Gabudeanu, Larisa; Brici, Iulia; Mare, Codruța; Șcheau, Mircea Constantin

Article

Privacy intrusiveness in financial-banking fraud detection

Risks

Provided in Cooperation with:
MDPI – Multidisciplinary Digital Publishing Institute, Basel

Suggested Citation: Gabudeanu, Larisa; Brici, Iulia; Mare, Codruța; Șcheau, Mircea Constantin (2021) : Privacy intrusiveness in financial-banking fraud detection, Risks, ISSN 2227-9091, MDPI, Basel, Vol. 9, Iss. 6, pp. 1-22, https://doi.org/10.3390/risks9060104

risks

MDPI

Article

Privacy Intrusiveness in Financial-Banking Fraud Detection

Larisa Găbudeanu [1], Iulia Brici [2,*], Codruța Mare [3], Ioan Cosmin Mihai [4] and Mircea Constantin Șcheau [5,6]

[1] Faculty of Law, Babes-Bolyai University, 400591 Cluj-Napoca, Romania; larisa.gabudeanu@ubbcluj.ro
[2] Faculty of Economics and Business Administration, Babes-Bolyai University, 400591 Cluj-Napoca, Romania
[3] Faculty of Economics and Business Administration and the Interdisciplinary Centre for Data Science, Babes-Bolyai University, 400591 Cluj-Napoca, Romania; codruta.mare@econ.ubbcluj.ro
[4] Police Faculty, "Alexandru Ioan Cuza" Police Academy, 014031 Bucharest, Romania; cosmin.mihai@academiadepolitie.ro
[5] European Research Institute, Babes-Bolyai University, 400591 Cluj-Napoca, Romania; mircea.scheau@ubbcluj.ro
[6] Faculty of Automatics, Computer Science & Electronics, University of Craiova, 200585 Craiova, Romania
* Correspondence: iulia.brici@econ.ubbcluj.ro

Abstract: Specialty literature and solutions in the market have been focusing in the last decade on collecting and aggregating significant amounts of data about transactions (and user behavior) and on refining the algorithms used to identify fraud. At the same time, legislation in the European Union has been adopted in the same direction (e.g., PSD2) in order to impose obligations on stakeholders to identify fraud. However, on the one hand, the legislation provides a high-level description of this legal obligation, and on the other hand, the solutions in the market are diversifying in terms of data collected and, especially, attempts to aggregate data in order to generate more accurate results. This leads to an issue that has not been analyzed yet deeply in specialty literature or by legislators, respectively, the privacy concerns in case of profile building and aggregation of data for fraud identification purposes and responsibility of stakeholders in the identification of frauds in the context of their obligations under data protection legislation. This article comes as a building block in this direction of research, as it contains (i) an analysis of existing fraud detection methods and approaches, together with their impact from a data protection legislation perspective and (ii) an analysis of respondents' views toward privacy in case of fraud identification in transactions based on a questionnaire in this respect having 425 respondents. Consequently, this article assists in bridging the gap between data protection legislation and implementation of fraud detection obligations under the law, as it provides recommendations for compliance with the latter legal obligation while also complying with data protection aspects.

Keywords: fraud detection; privacy; data protection; privacy by design; security by design; machine learning; data analytics; cybercrime

Citation: Găbudeanu, Larisa, Iulia Brici, Codruța Mare, Ioan Cosmin Mihai, and Mircea Constantin Șcheau. 2021. Privacy Intrusiveness in Financial-Banking Fraud Detection. *Risks* 9: 104. https://doi.org/10.3390/risks9060104

Academic Editor: Tomas Kliestik

Received: 26 April 2021
Accepted: 21 May 2021
Published: 1 June 2021

1. Introduction

In the last two decades, as the technology used by the financial banking sector evolved, so did the fraud schemes used by fraudsters (European Payments Council 2019). The main two areas where fraud takes place involve internet banking web or mobile applications and ATM, POS, or online merchant payments using bank cards. Nilson Report (2020) has emphasized the increased targeting of merchants by organized financial crime organization for the perpetration of frauds, with IT development of the country and of the merchant having an impact on the merchant's ability to prevent frauds (Hawash and Lang 2020; Nathan et al. 2019). Around 56% of Europeans are concerned about becoming the victim of fraud (Eurobarometer 2015). In 2019, 26% of the EU population reported receiving fraudulent messages, including those related to e-banking credentials (Eurostat 2020). Different families of malware have caused various damages to the consumer, critical infrastructures, financial and banking institutions, becoming favorite targets (Șcheau et al.

2020). Fraud mechanisms in terms of both internet banking and card transactions have particularities that can help in fraud detection, such as location of payment initiation, details of payment recipient, timestamp of payment.

Researchers, such as Carminati et al. (2018), have analyzed in the past decade various manners in which such details can be used for fraud detection and prevention. Their conclusions have led to various approaches for fraud detection algorithms, with emphasis on machine learning ones (Yang et al. 2020), as aggregation of data and historical analysis of data can assist in finding fraud patterns (Politou et al. 2019).

These fraud patterns can help in the detection or prediction of potential fraudulent transactions. Detection algorithms match existing characteristics of frauds to the current transactions being analyzed, whereas predictive algorithms attempt to identify frauds having different characteristics than the historical frauds.

Further, the European Union legislators are focusing on this area, directly or indirectly, through specific legislation on fraud prevention mechanisms (as is the case for the Payment Services Directive 2) or more general data protection legislation (GDPR) or information security legislation (financial sector-specific regulatory legislation, NIS Directive) than include general security measures aimed at also preventing frauds. In addition, the NIS2 Directive proposal brings further clarity and emphasis on cooperation for incident handling and vulnerability disclosure. This can increase timely responses to threats or fraud patterns identified by one of the countries or one of the private entities. A further improvement in this respect represents addressing the supply chain risk and accountability.

Consequently, the types of fraud detection algorithms have increased, especially given regulatory requirements and the business need to limit frauds.

Researchers have generally focused on the accuracy of results and on increasing data collection and aggregation of data in order to achieve this goal (Jha et al. 2012), both for detective and predictive algorithms. This article builds on this and brings new angles in terms of privacy, such as those outlined in data protection legislation and by legal scholars (Kaminski and Malgieri 2020; González and de Hert 2019) to the existing or proposed fraud detection algorithms.

The purpose of the data processing is essential in determining its intrusiveness, as outlined by Cormack (2020). In the case of fraud detection, the purpose represents the protection of an individual's financial account, and, at first sight, it may be argued that this security purpose allows all types of data to be processed. However, the benefits of the fraud detection have to be analyzed by comparison to the impact on the individuals in terms of collection of a large amount of data about their behavior (including financial behavior) (Canillas et al. 2018), sharing such data with other entities (credit/payment institutions) or merchants and direct or indirect consequences on individuals (discrimination (Galhotra et al. 2017) and (Romei and Ruggieri 2014), bias, lack of provision of a service, inaccurate profiles being created).

This type of analysis in terms of amount/types of data collected, sharing of data, and actions to be taken by the credit/payment institutions by reference to their legal obligations to prevent fraud and their legal obligations to ensure privacy has been analyzed scarcely by researchers, with the majority of researches, as Perera et al. (2019) and Gruschka et al. (2018), focusing broadly on big data and data analytics implications on privacy, as detailed in the following sections.

There is a necessity to balance the need of the companies and customers to prevent fraud and the need of customers for privacy. Therefore, in this article, we start from the characteristics identified for fraud detection algorithms, analyze these from a data protection perspective, with emphasis on the intrusiveness of the data collection, processing, and transfer, including insights and guidelines from legal scholars such as Wachter and Brent (2019), and validate this analysis through a questionnaire.

This article analyzes the type of algorithms proposed by researchers in the last three years since the GDPR has entered into force in order to identify their characteristics in terms of privacy implications and impact from a privacy perspective.

The main focus is on the intrusiveness of data processing, with emphasis on the large amount of data collected (from a data minimization and fairness perspective, including aggregation of personal data from various individuals and entities, as also emphasized by Clifford and Jef 2018), a consequence of data processing on individuals and responsibility of stakeholders concerning the data processing. Identifying the main characteristics from a privacy perspective helps in the recommendation of privacy-preserving mechanisms to perform fraud detection. Enhancing the anti-fraud mechanisms in banks is reflected in increasing the banking soundness and, finally, in increasing the trust in bank systems and financial systems (Achim and Borlea 2020, p. 152).

