You Are What You Pay – Personal Profiling with Alternative Payment Data and the Data Protection Law

PAULINE AFFELDT AND ULRICH KRÜGER

Pauline Affeldt, DIW Berlin/TU Berlin, e-mail: PAffeldt@diw.de
Ulrich Krüger, Hochschule Bremen, e-mail: ulrich.krueger@hs-bremen.de

Zusammenfassung: Nicht erst seit der Corona Pandemie gibt es weltweit den Trend zum bargeldlosen Zahlungsverkehr. Zudem beflügelt die Vorstellung eines zielgenauen Behavioral (Big Data) Scoring die Fantasien von Investoren in der Datentechnologiebranche. Es scheint ökonomisch verführerisch, beide Trends zusammenführen, wenn man alle Daten aus dem Zahlungsverkehr für ein persönliches Profil auswerten würde. Dieses Geschäftsmodell liegt jedoch mit dem Recht des Einzelnen auf informationelle Selbstbestimmung im Konflikt und wirft Fragen auf im Hinblick auf Ungenauigkeit, Diskriminierung und Intransparenz. Unser Artikel gibt einen Überblick über die ökonomische Entwicklung des Sektors und eine rechtliche Bewertung insbesondere aus Sicht der europäischen Datenschutz-Grundverordnung. Nicht alles was im Big Data Scoring mit alternativen Zahlungsdaten möglich sein könnte, ist in Europa auch rechtlich zulässig. Vor allem für die „klassischen" Banken könnte sich gleichwohl eine Möglichkeit eröffnen ihre internen Credit Scoring Systeme zu verbessern und mit angepasst-individuellen Kundenprofilen weitere ihrer Finanzdienstleistungen zu vertreiben.

Summary: The global trend toward cashless payment started well before the corona pandemic. Along with it, investors in the data-driven tech industry are inspired by the promise of targeted behavioral scoring based on big data. It seems economically tempting to combine these two trends by using all data generated by the payment services to create personal profiles. However, this business model conflicts with the individual's right of informational self-determination and raises questions regarding inaccuracies, discrimination, and the non-transparency of the algorithms underlying these profiles. Our article provides a short overview over the recent economic developments in the financial service industry and a legal assessment in light of the GDPR. Not everything that is feasible with big data scoring using alternative payment data is legally allowed in Europe. Nevertheless, traditional banks could have the opportunity to improve their internal credit scoring systems and use individual customer profiles to further market their financial services.

→ JEL classification: G20, G23, G28
→ Keywords: alternative payment data, personal profiling, credit scoring, GDPR, data protection law

DOI https://doi.org/10.3790/vjh.89.4.73
Vierteljahrshefte zur Wirtschaftsforschung | DIW Berlin | volume 89 | 04.2020 | pages 73–88

1 Introduction

"Facebook sees what you like and Google sees what you're looking for. We see what you're paying for and that can be more powerful in many ways."

This was the outlook Markus Braun gave as CEO for his Fin Tech payments company, Wirecard, in October 2019 (Lindner, 2019). In 2018, Wirecard had replaced Commerzbank, a large, old, and traditional bank based in Germany, in the DAX stock market index. Then, in June 2020, Wirecard declared bankruptcy, accused of a massive accounting fraud.

Despite this particular scandal, cashless payment systems are growing quickly. FinTechs like Wirecard and PayPal are pushing into the market, alongside BigTechs. Cashless payments generate data about who pays whom, when, how much, where, and possibly for which product or service. It is obvious that these kind of datasets can have great value for companies seeking to build customer profiles. With its credit scoring system, the financial services sector has a well-established form of customer profiling. Credit scoring systems once built on datasets containing traditional information like address, age, gender, and punctuality of payments. With the accelerating and ubiquitous dissemination of cashless payment systems, the attempts and temptations increase to use the data generated by cashless payments, which are "alternative" to the ones used up to now (Hurley and Adebayo, 2016; Consumer Financial Protection Bureau, 2019).

On the one hand, the benefits for the companies are obvious. On the other hand, these forms of personal profiling create numerous concerns for privacy and consumer protection. Such diverging interests must be balanced. As a first and important step to create a legal framework for the data industry, the European Union issued the General Data Protection Regulation (GDPR) in 2018.

Our article reviews the development and approaches for the economic use of payment data for customer profiles and provides a legal assessment of the potential data uses in light of the GDPR.

2 From Fintechs to BigTech in Financial Services

2.1 Developments in Financial Services Markets

The financial services industry has seen big changes since the global financial crisis in 2008. Prior to 2008, innovation was mainly driven by the incumbent financial institutions and their investment in technology to support their operations. Since 2008, so-called Fintech startups have increasingly entered the financial service market, disrupting traditional banking (Zetzsche et al., 2017).

Fintech is defined as "technology-enabled innovation in financial services that could result in new business models, applications, processes or products with an associated material effect on the provision of financial services." (Financial Stability Board, 2017, p.7). Thus, it comprises financial innovations based on digital technologies and the use of big data that have the potential to disrupt traditional banking.

The first Fintech companies mainly started by offering cashless payment services that allowed secure online payments in a world with increasing online shopping. In 2020, Fintech companies

DOI https://doi.org/10.3790/vjh.89.4.73

offer all kinds of financial services that were formerly solely provided by banks, including cashless payment, digital lending, digital banking, digital investment management, personal finance, blockchain, and insurtech (Stulz, 2019).[1] In many cases, Fintechs essentially unbundle services formerly offered by banks. However, Fintechs usually do not have a banking license, so they still need to mostly rely on existing payment infrastructure provided by financial institutions.

