contribute to current and future national and European regulatory debates concerning payment data and means of payment.



CONCLUSION/ACKNOWLEDGEMENTS

A WORD FROM THE COMMISSIONER

Philippe-Pierre CABOURDIN
Member of the CNIL college, senior counsellor to the Court of Accounts.

At the end of this economic and legal journey exploring the issues of privacy and the protection of personal data associated with payment data and means of payment, which shows all the complexity of these questions, three thoughts appear to me to stand out in particular.

The first is that means of payment are a good example of the strong links that unite personal data protection, competition regulation, financial regulation and consumer protection.

These fundamental objectives towards which this White Paper has built bridges show that regulators can only fully understand these questions by tackling them together. This subject calls for a high level of cooperation, which must be maintained and deepened between the CNIL and the ACPR or with the Autorité de la concurrence.

The second is about the diffuse nature of the flows of payment data and related data, across the economy, in France and abroad. The payment data that were once strictly defined and confined in the banking systems are now reused, even captured, and combined with other data, and they circulate internationally even for domestic transactions.

This advocates not only for the idea of making it subject to financial regulation or banking data protection, but also for the adoption of a broad vision of regulation, ranging from the responsibility of merchants and the emerging issues of monetary policy to the responsibility of the major Internet players. Part of this debate can obviously only be conducted at European level at least.

The third postulates that payment is an intrinsically political object, which must be addressed by public debate. Citizens must be able to decide, in full knowledge of the facts, to whom they entrust their payment data, with what risks and for what uses. They must have the tools to avoid the risks of their data being traced or compromised. Maintaining non-traceable means of payment, including for central bank digital currencies, and hence the free choice of means of payment below a threshold to be established, is essential for public freedoms and for our economic freedoms. Finally, payment is a matter of sovereignty, of individuals as well as of States.

This is why democratic control over the challenges of payment systems and the associated freedoms is absolutely essential. May this White Paper contribute to it!

Within the context of preparation of the CNIL White Paper "When trust pays off: today's and tomorrow's means of payment facing the challenge of data protection", the following entities were consulted:

- 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 (representing POS systems)

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

The CNIL would particularly like to thank its partners:
- Association du paiement
- ACSEL (digital economy association)
- La mission numérique grands groupes

GLOSSARY

3D-Secure protocol: protocol putting the payer in touch with the bank issuing the bank card in order to authenticate the payer for an online payment.

Account information services: under the PSD2, services that allow a natural person or legal entity to group together on a single interface the information on one or more of their payment accounts (Account Information Service Provider or AISP).

Account servicing payment service provider (ASPSP): in the PSD2 regime, a payment service provider that provides and manages payment accounts for payers.

API (application programming interface): programming interface allowing two programs or software packages to interact with each other, by connecting to exchange data, used in particular in the PSD2 regime.

Biometric data: personal data enabling a natural person to be uniquely identified.

Blockchain or Distributed Ledger Technology: register (large database) decentralised (shared simultaneously) between all its users, all also holders of this register, and who also all have the ability to enter data, according to specific rules established by a computer protocol secured cryptographically.

Book money: as opposed to fiat money, a form of money resulting from sets of entries in the accounts of private financial entities and representing a claim on these entities.

Cashless means of payment: payment cards, cheques, bank transfers, direct debits, paper instruments and electronic money.

Central bank digital currency (CBDC): element of the monetary base, exchangeable at par with fiat money and reserves, available permanently and in peer-to-peer transactions and circulating on digital media.

Central bank money: money issued directly by a central bank in the form of coins and banknotes (fiat money) and sums placed by commercial banks in the accounts they hold with the central bank, allowing them not only to stock up on banknotes, but also to ensure the maintenance of sums in reserve (the "minimum reserves").

Clearing: between financial institutions, a transaction always has a debtor and a creditor. Clearing is materialised by the book-entry transfer that traces the transaction. The credit to the creditor's account is said to clear the debit from the debtor's account.

Cryptocurrency: monetary value represented in digital and decentralised form, which uses cryptographic algorithms and a blockchain protocol to ensure the reliability and traceability of transactions.

Electronic money: monetary value stored in electronic form, including magnetic, representing a claim on the issuer, which is issued against the remittance of funds for the purpose of payment transactions and accepted by a natural person or legal entity other than the electronic money issuer.

Electronic purse or e-wallet: solution allowing a user to entrust to a third party, deemed to be trusted, payment instruments and data, without recourse to a bank account.

Fiat money: banknotes and coins issued by public authorities and being legal tender.

Highly personal data: according to the European Data Protection Board, data increasing the possible risk for the rights and freedoms of individuals, the violation of which would clearly have serious consequences in the data subject's day-to-day life (financial data that could be used to make fraudulent payments, for example).

Instant payment: permanently available electronic payment solution resulting from immediate or almost immediate interbank clearing of the transaction.

International data transfer: any communication, copy or movement of personal data intended to be processed in a country outside the European Union.

Means of payment: any instrument that allows a person to transfer funds, regardless of the medium or technical process used.

NFC ("Near Field Communication") contactless communication technology: technology allowing two terminals located near to each other and equipped with said technology, for example a smartphone and a payment terminal, to exchange data and instructions very quickly.

GLOSSARY

Payment (according to the French Civil Code): voluntary performance of the service due which discharges the debtor with regard to the creditor and extinguishes the debt.

Payment card data: for the CNIL, the data necessary for carrying out a remote transaction by payment card are the card number, the expiry date and the security code.

Payment initiation services: under the PSD2, services that allow a natural person or legal entity to order the execution of payment transactions, for example bank transfers, from an interface (website and/or mobile application) which is not necessarily that of the bank in which their account (or accounts) is (are) held (Payment Initiation Service Provider or PISP).

Payment system: type of market infrastructure providing interbank settlement of retail payments from bank customers or large amounts between financial institutions.

Payment operation: action initiated by the payer, or on his behalf, or by the beneficiary, consisting in paying, transferring or withdrawing funds, regardless of any underlying obligation between the payer and the beneficiary (definition from the PSD2).

Personal data: any information related to an identified or identifiable natural person, directly or indirectly (GDPR definition).

SCT Inst: euro area cross-border instant payment, also known as SEPA Instant Credit Transfer.

SDK or Software Development Kit: development tool used to create a feature on a platform.

Sensitive data: within the meaning of the GDPR, personal data revealing the alleged racial or ethnic origin, political opinion, religious or philosophical conviction or trade union membership, as well as the processing of genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning the sex life or sexual orientation of a natural person.

SEPA (EU): retail interbank payment system based on an infrastructure operating on the basis of multilateral clearing with deferred settlement occurring once a day in central bank money.

Strong authentication: in the PSD2 regime, procedure allowing the payment service provider to verify the identity of a payment service user, to protect the confidentiality of their data, and based on the use of two or more independent elements belonging to the categories "knowledge" (something that only the user knows), "possession" (something that only the user has) and "inherence" (something that the user is).

Tokenisation: computer security process making it possible to replace critical data with an equivalent element that has no intrinsic value or meaning that can be exploited once it has left the system. To present a satisfactory level of security, a token must be irreversible and generated randomly.

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