Consequently, the novelty of this paper stems from the multi-angle approach it analyses in terms of fraud prevention requirements and privacy needs of individuals by taking into account guidelines issued by relevant authorities in this respect, legal provisions, but, also, the opinion of individuals on this topic, through a questionnaire.

Further, the paper outlines the privacy aspects to be taken into account when setting up a fraud detection algorithm and calibrating it to the needs of a specific credit/payments institution.

Section 2 of this article outlines a taxonomy of fraud detection algorithms based on their privacy implications while detailing the main regulatory requirements that have shaped these algorithms. The third section details the intrusiveness angles in terms of data collection, processing, transfer, and decision-making based on the data analysis and recommendations toward privacy-preserving algorithms (Section 3). The fourth section details the responsibility angles to have in mind as per existing legislation and the potential need for revision of these (Section 4). The following sections outline the responses to the questionnaire while keeping in mind the main objectives of the research and the views of the specialty literature on the respective points (Sections 5–7), with the conclusions of the research and future work described in Section 8.

2. Taxonomy of Fraud Detection Algorithms Categorized from a Privacy Perspective

In view of identifying the types of fraud detection algorithms used or proposed since the entrance into force of the GDPR, we have analyzed the research papers published in the last three years in five research databases (ACM, Science Direct, Emerald Full text, IEEE Transactions, Springer-Link Journals), based on specific keywords aimed at identifying the privacy aspects had in mind by such algorithms ("gdpr banking fraud detection", "privacy banking fraud detection", "aggregation banking fraud detection techniques", "banking fraud detection techniques").

This exercise and its results have provided information about the current market status on such fraud prevention solutions and insights into the algorithms, aggregation, and collection methods used, which have been used to create the questionnaire taking into account the current trends in fraud prevention and the potential privacy pain points these can generate.

Searching for the articles of other authors from the last three years (from 2018 to 2021), with the help of these key expressions, we could find out that the subject is one very frequently approached. It highlights the importance of deeper research on this issue. After entering the key phrases, we have summarized the returned results, adjusted by relevance to our topic, in Table 1, which can be found below:

Table 1. Articles on topic—number of results adjusted by key phrases and relevance.

Database/Key Expression	ACM Digital Library	Science Direct	Emerald Full Text	IEEE Transactions	Springer-Link Journals
GDPR banking fraud detection	552 results	113 results	21 results	72 results	167 results
Privacy banking fraud detection	591 results	256 results	193 results	554 results	891 results
Aggregation banking fraud detection techniques	776 results	90 results	44 results	181 results	288 results

Source: Author's processing.

From this vast literature, we tried to capture the most common ideas approached by authors and to identify the level of their research. Thus, we have selected some relevant bibliographic sources, and in the following, we will present a brief review of the literature. Starting with 2018, writings related to the privacy policy of personal data (GDPR policy) have started to appear. Stalla-Bourdillon et al. (2018) conducted an interdisciplinary analysis of GDPR in the context of electronic identification schemes. The study was conducted in the United Kingdom and provided an overview of how to interpret these situations. Following the study, the author proposes a legal basis that can help the good management of privacy by both parties involved. In addition, in connection with this topic, studies have begun to appear on the degree of intrusiveness involved in requesting personal data. In this respect, Horak et al. (2019) addressed the issues of GDPR's impact on cybersecurity software, respectively, the operation side of incident prevention and incident handling. It was a very conclusive example of intrusiveness. The risks of breaching confidentiality and the data minimization principle by requesting personal data were investigated, as well as the fact that the sharing of this information by the client could raise similar concerns. The Data Privacy Impact Assessment (DPIA) performed for this scenario revealed that the risks are not high, given the specific risk mitigation mechanisms in place. The methodology used helped in understanding the existing risks and making them easier to manage.

These privacy intrusiveness problems are also closely correlated to the prevention of credit card fraud. A significant number of authors have addressed the issue of fraud detection, and the algorithms used are continuously being improved in order to incorporate the new mechanisms and schemes used by fraudsters. There are a number of studies that analyze card fraud from various perspectives: Credit Card Fraud Detection using Machine Learning Algorithms (Dornadula and Geetha 2019), Credit Card Fraud Detection using Pipeling and Ensemble Learning (Bagga et al. 2020), and Credit Card Fraud Detection Using Artificial Neural Network (Asha and Suresh Kumar 2021). From year to year, the tools used for identifying fraudulent activities are becoming more and more complex and efficient for the identified fraud patterns, with machine learning algorithms being some of the best options in this respect, as technology advancements cross borders and become available in more countries (Mehmet et al. 2012).

Öğrek et al. (2019) tried to evaluate the methods of credit card fraud using a model with the Kaggle dataset. The methodology chosen was multi-layered artificial neural networks (MANN). To identify fraud, the author used features such as: cash in/out, debt, payment, amount of transaction, or local currency. The results of the study showed that the chosen method is effective. Then, Li et al. (2021), also using the Kaggle dataset, came up with the idea of a hybrid method on attenuating class imbalance with overlap based on an idea of division and conquest. The dynamic weighted entropy evaluation criterion was used for this purpose. The experiment proved to be even more successful than the previous ones.

Then, we have identified studies that target the behavior of individuals in conducting transactions as a method of detecting fraudulent card transactions. Carminati et al. (2018) tests Banksealer, a decision support system. It builds a model for every user and then

modeling it on this system. In the second stage, the robustness of the Banksealer system is verified against potential criminals. This approach was taken in Italy, but the results of the study said that it could be a useful dataset worldwide. Chen et al. (2019) also developed a method for detecting transactions based on individuals' behavior. The model used here is called hyper sphere. This study concludes that the characterization effect of human behavior is related to the frequency of their transactions. In addition, Wang and Wang (2019) evaluate user behavior from the perspective of the inter-request time interval. The author notices that there are bot-like behaviors in the online banking system. The results of the study showed that, after comparing two algorithms, Renyi entropy is superior to Shannon entropy in differentiating bot behavior from human behavior.

Other authors have developed various models created in order to identify fraudulent transactions. Chen et al. (2020) developed a hybrid scoring model for this purpose. This model can obtain an exact credit score and even decrease credit risk. Misra et al. (2020) proposed a two-step model for identifying fraudulent transactions. In the first stage, an autoencoder is used, which transforms the transaction attributes into a smaller characteristic vector. The vector is used as input to a classifier in the second stage. The experiment was performed on a comparative dataset. It was observed that the two-stage model is more efficient than systems designed with only one of the two stages. Olowookere et al. (2020) proposes a framework, which combines the meta-learning ensemble techniques and cost-sensitive learning for fraud detection. The results of the study indicated that the cost-sensitive ensemble framework produces cost-sensitive classifiers that are efficient in detecting fraud in databases of payments.

Other studies have been focused on more specific detections. Amarasinghe et al. (2018) reviewed selected machine learning and previous detection techniques that can be integrated into a fraudulent financial transaction detection system. It was concluded that in order to detect bank fraud more efficiently, it is important to know specific algorithms (e.g., Bayesian networks, fuzzy logic, etc.). Dong et al. (2018) approached a very interesting area of the subject of fraud, namely mobile ad frauds. The author proposed a hybrid approach called FraudDroid to detect fraud in applications on Android devices. After analyzing 12,000 suspicious applications, FraudDroid has identified 335 cases of fraud, which confirms that it is a useful way of detecting this type of crime. In addition, on an innovative note, Sudharsan et al. (2019) proposes the realization of the vote through ATM Machine by providing Biometric authentication or Face Recognition authentication. By comparison with Aadhar cards for security and privacy, the ATM voting application is easier to use.

As detailed above, we have analyzed the various types of fraud detection algorithms and have identified approaches they take that may have an impact from a data protection legislation perspective or that are subject to different requirements from this perspective. The analysis has led to the conclusion that technology is used more often in terms of fraud prevention in more and more countries, as also shown by scholars such as Achim et al. (2021). Further, this analysis has led to the identification of the following types of fraud detection algorithms from a data protection perspective. In this section, we outline these types of algorithms and detail the data protection impact and relevant legal requirements for their implementation.