Fintech credit, which is credit activity that is facilitated by electronic platforms not operated by commercial banks, differs from traditional credit by being mostly digital: there is no branch distribution network and most customer and loan origination processes are digitalized, including the credit decision. In particular, algorithms and machine learning techniques are used to predict individual default risk based on big data (Claessens et al., 2018).

One classical example of a successful Fintech is PayPal, which started in 1998 as a money transfer and digital payment transfer system relying on existing payment infrastructure in the US. Some 22 years later, PayPal is one of the largest payment service operators worldwide with a presence in over 200 countries.[2] PayPal has also diversified into financial services other than cashless payment including lending activities (Tanda and Schena, 2019).

In addition to Fintechs, like PayPal or Wirecard, BigTech platforms, including Amazon, Facebook, and Google are increasingly pushing into the market for financial services. The financial service efforts of these companies is often termed TechFin, thus distinguishing them from Fintech companies.

Fintechs and TechFins have in common that they are all digital native companies that use technology to develop innovative financial services (Tanda and Schena, 2019). However, Fintechs are companies specializing in financial services and competing with specific product lines of banks, while TechFins start with their technology, data, and access to their customers before deciding to add certain financial services as part of their broad services, while their core business is still IT and consulting (Stulz, 2019, BIS, 2019).[3] Therefore, Zetzsche et al. (2017) characterize Fintechs as financial intermediaries and TechFins as data intermediaries, with the main competitive strength of TechFins coming from their massive datasets on customer transactions and behavior on their platforms as well as their data analytics capabilities (King, 2019).

1 Well-known examples of Fintechs in cashless payments are Stripe, PayPal, and Wirecard. Examples of Fintechs in digital lending include the peer-to-peer lending platforms LendingClub in the US and FundingCircle in Europe. An example of a Fintech in digital banking is N26, a German online bank, which initially started in 2013 as an interface with the backend provided by Wirecard; it obtained its own banking license in 2016. Robinhood is an example of a US Fintech that offers stock trading, ETFs, cryptocurrencies, and options via a mobile app. For more examples of successful Fintech companies see also Stulz (2019) or the 2020 Forbes list of the biggest Fintech Companies in America (https://www.forbes.com/sites/jeffkauflin/2020/02/12/the-10-biggest-fintech-companies-in-america-2020/#6015523c1259).

2 According to PayPal's Q4 2019 results, in 2019, over 12 billion payment transactions generated $712 billion total payment volume and almost 40 million net new active accounts led to 305 million active PayPal accounts at the end of 2019 (see https://www.paypal.com/stories/us/paypal-reports-fourth-quarter-and-full-year-2019-results).

3 According to BIS (2019), these activities account for about 46 % of their revenues while financial services only made up about 11 % in 2018. The sample includes Alibaba, Alphabet/Google, Amazon, Apple, Baidu, Facebook, Grab, Kakao, Mercado Libre, Rakuten, Samsung and Tencent. See BIS (2019) for further details.

DOI https://doi.org/10.3790/vjh.89.4.73

Most BigTech companies have entered financial services by offering payment services that facilitate their core business (e-commerce for Amazon, targeted advertising for Google and Facebook) (Frost et al., 2019). BigTech has also expanded into savings and investment products, insurance, and credit provision (BIS, 2019; Tanda and Schena, 2019). Just like Fintechs, they typically rely on existing payment infrastructures and offer most of their financial services in cooperation with financial institutions (Frost et al. 2019). For example, Apple, Google, and Facebook have all entered the financial service markets in North America and Europe by offering the inhouse payment tools Apple Pay, Google Pay, and Facebook Messenger, respectively. For this, they each partner with banks that provide the global payment network to process and settle payments (BIS, 2019).[4]

Some TechFins have also moved into credit provision, mostly to SMEs and consumers (BIS 2019). Amazon, for example, started building up not just payment services but also other strategically important financial services that support its e-commerce platform. In 2007, it started offering payment services with Amazon Pay to increase sales and obtain additional revenues from the interchange fees (King, 2019). Amazon then launched lending services to both consumers and small businesses (Tanda and Schena, 2019). Since 2011, Amazon Lending provides loans to small businesses that sell their products via Amazon, thus increasing sales on its e-commerce platform by helping the merchants finance their Amazon inventories (King, 2019).[5]

2.2 Reasons for BigTech Entry into Financial Service Markets

We believe that there are several reasons why BigTech companies are increasingly entering financial service markets, especially payment services.

First, they might be attracted by the profits from the financial services; for example, interchange fees from payment services. However, this is unlikely to be the main motivation underlying the proffering of financial services.

Rather, BigTechs started offering payment and lending services as a natural next step to strengthen their core business. Many of these platforms identified the need for secure online payments to ensure that sellers on the platform could not disappear with the money but without shipping the product (BIS, 2019). For example, Alibaba created the online payment gateway Alipay in 2004 as a means to solve the trust problem between merchants and customers on its e-commerce platform: it keeps the money in escrow accounts until merchants' goods are delivered to customers (King, 2019).

BigTechs, unlike Fintechs, are primarily technology firms whose essential goal is to create a whole ecosystem of core and complementary products and services where their users can fulfill all their needs (including financial services) on one platform (Tanda and Schena, 2019). There are strong

4 For example, Apple partnered with American Express and banks to offer ApplePay; in August 2019, it issued a credit card with Goldman Sachs (King, 2019, Frost et al. 2019)). Apple Card is a virtual credit card that can be used from the Apple Pay app and integrated into the Apple Wallet (Tanda and Schena, 2019). Facebook cooperates instead with PayPal to allow users to send money via Facebook Messenger (King, 2019). In June 2019, Facebook also announced its plans to launch a digital currency, Libra.

5 For example, in the US, Amazon has lent over $1billion to small and medium sized businesses in the period June 2019–May 2020 (Amazon, 2020).

DOI https://doi.org/10.3790/vjh.89.4.73

complementarities between the core activities of BigTech and financial services, thus allowing the companies to profit from economies of scale and scope (BIS, 2019).

BigTechs typically operate in multi-sided platform markets characterized by indirect network externalities between the different user groups. For example, for the buyer, the value of an e-commerce platform like Amazon increases with the number of sellers on the platform. Vice versa, the platform is more valuable for sellers, the more potential buyers they can reach via the platform. Offering a whole ecosystem of products and services might help BigTech companies to reinforce indirect network externalities. As more products and services are offered, the platform might attract more users on one side of the market (e. g. buyers), which in turn attract more users on the other side of the market (e. g. sellers), and so on.

Platforms might also bundle their existing services with their new financial products, such as offering cheap credit to customers who purchase via their e-commerce platform. This will help lock-in consumers on a given ecosystem while decreasing switching and multi-homing on competing platforms (De la Mano and Padilla, 2019). For example, Zhima Credit, the credit business of Alibaba's Ant Financial,[6] rewards customers for having a high credit score with easier access to loans from Ant Financial and a more trustworthy profile on e-commerce sites within the Alibaba Group.

Lastly, BigTech companies are essentially data firms that already "own" vast amounts of data on their customers. This provides two additional reasons for these firms to enter financial services.

First, in addition to the large installed customer base, the established reputation, powerful brands and access to capital markets, BigTechs can leverage their existing data advantage to provide (better) financial services efficiently (De la Mano and Padilla, 2019; Zetzsche et al., 2017). A core strength of BigTech firms is their ability to collect and analyze data on consumer behavior using artificial intelligence and recent machine learning techniques (King, 2019). This provides them a competitive advantage over banks. The customer data collected in their core business potentially gives BigTech companies superior information to assess, for example, the creditworthiness of borrowers based on soft information (e. g. consumer preferences, habits, and behavior) that banks do not have. Thus, they can provide credit to consumers who do not fulfill formal bank loan requirements or reduce the need for collateral (BIS, 2019; Frost et al., 2019). Their better knowledge of the analytical tools also implies an advantage in processing the massive datasets compared to financial institutions, which should be reflected in either lower costs per loan or lower default rates (Frost et al., 2019).

Second, BigTech firms might be interested in collecting even more data on their customers based on the financial services offered, such as customer payment data, to enlarge their databases even further. In particular, account information and payment transactions generate so-called "alternative" payment data, detailing who pays whom, when, where, and for what. According to De la Mano and Padilla (2019), BigTechs have incentives to expand into areas outside their core business to collect data generated in those markets because it allows them to combine the data generated on their various platforms, products, and services to create "super-profiles." These "super-profiles" allow for targeting consumers when and where they are likely to need their services. Additionally,

6 Ant Financial (formerly Alipay) is the company regrouping Alibaba's financial services.

DOI https://doi.org/10.3790/vjh.89.4.73

more data helps platforms to increase their network externalities: The richer data going into data analytics allows for offering even better services and products, which will again attract more users and so on (BIS, 2019). Thus, network externalities are stronger on platforms that offer a wide range of services and products.

2.3 Potential Uses of Alternative Payment Data

2.3.1 Alternative Payment Data

BigTech's financial services, in particular cashless payment services, allow for the collection of alternative payment data detailing who pays whom, when, where and for what. Alternative payment data is understood as data that goes beyond the conventional recording of payment punctuality. Even bank account transaction data includes information on utility and rent payments, regular transactions, records of deposits and withdrawals, medical and insurance claims, credit card transactions, and so on (Jagtiani and Lemieux, 2019).

Using all of this information, i.e. for the assessment of an applicant's creditworthiness, already goes beyond the traditionally used information on individuals' payment history, outstanding debt, length of credit history, pursuit of new credit, and debt-to-credit ratio. However, TechFins know much more about consumers than just this. The data collected by platforms like Amazon, Google, and Facebook contain information on transactions (sales volume and average selling price), reputation-related information (claim ratio, handling time, reviews, complaints), and industry specific characteristics (sales seasonality, demand trends) (BIS, 2019). Other non-traditional user data include information on occupation and education, retail preferences, browsing behavior, social media activities (and identity of "friends"), geolocation data, cable and cellphone account data, online purchase history, as well as criminal and arrest records (Hurley and Adebayo, 2016). TechFins could combine all of this information into a comprehensive view of their customers' preferences and behaviors (Zetzsche et al., 2017). For example, the alternative credit-scoring company ZestFinance states that it uses borrower's data,[7] proprietary data, public data,[8] and social network data. Proprietary data includes information obtained from data brokers, which can contain a lot of individual information from online and offline purchase history to health and medical information. Social media activity can include aggregated information from applicants' as well as his/her social network's social media posts (Hurley and Adebayo, 2016). These firms typically own thousands of data points on each individual. Jack Ma, founder of Alibaba, stated in 2015 that Alibaba has an average of 20,000 to 25,000 data points on each individual consumer (Zetzsche et al., 2017); a number that has surely only increased.

This naturally raises the question regarding the purposes for which BigTech firms want to use these massive customer datasets, including the payment data generated by their payment services.

7 Borrower's data includes the information provided by the credit applicant during the application process but also browser activity during the application process. For example, it might be recorded how much time an applicant spent reviewing the terms and conditions.