The characteristics of these algorithms have been included in the questionnaire in order to view the opinion of the respondents on their intrusiveness. Below, we outline the main points to consider from a data protection perspective, with details about each point included in the following section.

Static rules have been used since the first versions of fraud detection algorithms. The rules are generally created manually by fraud prevention professionals based on characteristics of identified fraud or fraud trends presented by authorities or industry reports. The types of algorithms are generally not intrusive, provided the manual analysis conducted beforehand was not intrusive.

The use of transaction details generally should not be viewed as intrusive, as these are essential for identifying fraud and are the basis for manual analysis in the past as well (Rojas et al. 2018). However, certain types of analysis on transaction details may be considered intrusive, especially those referring to the private life of an individual, such as the exact merchant codes (including healthcare ones), analysis of daily patterns and shopping locations, reviewing the details of the transaction for specific keywords usually used in fraud transactions and automatically labeling them as frauds.

In case transactions time and/or location patterns are also included in the algorithm, intrusiveness may occur, as, depending on the actual algorithm and whether connection maps are created based on this information (Hacker and Petkovka 2017), there may be a risk of intrusiveness, as the connection creation may lead to a biased response of the algorithm in certain cases.

Recipient details may prove useful in certain situations, especially if these are mapped by reference to the accounts or names of confirmed fraudsters (or of their companies). However, these details may also be used to create a mapping system in which the recipients are monitored even if the credit/payment institution where they are holding their accounts is not sharing data with the monitoring entity or is not performing any monitoring itself. In such cases, there is a lack of predictability about the data processing, lack of application of the data minimization principle, potential discrimination (direct or indirect, as outlined by Hajian and Domingo-Ferrer 2013), and may be considered intrusive. Proper analysis of the consequences on the recipients and accuracy of data mechanisms should be implemented to comply with data protection legal requirements.

Including user behavior profile for financial services in the algorithm may lead to very intrusive analysis, as a specific situation for the general data analytics one detailed by Green and Viljoen (2020), as this type of data is not closely linked to the transaction from a data minimization and purpose limitation perspective (as further detailed in the below section) and, in certain cases, may lead to inaccurate inferred data. Further, there may be a lack of predictability by the individual about the use of such data for fraud detection rather than just for service provision. Therefore, for this type of algorithms, the data protection concerns outlined in this article should be analyzed in the design phase and re-assessed periodically based on the testing of the algorithm.

An algorithm also focusing on device patterns may be useful in terms of a wide variety of attacks, including the use of credentials after phishing attacks. Nevertheless, in view of preventing intrusive analysis, the amount of details about the devices should be limited to general ones such as operating system version, telephone model, internet banking installation date, browser version and not go into personal settings of the device, list of applications on the device or continuous location monitoring.

Previously non-transactional information held by the credit/payment institution about its clients is most probably to be considered intrusive, as this does not fulfill the data minimization, purpose limitation, and predictability requirements.

The above types of fraud prevention approaches (data collection, data aggregation, and data analysis) are relevant for the following sections that are analyzing the privacy implications of such algorithms and the opinion of individuals in this respect.

Generally, the processing basis for fraud detection, according to data protection legislation, is a legal obligation. Under banking sector legislation, especially the Payments Services Directive, there is an obligation to identify potential payment frauds for the executing or acquiring entity, including for TPPs (third party providers) that access the account (European Banking Authority EBA, EBA). Even if the legal provisions include general requirements and leave the actual implementation steps to the credit/payment institutions, this implementation also refers to the case-by-case analysis in terms of data protection legislation for the main concerns mentioned in this paper.

In order for an exemption from the SCA (Strong Customer Authentication) rules and provide user-friendly payment methods, both receiving and paying credit/payment institutions are incentivized to identify potential frauds, rate from a fraud perspective

the payer and the recipient of the payment. In practice, credit/payment institutions also analyze the fraud rate of the merchants in order to keep themselves with a low fraud rate.

In addition to this specific legislation related to the banking sector, as also expressly stated in the payments legislation, the data protection legislation has to be taken into account in order to provide protection of the personal data of the payer and recipient, as also mentioned for general data analysis by Wachter et al. (2020).

Further, the intrusiveness can be analyzed based on the actual direct or indirect legal or similar effects on the individual, which are broadly defined by the GDPR and legal doctrine (Article 29 Data Protection Working Party 2018) as any action taken concerning the individual (e.g., blocking of payments, client fraud rating changes), whether it produces direct legal effects or just indirect effects of a non-legal nature (e.g., not receiving advertising for a specific product). In this respect, as in other cases of automated decisions with impact on individuals (Kamiran et al. 2013), the automatic blocking of payments by the credit/payment institution may be intrusive, especially in case the data used for the fraud alert to be triggered are related to the private life of the individual or include an inaccurate profile or inferred data.

Further, the other option that can be implemented, respectively, allowing individuals to monitor their transactions based on the fraud detection algorithm may also lead to the risk of legitimate transactions being blocked or abusive use of the blocking function by the individual for payment he/she wishes to revert. Thus, the decentralization of fraud prevention may not prove efficient from an operational perspective.

3. Intrusiveness of the Data Processing

As outlined above, there are various approaches toward fraud detection, but most of them mention that the collection of relevant data and aggregation of such data improved the fraud detection levels, as detailed by Whitrow et al. (2009) and Jiang et al. (2018).

In terms of data protection legislation, the following aspects are relevant in this context, all closely tied to the intrusiveness concept: data minimization in terms of collection, processing, and transfer (including the possibility to use pseudonymized data), the impact of automated decision-making on individuals and the fairness principle (Clifford and Ausloos 2017). Further, from a data processing cycle perspective, these aspects have to be analyzed at the moment of collection of personal data, during the analysis process, and in terms of action taken after analysis is completed (Council of Europe 2019).

The dimensions and implications of data analytics and the use of machine learning have been analyzed by data protection authorities throughout the European Union, and the concerns they outline can be directly applied to the fraud detection scenario (European Parliamentary Research Service EPRS; AEPD 2020; ICO 2017).

3.1. Data Minimization

Data minimization entails the use of and access to only the personal data needed for a data processing activity. In the fraud detection context, this first means that the collection of data should include only the data actually used by the algorithm while excluding any intrusive types of personal data. Secondly, as detailed by Finck and Asia (2021), during the analysis phase, only the data for the specific analysis should be processed, and, in case of aggregation or transfer of data to other entities, this should occur only if required.

A relevant example in this respect is the ECJ (ECJ 2014) decision concerning metadata collected about individuals. In this decision, data collection was considered excessive by reference to the processing purpose, respectively, provision of a calling service. The service provider collected excessively metadata such as date, time, duration and type of communication, identification of user's device and location thereof, the call recipient's number and an IP address, as such information could provide a very detailed profile about an individual, which is not needed for the services provided. This is relevant for the fraud detection algorithms as well.

Out of the types of algorithms identified in the above section, the ones that include non-transactional information about the individual should perform case-by-case analysis in order to reflect the data minimization principle (Biega et al. 2020), as not all data about an individual can help with fraud prevention profiles. The algorithms that collect device data, data about recipients (generally from other transactions they were involved in), or service usage profile may require certain adjustments based on the actual types of data needed for the profile creation. The other algorithms that rely mostly on transaction data can be considered as complying with the data minimization principle in general, provided analysis of payment details is limited and not leading to inferred data about the individual.

Access to data, as mentioned by Goldsteen et al. (2020), is also important from a data minimization perspective. This entails that only natural persons and entities that require access to the data should access it or store it. This is relevant in terms of data aggregation. Whereas aggregation of data from multiple accounts held with the same credit/payment institution may seem reasonable for fraud detection purposes, the sharing of data with other credit/payment institutions may not seem reasonable and may also have an impact from a banking secrecy perspective, as it divulges financial data to other entities.

For this reason, one manner of approaching data collection and, especially aggregation of data, for fraud detection purposes is to use pseudonymized data (or even anonymized data, if possible, as detailed in certain researches, as Yu (2016)) to ensure limiting negative consequences on individuals.