8 Public data is all information that can be obtained on an individual via automated Internet searches and webscraping.

DOI https://doi.org/10.3790/vjh.89.4.73

2.3.2 *Potential Uses*

First, alternative payment data could be processed and used in customer profiling for credit scoring. In credit scoring, using alternative payment data, all information on an individual's payment history, but also her preferences and behaviors, is processed through machine learning algorithms that have established correlations between certain preferences or behaviors and an individual's default risk. These scores might draw a much more nuanced picture of creditworthiness than traditional bank assessments (Zetzsche et al., 2017; De la Mano and Padilla, 2019).[9] The digital footprint of an individual, for example, provides proxies for character. As an example, self-control can be proxied by the time of the day when a customer makes a purchase. Berg et al. (2018) find that customers who make a purchase between noon and 6pm are about half as likely to default on a payment as customers purchasing between midnight and 6am.

This credit scoring could be internal credit scoring by the company collecting the data, i. e. BigTech companies, because they are active themselves in payment or credit services. For example, Amazon wants to assess small merchants' default risk before granting credit lines to finance merchants' Amazon inventories.

Alternatively, BigTechs could sell the (raw or pre-processed) alternative payment data and further consumer information to external credit scoring firms (like ZestFinance) and financial institutions who then process and feed it into their algorithms to determine credit scores.

Zetsche et al. (2017) argue that TechFins enter financial services typically in three stages. In the first stage, they simply license out aggregate data to financial institutions or Fintechs for data analytics such as credit scoring. In the second stage, they use the data to guide their own business decisions, such as Amazon assessing risk before lending money to small sellers. In the third stage, TechFins might offer a broader range of financial services and actually compete with incumbent banks.

Secondly, the data could be used to create customer profiles for marketing BigTech companies' own financial services. For example, when a consumer searches for a car or a house via Google's search engine, Google can directly offer its own financial services (De la Mano and Padilla, 2019). Furthermore, based on customer profiles, TechFins may be able to assess consumers' willingness to pay for certain services, allowing them, for example, to adjust credit rates to the borrower's default risk but also to price discriminate if the data allows for identifying the highest rate the borrower would be willing to pay (BIS, 2019; Zetzsche et al. 2017). This implies that TechFins could increase prices for price inelastic customers or customers with high switching costs (De la Mano and Padilla, 2019).

9 Berg et al. (2018), for example, predict payment default risk based on a dataset with about 250,000 observations from an e-commerce company located in Germany. They use simple digital footprint information, like the device type, the operating system, the time of the day when purchasing etc. as predictors of default risk. They find that these variables, which are constructed from the digital footprint, proxy for income, character, and reputation, and actually lead to better predictions of default risk than when using the credit bureau score used by the e-commerce company. The best predictions are reached when combining the credit bureau score and the digital footprint data. All of the analysis is based on parametric regressions. Instead, Björkegren and Grissen (2019) use standard machine learning techniques – random forests and logistic regression using a model selection procedure – to predict payment default of mobile phone bills in a middle-income South American country based on mobile phone usage data. Of course, the context is different as, firstly, it is not about traditional bank loans and secondly, the question is also whether access to credit can be given to the unbanked based on non-traditional data. However, this paper also finds that predictions based on mobile phone usage data outperform those based on credit scores (where available). These two empirical papers indicate that the use of non-traditional data in credit scoring could indeed lead to more accurate predictions of default risks.

DOI https://doi.org/10.3790/vjh.89.4.73

Lastly, BigTechs could use customer profiles based on payment data to increase sales of their other services. For example, Amazon could help merchants with price discrimination depending on individuals' willingness to pay, while more precise customer profiles help Google and Facebook improve the quality (and therefore sales) of targeted advertising space. This advertising could relate to non-financial and financial products alike. For example, Google could also use its customer profiles to advertise and price third-party financial services, like credit or insurance, at the moment a user needs them (BIS, 2019). Google's and Facebook's business models are to monetize data, so it is likely that all collected data (alternative payment data and other) will be used to improve their targeted advertising.

The use of these massive consumer level datasets raises many issues. It is unclear whether using this data for the aforementioned purposes is beneficial in terms of consumer surplus or total welfare. It also raises important privacy and consumer protection issues. In light of the introduction of the GDPR in May 2018, we assess in the remainder of this article whether these potential uses of customer data, in particular customer payment data, are permitted under the GDPR.

3 The Legal Framework of Personal Profiling with Alternative Payment Data

After years of negotiation and under considerable lobbying pressure of powerful interest groups, especially from the US digital industries, the GDPR came into force on May 25, 2018. It applies to the processing of personal data in the context of the activities of a company in the European Union, regardless of whether the processing takes place in the EU or not (Art. 3 GDPR[10]). In a 2020 judgement the Court of Justice of the European Union invalidated the Privacy Shield Decision for the transfer of data to the US (CJEU Judgement, July 16th, 2020, C-311/18 "Schrems II"). It made clear that the law is strict regarding its territorial scope. The regulation is also strict in its standard of data protection: the processing of personal data is generally forbidden, unless it is allowed under the exceptions in Art. 6.

The GDPR provides special rules to protect users from the risks of customer profiling which is defined in Art. 4 (4) as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements." The GDPR's rules for data protection in the area of customer profiling have two dimensions: on the one hand, there are legal restrictions *for processing* personal data for personal profiling as such (Art. 6 etc.) and, on the other hand, *for the use* of these personal profiles for automated individual decision-making (Art. 22). Following these two legal perspectives, personal profiling with alternative payment data will be subsumed below under the GDPR data protection rules.