The retention period is also closely related to data minimization. In this respect, it is essential to identify the period of time for which the data is needed (as per legal requirements or objective fraud detection needs). In the case of algorithms based on machine learning, this is particularly difficult to achieve, given the learning process of the algorithm and the creation of profiles based on previous input. In certain cases (Article 29 Data Protection Working Party 2018), if profiles for each user are created, this approach may lead to an inaccurate date and, consequently, such situations should be addressed from the outset of the algorithm development phase, with various approaches, including providing for learning only data of confirmed frauds and leaving the algorithm to build on these with analysis of abnormal payment behavior of the individual.

For the same reason, it is important to keep the purpose of data processing to fraud detection without using the data for other purposes. This is also closely linked to the purpose limitation principle as detailed by scholars such as Forgó et al. (2017). For instance, a profile created for fraud prevention should not be used to refuse to offer financial banking services to an individual, as the individual was categorized as a potential fraudster, either as the individual making or receiving fraud payments.

3.2. Automated Decision-Making

In implementing an effective fraud detection mechanism, this should be in real-time (when the payment is being made) and should have an adequate response to the potential fraud. Responses may include a notification to the payer requesting the payer to accept the payment or blocking the payment.

In the latter two cases, an automated decision is being made, as this is defined under the data protection legislation, given that the decision has a legal effect on the individual by temporarily or permanently blocking his/her payment.

According to data protection legislation and the guidelines issued by Article 29 Data Protection Working Party (2018), there are certain cases in which an automated decision can be taken, such as legal obligation or performance of the agreement. In this case, even if there is a general legal obligation to prevent fraud, as the actual implementation details are established by each entity, it may be argued in certain cases that more processing is performed than expressly required by law. In such cases, blocking of payments may be considered as lacking a proper processing basis. For this reason, an analysis on a case-by-case basis (Kaltheuner and Bietti 2018) should be performed in order to ensure proper implementation of legal requirements on automated decision-making, including steps

taken for data relevance for the legal fraud prevention requirement and accuracy of the fraud detection algorithm.

Further, in case of profiles created about recipients of payments, automated decisions have to be generally taken in case of a legal obligation, with proper analysis being conducted for the specific situation in other scenarios than specific legal requirements in order to address the data protection concerns mentioned in this paper, with emphasis on the type of effects on the individual. Otherwise, such decisions cannot be taken based on the profile obtained through analysis of payments they received, as there is no processing basis in this respect, and the profile created may be inaccurate, given the limited amount of information gathered about them.

3.3. Fairness of Data Processing

The fairness of a data processing activity is considered, as detailed by Malgieri (2020) and Abiteboul and Stoyanovich (2019), to be closely linked to the following aspects, in addition to the data minimization principle mentioned above: discrimination of individuals, bias/harms brought to individuals, lack of predictability of data processing performed.

The discrimination of individuals.

Discrimination or bias toward an individual are concepts that are not defined by the legislation, case law, and specialty literature but rather referred to in general terms, as is the case also in guidance issued by authorities (Datatilsynet 2018). Generally, any action taken that leads to unequal treatment (e.g., based on inferred data, certain types of transactions are blocked inaccurately) that are in similar circumstances can be viewed as discrimination.

Thus, as also outlined by Dwork et al. (2012) the discrimination is relevant mostly in cases where actions are taken concerning the individuals, groups of individuals, or transactions (or in case of ranking creation) and can increase when inferred data is used, depending on the accuracy of the algorithm.

Bias and harms brought to individuals.

Types of harms that can be brought to an individual are not expressly mentioned by legislation but have been debated in the legal doctrine. However, given the cultural differences, mostly in continental and common law legal systems, there is no common approach in this respect. In Europe, the French data protection authority (CNIL 2018) has issued a taxonomy of privacy harms. Generally, as outlined in (Citron et al. 2021) and (Reidenberg et al. 2014), harms include any damage, loss, or distress to individuals brought by the data processing. In the case of fraud detection algorithms, the harms mainly refer to blocking of payments and, if the case, decrease in fraud ranking of the individual. This is closely tied to the automated decisions or use of the individual's profile created.

Lack of predictability of data processing performed.

Predictability entails that an individual is aware of the data collection and data processing occurring with respect to his/her personal data and is also essential in the automated decision-making context, as outlined by Malgieri (2018). In case of fraud detection, the types of data collected should be outlined to the individual, including any updating thereof. Further, as provided by law and emphasized by scholars such as Edwards and Veale (2017), a brief detailing of the algorithm should also be brought to the attention of the individual. This, as also detailed in (Abiteboul and Stoyanovich 2019) ensures, correlated with the other aspects in this section, that the data processing activity is not intrusive on the private life of the individual.

The individual who is not a client of the credit/payment institution cannot be notified directly of the data processing activity properly and, thus, the predictability principle cannot be fully addressed in this respect and may lead to intrusive processing in case of profile creation for such individuals. Nevertheless, given the purpose of the processing, an exemption from the transparency principle may be applied after analysis on a case-by-case analysis.

Aside from the above, the use of fraud detection algorithms leads to issues concerning the access right, the right to be forgotten (analyzed preliminary by Ginart et al. 2019), and data rectification, especially in cases where the initial data aggregated or the inferred data

is not accurate and in cases where the machine learning algorithm has used such inaccurate information in its supervised or unsupervised learning process.

4. Responsibility for Fraud Detection Algorithms

Responsibility is covered in the legislation on fraud detection and under the data protection legislation (Vedder and Naudts 2017). For the former, the algorithm has to include reasonable data analysis to prevent frauds, and, for the latter, all data protection requirements, including those referred to in the previous section on intrusiveness, have to be fulfilled and properly documented (Butterworth 2018) and (Castets-Renard 2019). These are applicable for any stakeholder involved in the payment process, as per the liability set out in the legislation. In case of exemptions from the SCA being applied, the entity requesting the exemption becomes liable for any fraud. As a consequence, the merchants have also implemented fraud detection mechanisms in order to rely on these when requesting such exemptions.

Even if the credit/payment institution has the responsibility to identify frauds and to prevent intrusive processing of personal data, certain users may wish to be able to configure the profiles and to decide the blocking of certain transactions (Wachter et al. 2017). Whereas for the transaction blocking, this may be implemented while complying with legal requirements, for the types of data analyzed in the fraud detection algorithm, it may be difficult from an operational perspective to have different types of data for different individuals (Floridi et al. 2017). Further, for non-intrusive types of personal data, it may be considered reasonable to have these in the fraud detection algorithm without an opt-out option for individuals. For the intrusive ones, consent of the individual may be used to include them in the fraud detection algorithm as per the guidance of European Data Protection Board (EDPB).

Even in cases where the individual can choose certain types of data to be processed or to take actions about potential frauds identified by the fraud detection algorithm, to a certain extent, as outlined by Hoffmann and Birnbrich (2012) on the view of customers on fraud prevention techniques, the obligation to prevent fraud remains with the credit/payment institution, which has to ensure that payments that are clear frauds are not made (Malgieri and Comandé 2017). In case of actions taken by the individual, such as falling victim to a phishing attack, it may be argued under the provisions of PSD2 (AMLC 2017) and related banking regulatory legislation that the credit/payments institution is not liable for fraud prevention. However, in order to protect their customers, generally, a fraud detection algorithm attempts to address this type of attack that relies on the actions of the individuals.

When third parties are used to provide the fraud detection algorithm or to perform the analysis, generally, the responsibility remains with the credit/payment institution (as per article 28 of the GDPR on data processors), with the contractual liability of the third party toward the credit/payment institution to be considered as well.

5. Objectives

Based on the characteristics identified about fraud detection algorithms from a privacy perspective, we have developed a questionnaire to analyze the views of the consumers on the privacy concerns in terms of data processing in fraud detection. The three objectives of the questionnaire are:

Objective 1: Monitoring techniques on transactions for fraud prevention are considered by individuals as being intrusive on their privacy, especially when data is aggregated from multiple sources.

Objective 2: Individuals wish to be in control of their data and transactions and not have their transactions blocked automatically based on artificial intelligence, but rather have the opportunity to confirm or reject the potential fraud.

Objective 3: Individuals consider credit/payment institutions as responsible for identifying potential frauds on their transactions.