In addition, aspects of consumer protection play a role when personal profiles like credit scores are used to decide which kind of contract should be concluded with which consumer and on what terms. Consumer protection under an (neo-classical) economic perspective reflects mainly the functionality of consumer markets with the ideal of the "average, reasonably well-informed and

10 Until otherwise specified, cited Articles are from the GDPR.

DOI https://doi.org/10.3790/vjh.89.4.73

reasonably observant and circumspect consumer", a concept developed by the Court of Justice of the European Union in the 90s. Over the last 20 years the perspective changed more to the legal protection of the weaker party in the socio-economic situation of "vulnerable consumers"[11]. They could be particularly affected for example by alternative credit assessment tools targeting them with high-cost loan products (Hurley and Adebayo, 2016)

The usage of alternative payment data to create customer profiles is "processing of personal data wholly or partly by automated means" (Art. 2) and, therefore, within the material scope of the GDPR. Art. 5 describes the basic principles of data protection, e. g. that data relating to natural persons may only be used for the purpose specified in advance (Art. 5 I b). The "data subject" must be informed about this in a "concise, transparent, intelligible and easily accessible form, using clear and plain language" (Art. 12). However, to be lawful, the processing must, above all, fulfil at least one of the six legal prerequisites in Art. 6. In addition, the special rule for scoring in the German law in § 31 BDSG (Bundesdatenschutzgesetz) must be taken into account.

3.1 GDPR: The Legal Basis in Art. 6

For the case of processing alternative payment data, there are three relevant legal bases in Art. 6: (a) consent, (b) necessity for the performance of a contract, and (f) legitimate interest. Before assessing these legal conditions in the concrete case of alternative payment data, we provide a short explanation of each basis.

3.1.1 Consent, Art. 6 I a)

Processing of personal data shall be lawful only if, and to the extent that, the data subject has given consent to the processing of her or his personal data for one or more specific purposes (Art. 6 I a)). Consent must be freely given, specific, informed, and unambiguous (Art. 4 II, Art. 7).

The requirements for the consent of the user under the rules of the GDPR are high. This is not an expression of paternalism but reflects the actual contractual situation with significant inequality and massive lock-in effects. In addition, users show cognitive difficulties in decision making, since they generally consider privacy issues as very important but are quite willing to give away their own personal data for minor advantages ("privacy paradox"). Consent as the contractual instrument to balance interests needs further legal arrangements. All in all, here the GDPR shows a convergence with the consumer protection rules on unfair terms in European contract law (Simitis et al., 2019, Albrecht, Art. 6 GDPR, 4 ff.; Clifford et al., 2019).

Aside from the high standards for a legally binding consent, the risk of its free withdrawal guaranteed by Art. 7 III GDPR makes the justification of data-processing based on the user's consent often problematic from the payment companies' point of view. In addition, the possibility for a

11 The concept of the "vulnerable consumer" is by now well established and can be summarized by distinguishing five dimensions of consumer vulnerability: "A consumer, who, as a result of socio-demographic characteristics, behavioural characteristics, personal situation, or market environment is
- at higher risk of experiencing negative outcomes in the market,
- has limited ability to maximise their well-being,
- has difficulty in obtaining or assimilating information,
- is less able to buy, choose or access suitable products, or
- is more susceptible to certain marketing practices" (European Commission, 2016, p. XX).

DOI https://doi.org/10.3790/vjh.89.4.73

payments company to swap from consent to a different basis would be difficult: first asking customers for their consent, and then stating that it was not needed anyway is not a convincing reasoning (Uecker, 2019).

3.1.2 Necessity for Performance of Contract, Art. 6 I b)

According to Art. 6 I b), data processing is allowed if it is necessary (and not only useful!) for the performance of or the entering into a contract. An online-shop, for example, can lawfully transfer the address of the customer to the postal service to deliver the goods. On this basis, companies avoid the difficulties of getting a valid consent and the customers have neither a free right of withdrawal (Art. 7), because there is no consent involved, nor a right to object to the processing according to Art. 21, because it is not based on Art. 6 I f) (Gausling, 2019).

3.1.3 Legitimate Interest, Art. 6 I f)

Nevertheless, in many cases the proportionality test in Art. 6 I f) of the GDPR is the most important legal basis. Data processing is deemed lawful when processing is necessary for the purposes of the legitimate interests pursued by the company, except where such interests are overridden by the interests or fundamental rights and freedoms of the customer.

This rule is flexible and vague as well. Regardless, it imposes extra responsibility upon the company to ensure that the processing of data has a minimal privacy impact, in a way users can reasonably expect. Furthermore, as mentioned, Art. 21 states for the basis of Art. 6 I f) that "the data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data (...), including profiling".

3.2 Special Rule for Scoring in German Law: § 31 BDSG

The German legislature has decided to regulate scoring-systems in § 31 BDSG in succession to pre-existing German rules, albeit with reference to the EU GDPR. Even if it is uncertain whether the German legislature had the competence to pass European legislation on the opening clause of Art. 22 II b),[12] it remains an additional basis for the legal assessment of credit scores in Germany. Moreover, good reasons can be found to welcome a first form of regulation of algorithms, especially in the area of credit scoring.

§ 31 BDSG is not applicable to forms of customer profiling for advertising purposes, as the necessary concrete reference to a contractual relationship is missing (Simitis et al., 2019, Ehmann, Art. 6, annex 2 GDPR, 31). However, the processing must be lawful according to Art. 6 GDPR. In addition, German law requires that the data used to compute the probability value, based on a scientifically recognized mathematical-statistical procedure, must be significant for calculating the probability of the specific behavior. To use exclusively the address for this purpose is forbidden by law (§ 31 I No. 3 BDSG).

12 contra: Simitis et al. (2019, Ehmann, Art. 6, annex 2 GDPR, 20), pro: Krämer (2020).

DOI https://doi.org/10.3790/vjh.89.4.73

3.3 Lawfulness of Processing Alternative Payment Data for Personal Profiling

Each of the potential uses of customer profiles based on alternative payment data, carved out in B III., are assessed in light of these legal requirements.