6. Data and Methodology

For the present research, we have applied a questionnaire on the idea of fraud detection and monitoring issues for fraud prevention. The questionnaire was distributed on the internet, via e-mail addresses and social platforms (such as Facebook, LinkedIn, etc.), using a random sampling procedure, in order to avoid as much sampling bias as possible. The survey was distributed both to regular people and to specialists in the field from Romania. A response rate of 82% was obtained. After all quality checking procedures such as deleting repeated attempts, missing answers, etc., a valid sample of 425 respondents was left in the analysis. The survey was conducted in the months of March and April 2021.

A detailed description of the variables used is provided in Table 2. For demographic aspects, we asked for the professional area, age group, sex, and education in the form of the latest educational level completed.

Table 2. Variables' description.

Set	Variable	Description
Data aggregation and use of AI to prevent fraud: case of bank/payment institution	Usefulness—payment institution	Useful to identify frauds
	Excessive collection—payment institution	Intrusive on my privacy, as it entails collecting too much data I consider to be private information
	Automated decisions—payment institution	Intrusive on my privacy, as it may lead to blocking transactions that I actually want to make
	Lack of predictability—payment institution	Intrusive on my privacy, as the algorithm used is not known to me and, thus, I question whether it is used fairly and in good faith
Data aggregation and use of AI to prevent fraud: case of merchant	Usefulness—merchant	Useful to identify frauds
	Excessive collection—merchant	Intrusive on my privacy, as it entails collecting too much data
	Automated decisions—merchant	Intrusive on my privacy, as it may lead to blocking transactions that I actually want to make
	Lack of predictability—merchant	Intrusive on my privacy, as the algorithm used is not known to me and, thus, I question whether it is used fairly and in good faith
Intrusive analysis on your data/privacy case of bank/payment institution	Transaction data—payment institution	Analysis of details about transactions (recipients, bank account of recipient etc.)
	Devices details—payment institution	Analysis of details about devices (used to perform payments e.g., internet banking, authentication device details, operating system)
	IP address—payment institution	Analysis of IP addresses of the devices used for performing payments
	Transaction behavior—payment institution	Analysis of the behavior models performed through artificial intelligence based on previous transactions, including recipients, frequency, value
	Payment details—payment institution	Analysis of the payment details field and details about ATM/POS/Internet banking/payment order
	Recipient location—payment institution	Analysis of recipient location (e.g., country)
	Previous fraud details—payment institution	Analysis of details about previous frauds
	Recipient's bank—payment institution	Analysis of details about the recipient's bank
	Other data held—payment institution	Analysis of details already held by the bank about you

Table 2. *Cont.*

Set	Variable	Description
Intrusive analysis on your data/privacy case of merchant	Previous payments—merchant	Analysis of the previous payment profile for that merchant
	Previous payments aggregation—merchants	Analysis of your previous payment profile for other merchants
	IP address-merchant	Analysis of the IP address correlated with the card issuance country/entity
	Fraudsters' device details—merchant	Analysis through comparing of your device details to known fraudsters
	Fraudsters' purchasing profile—merchant	Analysis through comparing your purchasing profile to that of fraudsters
Do when identifying a potential fraud	IPF_block	Identify the potential fraud in real-time and block the transaction until I confirm it by phone, in my internet banking, or other agreed method
	IPF_notify_noblock	Identify the potential fraud in real-time and notify me by e-mail or in my internet banking application, without blocking the payment
	IPF_call_noblock	Identify the potential fraud in real-time and call me without blocking the payment
	IPF_endday_noblock	Identify the potential fraud at the end of the day and notify me without blocking the payment
Who do you consider responsible for preventing fraud transactions	Own_bank	The bank where you have your bank account
	Other_bank	The bank to which your money is transferred
	Merchant	The merchant (online store, store that has one or more POS installed) that receives payment from your bank card

Source: Author's processing.

Approximately 65% of the sample is made up of women. Most of the respondents have a bachelor's degree (42.4%), while the second most frequent group has a master's degree (36.2%). As only less than 7% are respondents with a high school degree, we can conclude that the educational level of the sample is high. In respect to the professional area, the majority consists of economists, followed by other professions, as emphasized in Figure 1.

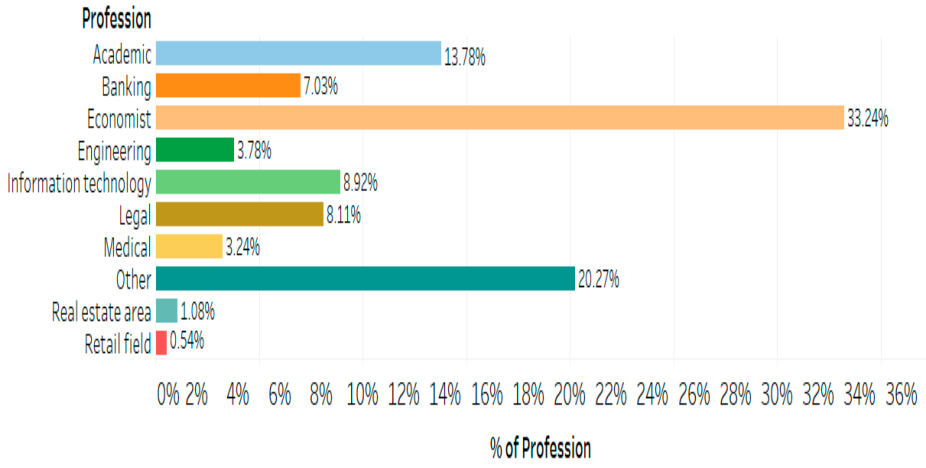

Figure 1. Distribution of the sample based on professional field. Source: Authors' processing in Tableau.

In respect to age, approximately 24% of the respondents are between 18 and 23 years of age. A similar share belongs to the 31–40 group age. Respondents ranging from 41 to

50 years of age represent 22% of the sample, followed by the 24–30 group (17.3%). Older people belong to the sample at a lower extent (the rest of the sample—approximately 13%). However, we do not consider this a sample significance problem, as older people tend to be more conservatory, so the probability for them to use the internet environment is smaller.

Data were analyzed using frequencies and charts in the descriptive evaluation stage. Multiple response sets were constructed in order to assess the research objectives. They allow for a ranking of the choices as they provide the percentages both in respect to cases and to answers. The significance of the results was assessed using Friedman and Kendall's W test for related samples, along with the Student t and the Mann–Whitney tests for paired variables.

Analyses were conducted in SPSS 24, while visualization procedures were conducted in SPSS 24 and Tableau.

7. Results

The first objective of our research is related to intrusiveness in the privacy of the individuals. Results show that respondents have more or less a neutral attitude toward this—the average score is around the middle of the Likert scale, 3 (Figure 2), while these values are also the most frequent (shares between 30% and 40%).

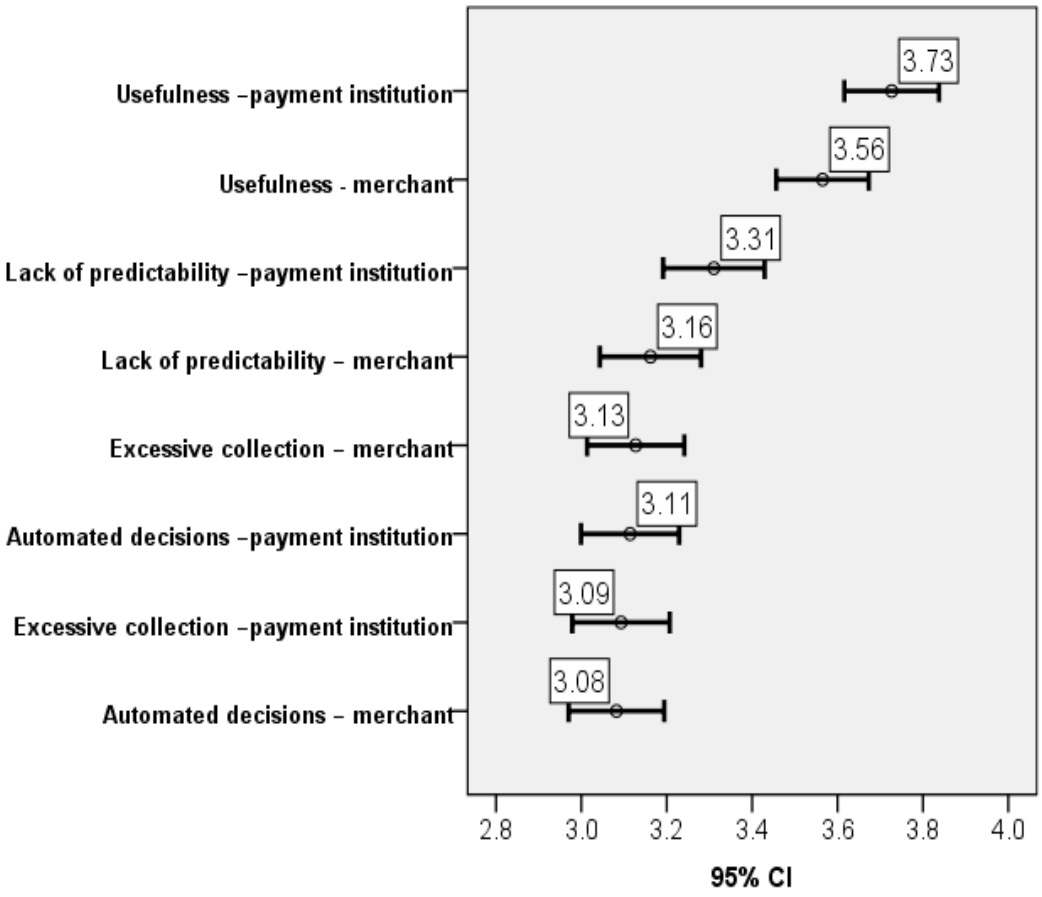

Figure 2. Data aggregation and use of AI. Source: Authors' processing in SPSS 24.

While, generally, there is a tendency to find useful the use of AI on aggregated data by credit/payment institutions (3.73), it is considered slightly less useful for this to be performed by merchants (3.56) (p-value = 0.000). In terms of lack of implementation of the data minimization principle and excessive automated decision-making by blocking payments, respondents were of the view that there is some risk in this respect (around 3.10) for bank and merchant fraud prevention solutions alike.

The results show that the respondents view both credit/payment institutions as having reasons to protect their financial accounts against fraud. This is slightly different than currently envisaged in the legislation, with the emphasis being put on the credit/payment institutions. Further, the results emphasize that the respondents consider the usefulness of AI analysis of aggregated data (3.73 and 3.56) greater than their perception of such data collection and data processing being intrusive (between 3.08 and 3.31) (results highly significant, with a global *p*-value for related samples of 0.000). Therefore, even in certain situations not provided by law, respondents are inclined to allow to a certain degree the aggregation of their data and the AI analysis thereof in exchange for the protection against potential frauds. Nevertheless, given the very close results, it is worth exploring more in depth the limitations the respondents impose on their data collection, processing, and aggregation in exchange for fraud protection and, thus, the tipping point in the scale between privacy and protection against frauds. When conducting comparison analysis on pairs of the variables in the sample, we have depicted that the scores for both merchants and credit/payment institutions are similar in respect to privacy (collection of too much data versus blocking transactions, with *p*-values ranging from 0.290 to 0.742). In all other cases, the importance of the credit/payment institution is perceived as being significantly higher (p-values < 0.05).

When going deeper into analysis and considering different aspects that could be used to obtain information and prevent frauds, the scores become even lower, but still with significant differences in the distributions between the aspects considered (*p*-value for Friedman and Kendall's W tests 0.000). This implies that respondents consider that all the information related to those aspects is not intrusive in their personal life. For this group of variables, the share of the middle score ranges between 20% and 30%. In the case of analysis of details about previous frauds and analysis of details about the recipient's bank, almost 30% of the responses declared that these do not intrude at all in their own lives.

In terms of types of data analysis to be performed and its intrusiveness, the general attitude of respondents is of partial agreement with the intrusiveness of data processing. This has been the result for all types of data collection, data comparison, and data processing presented in the questionnaire, regardless of the manner in which such data processing was treated in the legal doctrine, either less or more intrusive by reference to the fraud protection purpose.

Nevertheless, there are certain small differences in opinion that are worth mentioning and further exploring. For instance, whereas respondents found intrusive with a median of 3.25 the data processing of their payments profiles by the credit/payment institutions, for the same type of data processing performed by merchants, the median was just 3.02. The reasoning for this slight difference in opinion between the two data controllers can be further explored, as it may relate to various reasons. One could be the fact that credit/payment institutions have a very detailed profile of the individual, whereas merchants have a narrow view of the private life of individuals. Another could be that individuals consider merchants to be able more easily to identify purchases out of character for the individual, given they also possess the browsing history of the individual.

Details about previous frauds and about the recipient's bank have been considered less intrusive by respondents (p-value = 0.319 for the bank and p-value = 0.964 for the merchant, but p-value < 0.05 in respect to other options stated in the questionnaire). This is in line with existing legislation and interpretation of the intrusiveness of data processing, as these aspects do not take into account the personality or private life of the individual. However, it is interesting that the score for these items was not lower, toward partial or full disagreement that these constitute intrusive analysis.

Consequently, the collection and processing of certain data concerning the individual are generally viewed as slightly intrusive, irrespective of the amount or types of data collected. It is interesting that this was the response to all of the types of data, including data about the payments of the individual, but also details already held by credit/payment institutions about the individual in other circumstances than the performance of payments.

Generally, such type of data collection and processing as the latter would be considered in legal doctrine as intrusive, given the data minimization and purpose limitation principles.

In respect to objective 1 of the study, we conclude that there is a neutral attitude of individuals in terms of the degree of intrusiveness in their personal life, with some of the aspects being considered less intrusive (Figure 3).

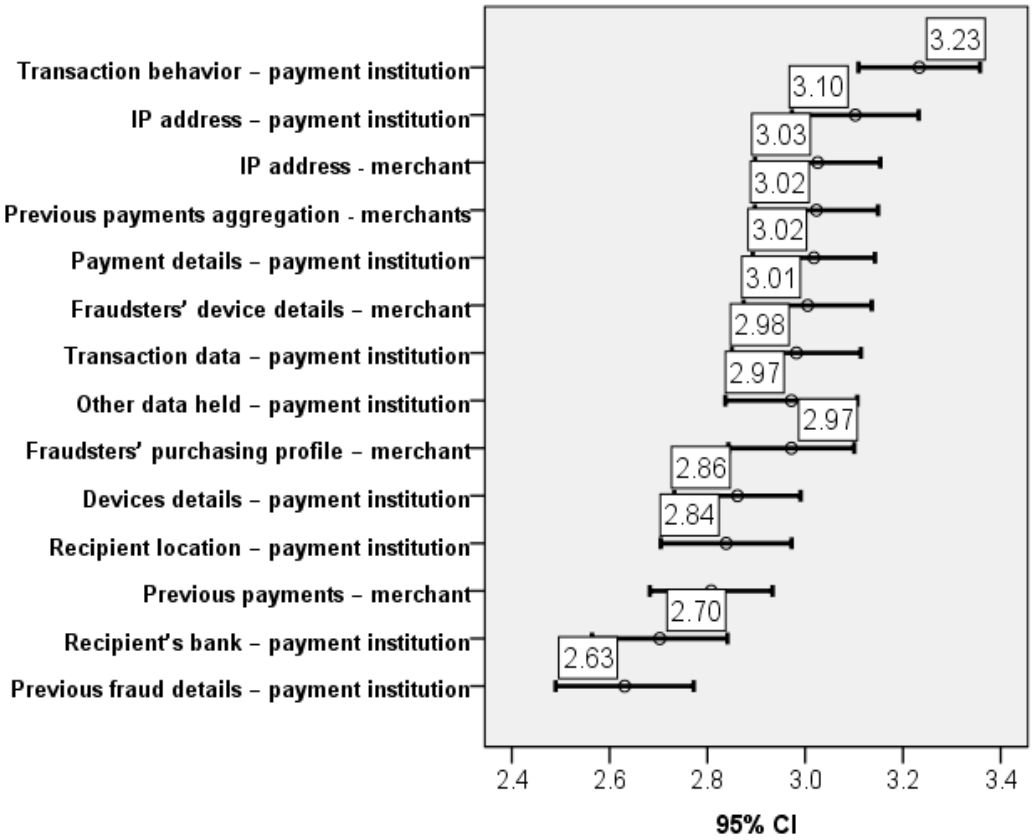

Figure 3. Intrusiveness of data collection and data processing for fraud prevention, *Source:* Authors' processing in SPSS.