3.3.1 Internal Credit Scoring

Normally, banks check the creditworthiness of their customers before granting a loan with a query at an external credit agency but also with information available within the bank, mostly with internal scoring systems. To use alternative payment data for this, the data processing could be justified either with a consent according to Art. 6 I a), which would have to meet the high requirements mentioned above, or, in case of a specific credit inquiry by the customer, with the necessity of a credit assessment prior to entering into a contract pursuant to Art. 6 I b).

Most important is the justification of data processing with the balancing of interest in Art. 6 I f): In case of contracts with a credit risk, there is a comprehensible economic interest of the contractual partner in being able to estimate the risk. Credit scoring provides a suitable means for this purpose. In addition, there is, as mentioned, a legal obligation to do so under European law (Directive 2014/17/EU), which is implemented in German law in § 18 a KWG (Kreditwesengesetz) and § 505 a BGB (Bürgerliches Gesetzbuch). On the other hand, the processing of alternative payment data can be burdensome from a consumer's point of view: A lot of data detailing financial and personal circumstances are processed here, which will be incorporated into profiles based on predictive algorithms. However, a positive credit scoring, especially from alternative payment data, can give people access to financial services that they would not otherwise have had access to (Consumer Financial Protection Bureau, 2019).

In addition, the payment service provider must be able to prove, according to § 31 BDSG, that the data is relevant for the algorithmic procedure of the probability calculation. When we assume that the internal credit scores obtained from alternative payment data could be used to accurately determine creditworthiness, data processing is permitted for this purpose.

3.3.2 Disclosure for External Credit Scoring

Currently external credit scoring companies still predominate in algorithmic credit scoring. Therefore, it is likely (and already practiced in the US) that alternative payment data should be passed on to them. Within the EU, this is unlikely to be permissible either with consent or under the general consideration of interests (Simits et al., Schantz, 2019, Art. 6 GDPR, 137). The transmission of extensive data sets on trouble-free payment transactions ("positive data") for the purpose of establishing a score on creditworthiness is associated with considerable risks for the persons concerned. It is especially burdening when used simultaneously for other purposes than credit (e. g. housing, in the US: job market, etc.). In addition, a transmission of all payment data would be surprising for the customers and they would not have to expect it (see the recital 47 to the GDPR). However, even taking a different opinion (v. Lewinski/Pohl, 2018), the only data allowed to be passed on would be information concerning credit or guarantees. A transfer of all payment data to external credit scoring companies would not be lawful (Krämer, 2020).

DOI https://doi.org/10.3790/vjh.89.4.73

3.3.3 *Customer Profiling for Marketing of Own Financial Services*

A customer profiling for the marketing of one's own financial services only serves to initiate but not to fulfil a specific contract, so the basis of Art. 6 I b) is not applicable here. The high requirements for voluntary, informed, and unambiguous consent in a precisely defined case make the justification of data processing on the basis of Art. 6 I a) particularly difficult in the case of general customer profiles. In contrast to this, the weighing of interests within the meaning of Art. 6 I f) is particularly relevant. If the interest of the data processing company is to advertise its financial services as accurately as possible, he or she exposes the customer only to minor risks for his rights. The evaluation of payment behavior for a bank's targeted advertising of other financial services is generally not surprising for the customer. The situation may be different if customer profiles are used in a targeted manner for the sale of financial services to vulnerable consumers, taking advantage of their weak economic situation. However, generally speaking, it can be assumed that data processing for this marketing purpose is permissible.

3.3.4 *Customer Profiling for the Marketing of Other Services, Products or External Advertising*

The situation is different if the alternative payment data is used for profiling to market other services or products, or if it is sold to third parties for advertising purposes. Such data processing would hardly be justifiable on the basis of consent under Art. 6 I a), if only because the purpose of the processing has to be specifically described. Furthermore, there would be considerable doubt as to whether consent is "freely given" because the performance of a contract "is conditional on consent to the processing of personal data that is not necessary for the performance of that contract" (Art. 7 IV).

In addition, the interest of the company to market other products or to use the profile for external advertising is, according to Art. 6 I f), disproportionate in relation to the original purposes of the data-processing and the rights of the customers. They are exposed to high risks under such forms of extensive profiling and would not reasonably have to consider the processing of their payment data for this purpose (see No. 47 recital GDPR). Thus, the creation of customer profiles for general marketing of services, products, or external advertising based on alternative payment data is not lawful.

As an interim result, we can summarize that the transfer of payment data to an external credit scoring company and the processing for the purpose of marketing products other than financial services is not allowed under GDPR rules. In contrast, the processing of alternative payment data for internal credit scoring systems and the marketing of own financial services is lawful. Nevertheless, also in these two cases there are further legal restrictions for the usage of the personal profiles:

3.4 Personal Profiling and the Protection Against Automated Individual Decision-making

Statistical probabilities can turn out to be individually wrong. There is a danger of erroneous, unfair, manipulative, and discriminatory conclusions. Therefore, no one should be a mere object of data processing that has consequences for the person without knowing the underlying data and evaluation criteria and not being able to influence it. Answering these problems at least partially, Art. 22

DOI https://doi.org/10.3790/vjh.89.4.73

grants a natural person the right "not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."

Additionally, the GDPR mentions in No. 71 of the recitals a "fair and transparent processing" with "appropriate mathematical or statistical procedures for the profiling" to minimize "the risk of errors" and to prevent the "discriminatory effects". Although the recitals are not legally binding, they are an important source for the interpretation of the GDPR in legal practice.

3.4.1 Decisions Based on Internal Credit Scoring

The automatic refusal of an online credit application without any human intervention is a paradigmatic case for the prohibited use of personal profiling under Art. 22 (see recital No. 71). Even automated decision-making about different interest rates or payment methods for different customers can "similarly significantly affect" the customer and be unlawful, even though this is controversial (Golland, 2020; Simitis et al., 2019, Scholz, Art. 22 GDPR, 36). However, even purely automated decisions are permissible under Art. 22 II a), if it is necessary for entering into, or performance of, a contract (Simitis et al., 2019, Scholz, Art. 22 GDPR, 43). Because (European) law provides for a mandatory credit assessment, it could be argued that automated lending based on a score might be lawful in general. However, the law does not require a creditworthiness check based on a score developed with alternative payment data. Therefore, it is very doubtful that the use of this score could be justified according to Art. 22 II a).

On the other hand, it is not an exclusively "automated decision," if an employee in a bank processes the credit application and has his own decision-making power. In this case, Art. 22 does not apply. The usage of the personal profile would then be allowed.

3.4.2 Customer Profiles for Financial Services

Targeted advertising could be seen as an automated decision-making, but normally it is not "similarly significantly affecting" the customer according to Art. 22 I and, therefore, is lawful. At best, frequent personalized advertising to vulnerable consumers, especially behavioral advertising in social networks, might be similarly affecting and therefore unlawful (Simitis et al., 2019, Scholz, Art. 22 GDPR, 37). The possible justification for this kind of burdening advertising could be explicit consent from the customer according to Art. 22 II c). However, this seems exceptionally unrealistic since the high information requirements also concerns the algorithm itself.

3.5 Data Protection Impact Assessment

The GDPR establishes rules for the "data protection impact assessment" which could be seen as binding guidelines for an effective data management and as an obligation to take organizational measures to ensure a high level of data protection. This assessment is necessary when a type of processing is likely to result in a high risk to individuals as "a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person" (Art. 35 III a)). This is the case for personal profiling. Therefore, the processing company must carry out a "data protection impact assessment," based on Art. 35. Whenever a data protection impact assessment under Article 35 indicates that the processing would

DOI https://doi.org/10.3790/vjh.89.4.73

result in such a high risk and that the data controlling company cannot mitigate this, it shall consult the supervisory authority prior to processing (Art. 36).

3.6 Result

We assess the legal situation for personal profiling with alternative payment data as following:

Unlawful is the transfer of payment data to an external credit scoring company as well as building customer profiles based on alternative payment data for the marketing of products or services other than financial services. Marketing these profiles for external advertising is forbidden under the GDPR as well.

Lawful is the processing of alternative payment data for internal credit scoring systems and the marketing of own financial services. Using an internal credit score to decide about a loan is allowed if an employee in the bank or credit company with own decision-making power is involved in the process. The use of customer profiles for marketing own financial services is also lawful in general, although advertising targeting vulnerable consumers might be seen different.

4 Conclusion

Our overview shows that both Fintechs and TechFins are increasingly entering the market for cashless payments and other financial services. Clearly, the companies hope that this will give them access to as much payment data as possible, which can be incorporated into personal profiles. This could have positive effects: the use of new technologies and detailed customer data promise greater convenience, lower transaction costs, better credit risk assessment, and greater financial inclusion, especially for those without conventional credit scores (Claessens et al., 2018).

However, we are also able to show that these developments in Big Data Scoring are problematic from the perspective of data protection law. On the basis of the European GDPR, personal profiling based on alternative payment data is most likely to be permissible only for banks within the framework of internal credit scorings and to market financial services. This could be an opportunity for the traditional banking sector. Indeed, commercial banks have started using Fintech credit innovations to increase efficiencies, either relying on Fintechs' credit scoring or have set up their own credit platforms introducing machine learning techniques (Claessens et al., 2018).

In general a replacement or even an extension of the classic credit assessment with big data scorings faces a number of challenges: insufficient transparency, potentially inaccurate input data, potential for biased and discriminating scorings, risks that these tools target vulnerable consumer, and consumers unaware of which factors count for the score, followed by a lack of empowerment to complain (Hurley and Adebayo, 2016). All in all, the triumphant progress of predictive algorithms raises substantial concerns for a "scored society" (Citron and Pasquale, 2014). The existing data protection law, at least initially, approaches these problems, even though it is not targeting predictive algorithms directly. Their regulation is complex and carries the risk of impeding technological and economic development in this area. However, it seems very questionable to trust forms of voluntary "Corporate Digital Responsibility" or self-regulation in this field. As there has been little reason for trust in the past, further legal regulations are to be expected and under discussion for scoring systems: strengthening the supervisory authorities, an improved right to information

DOI https://doi.org/10.3790/vjh.89.4.73

for the customer in accordance with Art. 15 GDPR concerning discrimination, a right of legal action for NGO's, a duty of companies to explain the score and the data management to the supervisory authority (Sachverständigenrat, 2018).

But regardless of the legal status, it must also be noted that the development of big data scoring is still in its infancy and it is still unclear how well it works. The danger of pure window dressing for investors in the growth-driven tech industry remains high. Wirecard's dreams of accurate predictive scorings with payment data and the collapse of the company in 2020 can be seen as a warning signal. In addition, it is not unlikely that Fintechs with big data scorings also cater to a higher share of riskier, marginal borrowers when they try to expand. In general, increasing competition in credit markets could lead to lower lending standards (Claessens et al., 2018).