The second aspect related to objective no 2 is the level of control of the clients/individuals when the AI applications detect potential frauds. Figure 4 clearly emphasizes that the assumption we made under this research objective is rejected, as respondents strongly agree with blocking a transaction and then asking for their confirmation in respect to the situation of more control on their part. The blocking option received a high average score of 4.52, with almost 70% of the answers being with the highest score—5. In opposition, almost 70% of the respondents strongly disagree with the most relaxed option that was available in the questionnaire-Identify the potential fraud at the end of the day and notify me, without blocking the payment. This means that respondents in the sample prefer to be safe than sorry. The other two options were also graded 1 by most of the individuals, but this time with a lower share of almost 40%.

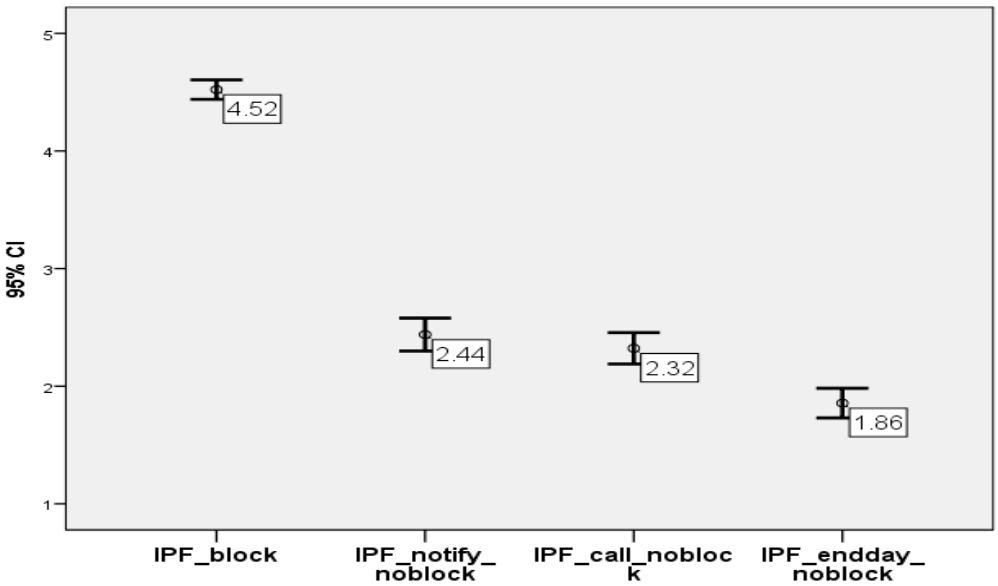

Figure 4. Level of control of individuals and possible reactions to fraud detection. *Source:* Authors' processing in SPSS 24.

This result is in line with the tendency of the legislator, including under PSD2, to have real-time analysis of the transactions for fraud prevention and to have them confirmed by the payer. Further, it is also in line with the data protection requirements in case of automated decisions that have a legal or similar effect on the individual, which mentions that such type of decisions, in the absence of express legislation on such actions to be taken, have to take into account the consent of the individual in order to proceed with the automated decision. The other options with which the respondent disagreed to a large extent did not provide them the opportunity to consent to the automated decision having an impact on them.

Our third objective deals with the responsibility of fraud detection. We asked the respondents to rank, on the same 1 to 5 Likert scale, who is responsible for identifying and preventing fraud: own bank, the other bank, or the merchant where the card payment is made. All three options received the highest score (5) from most of the respondents along with similar distributions (see Figure 5). Actually, in all three cases, only approximately 25% of the sample provided scores lower than 3. However, when constructing and analyzing the multiple response sets, it was clearly emphasized that most of the respondents consider their own bank as being responsible for fraud detection and prevention (Table 3). Of the respondents, 86.5% were assigned a grade of 5 (most important) for the personal bank. In comparison, approximately half of the grades represented 5 for the other two options: the other bank and the merchant. The significant importance of the own bank in identifying and preventing frauds is also shown by the fact that this option was given 45% of the scores of 5. Testing procedures applied have also validated the existence of significant differences in the perceptions related to research objective 3. The Friedman and Kendall tests for related samples have both returned a p-value of 0.000. Additionally, when constructing pairs of the variables in the multiple response set, the p-values obtained were of the same value (0.000), with the exception of one situation, with a p-value = 0.029, also accepting significant differences in the perceptions. Consequently, all analysis procedures that were applied confirm that the own bank is significantly important in identifying and preventing fraud with respect to the other options.

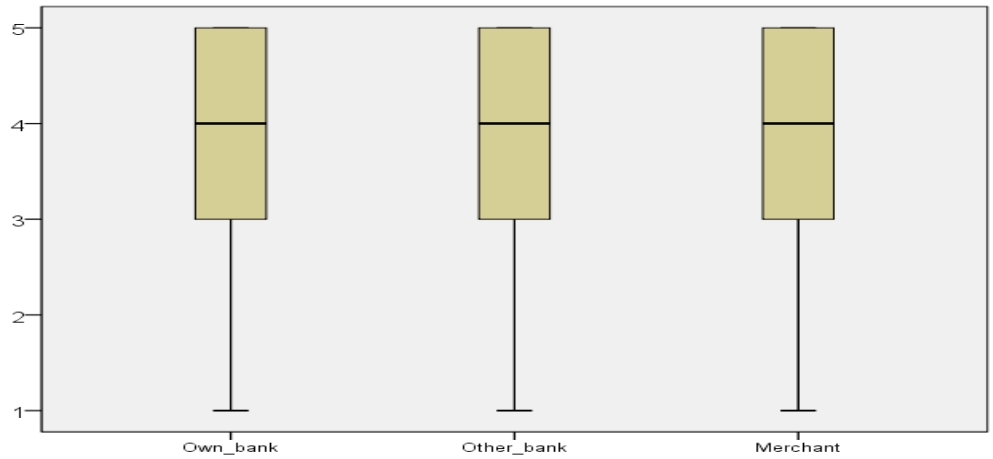

Figure 5. Distribution of the sample based on responsibility for fraud detection—boxplot. *Source:* Authors' processing in SPSS 24.

Table 3. Who is responsible for fraud detection—analysis of the multiple response set for the 5 score.

	Responses		Percent of Cases
	N	Percent	
The bank where you have your bank account	192	45.2%	86.5%
The bank to which your money is transferred	119	28.0%	53.6%
The merchant (online store, store that has one or more POS installed) that receives payment from your bank card	114	26.8%	51.4%
Total	425	100.0%	191.4%

Source: Authors' processing in SPSS 24.

It is interesting to see that the respondents have also focused their attention on the merchants to a greater extent than we expected. Whereas there is legislation in place in terms of credit/payment institutions making or receiving payments, the legislator has only recently started to focus its attention on the role of the merchant in this ecosystem with the adoption of PSD2. It remains to be seen how the merchant can fit into this fraud prevention mechanism and whether the sharing of data between the credit/payment institutions and merchants can help better analyze the data for fraud prevention purposes.

In conclusion, objective 3 of the study is validated.

8. Conclusions

In this article, we have analyzed the main data protection concerns in the implementation of fraud prevention solutions. On the one hand, the legislation on fraud prevention is becoming more and more emphasized on real-time detection of fraud by stakeholders involved and, on the other hand, the technical solutions for fraud prevention are becoming more and more complex, using machine learning and collecting (and aggregating) a vast amount of data.

This gives rise to issues on the intrusiveness of the data collection and processing, which has been limitedly analyzed by the scholars. Given that the legal provisions in terms of fraud prevention are rather general and broad, their implementation and correlation are left to the stakeholders, such as credit/payment institutions. This article bridges this gap by analyzing the key areas of concern from a data protection perspective, based on the manner in which the fraud prevention algorithms are constructed and on the views of the respondents to a survey on this specific topic.

In order to identify the main data protection concerns, we identified the types of fraud prevention algorithms currently described in relevant specialty literature. These start with

static rules, the use of transaction details, device patterns, and go on to more complex collection and analysis that entails analysis of transaction time and/or location patterns, of recipient details, of user behavior profile and of data held about the individual, which is non-transactional data.