The actual socio-economic situation is Janus-faced. On the one hand, some consumers who do not get reasonable priced credit or credit at all could see greater access to financial services (Consumer Financial Protection Bureau, 2019). On the other hand, however, the development could negatively affect especially vulnerable customers with higher costs and worse conditions leading to over-indebtedness. Regulating algorithms in a way that successfully balances business interests, technological development, personal rights and consumer protection is still far off. Until then, it will be the story that David Caplovitz describes in his famous book, "*The Poor Pay More*" (Caplovitz, 1963).[13] Taking into account the problems of consumers who do not have enough (or good enough) credit data for a sufficient credit score ("financial invisibles") on the one hand and the risks of personal profiling with alternative payment data on the other hand, we append the title *"With Data."*

5 References

— Amazon (2020): "Small Business Success in Challenging Times". 2020 Amazon SMB Impact Report.
— Bank for International Settlements (2019): Annual Economic Report.
— Berg, T., V. Burg, A. Gombovi, and M. Puri (2018): "On the Rise of Fintechs – Credit Scoring using Digital Footprints", *NBER Working Papers*, No. 24551.
— Björkegren, D., and D. Grissen (2019): "Behaviour Revealed in Mobile Phone Usage Predicts Credit Repayment", *The World Economic Review*, 0(0): pp. 1–17.
— Caplovitz, David (1963): "The Poor Pay More: Consumer Practices of Low-Income Families", New York: Free Press of Glencoe.
— Citron, K. D., and F. Pasquale (2014): "The Scored Society: Due Process for Automated Predictions", *Washington Law Review* 89, 2014, pp. 1–33.
— Claessens, S., J. Frost, G. Turner, and F. Zhu (2018): "Fintech Credit Markets around the World: Size, Drivers and Policy Issues", *BIS Quarterly Review*, September 2018, pp. 29–49.
— Clifford, D., I. Graef, and P. Valcke (2019): "Pre-formulated Declarations of Data Subject Consent – Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections", *German Law Journal*, pp. 679–721.

13 Silber (2017) gives a short explanation why that book stimulated the reconstruction of consumer financial protection law in America and around the world.

DOI https://doi.org/10.3790/vjh.89.4.73

— Consumer Financial Protection Bureau (2019): "Building a Bridge to Credit Visibility" – A Report on the CFPB's September 2018 Building a Bridge to Credit Visibility Symposium, 2019.
— De la Mano, M., and J. Padilla (2019): "Big Tech Banking", *Journal of Competition Law and Economics*, 14(4): pp. 494–526.
— European Commission (2016): "Consumer vulnerability across key markets in the European Union", written by: London Economics, VVA Consulting and Ipsos Mori consortium
— Financial Stability Board (2017): "Financial Stability Implications from FinTech: Regulatory and Supervisory Issues that merit Authorities' Attention", June.
— Frost, J., L. Gambacorta, Y. Huang, H. S. Shin, and P. Zbinden (2019): "BigTech and the Changing Structure of Financial Intermediation", *BIS Working Papers*, No. 779.
— Gausling, T. (2019): "Datenschutzrechtliche Bewertung KI-gestützter Kommunikations-Tools und Profiling-Maßnahmen", *Zeitschrift für Datenschutz*, pp. 335–341.
— Golland, A. (2020): "Herausforderungen von Algorithmen im Schnittbereich von Ethik, Ökonomie und Datenschutz", *Computer und Recht*, pp. 186–194.
— Hoeren, T., and S. Pinell (2018): "Das neue kalifornische Datenschutzrecht am Maßstab der DS-GVO", *MultiMedia und Recht*, pp. 711–716.
— Hurley, M., and J. Adebayo (2016): "Credit Scoring in the Era of Big Data". *The Yale Journal of Law and Technology*, 18(1): pp. 148–216.
— Jagtiani, J., and C. Lemieux (2019): "The Roles of Alternative Data and Machine Learning in FinTech Lending: Evidence from the LendingClub Consumer Platform", Federal Reserve Bank of Philadelphia, *Financial Management*, 48(4): pp. 1009–1029.
— King, M. R. (2019): "The Competitive Threat from TechFins and BigTech in Financial Services." Michael R. King and Richard Nesbitt (eds.), *The Technological Revolution in Financial Services*. Toronto: University of Toronto Press, Forthcoming.
— Krämer, W. (2020): "Die Rechtmäßigkeit der Nutzung von Scorewerten", *Neue Juristische Wochenschrift*, pp. 497–502.
— Lewinski, K. v., and D. Pohl (2018): "Auskunfteien nach der europäischen Datenschutzreform", *Zeitschrift für Datenschutz*, pp. 17–23.
— Lindner, R. (2019): "Zahlungsabwickler Wirecard – Was wir heute machen, bringt in zehn Jahren kein Geld mehr", 2019 October 11th, *Frankfurter Allgemeine Zeitung*.
— Sachverständigenrat für Verbraucherfragen (2018): "Verbrauchergerechtes Scoring", Gutachten des Sachverständigenrats für Verbraucherfragen.
— Silber, N. (2017): "Discovering that the Poor Pay More: Race Riots, Poverty, and the Rise of Consumer Law", *Fordham Urban Law Journal*, pp. 1319–1328.
— Simitis, S., G. Hornung, and I. Spiecker (eds.) (2019): "Datenschutzrecht – Kommentar zur DSGVO mit BDSG".
— Stulz, M. (2019): "FinTech, BigTech, and the Future of Banks", *Journal of Applied Corporate Finance*, 31(4): pp. 86–97.
— Tanda, A., and C.-M. Schena (2019): "FinTech, BigTech, and Banks – Digitalisation and its Impact on Banking Business Models.", Palgrave Macmillan Studies in Banking and Financial Institutions, Philip Molyneux (eds.).
— Uecker, P. (2019): "Die Einwilligung im Datenschutzrecht und ihre Alternativen", *Zeitschrift für Datenschutz*, pp. 248–251.
— Zetzsche, D., R. Buckley, D. Arner, and J. Barberis (2017): "From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance", *EBI Working Paper Series 2017*, No. 6.

DOI https://doi.org/10.3790/vjh.89.4.73