Based on these structuring concepts and types of data collected and processed, we created a set of questions to address three main angles. These questions make up a questionnaire that we launched both nationally and internationally. We have received 425 valid answers.

In elaborating this questionnaire, we considered the establishment of three basic objectives. The first objective focuses on the identification of the threshold of data collection and data processing found to be intrusive, including in terms of data aggregation.

Generally, intrusiveness includes the following areas of concern for data collection and data processing, including in the context of fraud prevention: data minimization upon collection and processing, proper measures for automated decision-making having an effect on the individual and fairness of the data processing, including lack of discrimination, bias, harms, and existence of data processing predictability for the individual.

For various forms and types of data collection and data processing, as generally used in fraud prevention algorithms, the general result of the questionnaire has been of slight intrusiveness thereof. Thus, even in cases where the legal doctrine describes data processing as intrusive even by reference to the fraud prevention purpose, the respondents mentioned it is only slightly intrusive even when the algorithm used is based on machine learning and includes analysis of aggregate data from multiple sources. Given the rather neutral results, this study can be considered a ramp to launch a much deeper study in order to identify the reasons for which respondents did not find these solutions as not intrusive at all or very intrusive. These can be rather different and may include matters such as: financial security purpose of the processing, data controllers involved in the processing (credit/payments institutions whose activity is highly regulated), lack of knowledge about the manner in which the data is being processed by the algorithms due to lack of transparency thereof, etc. Of course, a wider audience of respondents would be beneficial to the study, and why not, the niche formulation of the questions depending on their field of activity or the frequency of use of financial banking services.

Further, it is worth exploring the role of merchants in fraud prevention, as their role has been generally considered by respondents as closely linked to the role of the credit/payments institutions. Future research can analyze the manner in which the merchants and credit/payment institutions can share data for fraud prevention purposes while also complying with data protection requirements.

The second objective aims at identifying the preferences of the respondents in terms of the default approach toward potential frauds and the level of control they wish to have on their payments. The respondents have provided input, which is in line with the current legislation trends, respectively, automatic blocking of transactions, with the payer being able to mark the transaction as not being a fraud when he/she is contacted by the credit/payments institution to confirm the transaction. A suggestion to implement for this purpose can be the popularization of internet banking facilities. Probably many of the respondents do not face potential fraudulent activities because they do not use banking applications, e-mail notifications, text notifications on the phone number, or other options that the bank offers to them.

The third objective relates to the responsibility in terms of fraud prevention in terms of legislation and views of the individuals. It is interesting to see that, aside from the credit/payment institutions being considered primarily responsible for fraud identification and mitigation, with the payer credit/payment institution being considered more responsible in this context, the respondents also view the merchants as having a role in this respect. In future research, this can be further analyzed in order to identify the need for cooperation and information sharing between payer and recipient credit/payment institution and also merchants, while, at the same time, having in mind the principles of the data protection

legislation. The bank cannot be blamed 100% for these unpleasant situations. There are cases in which the institution does its duty, but the client does not pay attention to warnings about risky operations. In future studies, it would be ideal for identifying which category of clients do not comply with their obligations and what are the reasons for not doing so. An example of a category that can be easily predicted is the elderly because they are also the most exposed and vulnerable when it comes to any type of scams.

Overall, the use of artificial intelligence and data aggregation is viewed in a neutral manner by respondents. This encourages the need for further awareness about the manner in which the algorithms work and the need for further clarity on the role of each stakeholder in fraud prevention, together with cooperation mechanisms among stakeholders for more efficient fraud prevention. Artificial intelligence is generally presented with all its disadvantages in the foreground, but the awareness of the benefits of using it should prevail. In this sense, a financial education campaign from the state leadership, in partnership with financial institutions and academic institutions, would be welcomed. In any important initiative, a theoretical, practical, and financing contribution is needed to form a whole.

Author Contributions: Conceptualization, L.G. and M.C.Ș.; Methodology, L.G., C.M. and M.C.Ș.; Formal analysis, L.G., I.B. and C.M.; Investigation, I.C.M. and M.C.Ș.; Resources, L.G. and I.B.; Data curation and analysis, C.M.; Writing—original draft preparation, L.G., I.B. and M.C.Ș.; Writing—review and editing, L.G., I.B., C.M., I.C.M. and M.C.Ș.; Visualization, I.C.M., C.M. and M.C.Ș.; Supervision, M.C.Ș.; Project administration, M.C.Ș.; Funding acquisition, M.C.Ș. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by a grant from the Romanian Ministry of Education and Research, CNCS-UEFISCDI, project number PN-III-P4-ID-PCE-2020-2174, within PNCDI III. This paper is part of the project COST CA19130 FinAI-Fintech and Artificial Intelligence in Finance-Toward a Transparent Financial Industry.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data used in this analysis is not public but available upon request.

Conflicts of Interest: The authors declare no conflict of interest.

References

Abiteboul, Serge, and Julia Stoyanovich. 2019. Transparency, Fairness, Data Protection, Neutrality: Data Management Challenges in the Face of New Regulation. *Journal Data and Information Quality* 11: 3. [CrossRef]

Achim, Monica Violeta, and Nicolae Sorin Borlea. 2020. *Economic and Financial Crime. Corruption, Shadow Economy, and Money Laundering*. Berlin: Springer. [CrossRef]

Achim, Monica Violeta, Nicolae Sorin Borlea, and Viorela Ligia Văidean. 2021. Does technology matter for combating economic and financial crime? A panel data study. *Technological and Economic Development of Economy* 27: 223–61. [CrossRef]

AEPD. 2020. GDPR Compliance of Processings That Embed Artificial Intelligence An Introduction. Available online: https://www.aepd.es/sites/default/files/2020-07/adecuacion-rgpd-ia-en.pdf (accessed on 9 April 2021).

Amarasinghe, Thushara, Achala Aponso, and Naomi Krishnarajah. 2018. Critical Analysis of Machine Learning Based Approaches for Fraud Detection in Financial Transactions. In Paper presented at the ICMLT '18: Proceedings of the 2018 International Conference on Machine Learning Technologies, London, UK, June 27–30; pp. 12–17. [CrossRef]

AMLC. 2017. The Second European Payment Services Directive (PSD2) and the Risks of Fraud and Money Laundering. Available online: https://www.amlc.eu/wp-content/uploads/2019/04/The-PSD2-and-the-Risks-of-Fraud-and-Money-Laundering.pdf (accessed on 9 April 2021).

Article 29 Data Protection Working Party. 2018. Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679. Available online: https://www.dataprotection.ro/servlet/ViewDocument?id=1436 (accessed on 9 April 2021).

Asha, R. B., and K. R. Suresh Kumar. 2021. Credit Card Fraud Detection Using Artificial Neural Network, Global Transitions Proceedings. *Journal Pre-Proof*. [CrossRef]

Bagga, Siddhant, Goyal Anish, Gupta Nmaita, and Arvind Goyal. 2020. Credit Card Fraud Detection using Pipeling and Ensemble Learning. *Procedia Computer Science* 173: 104–12. [CrossRef]

Biega, Asia J., Peter Potash, Hal Daumé, Fernando Diaz, and Michèle Finck. 2020. Operationalizing the Legal Principle of Data Minimization for Personalization. In *Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval (SIGIR '20)*. New York: Association for Computing Machinery, pp. 399–408. [CrossRef]

Butterworth, Michael. 2018. The ICO and artificial intelligence: The role of fairness in the GDPR framework. *Computer Law & Security Review* 34: 257–68. [CrossRef]

Canillas, Rémi, Rania Talbi, Sara Bouchenak, Omar Hasan, Lionel Brunie, and Laurent Sarrat. 2018. Exploratory Study of Privacy Preserving Fraud Detection. Paper presented at the 19th International Middleware Conference Industry (Middleware 18 Industry), Rennes, France, December 10–14; New York: ACM.

Carminati, Michele, Mario Polino, Andrea Continella, Andrea Lanzi, Federico Maggi, and Stefano Zanero. 2018. Security Evaluation of a Banking Fraud Analysis System. *ACM Transactions on Privacy and Security* 21: 3. [CrossRef]

Castets-Renard, Céline. 2019. Accountability of Algorithms in the GDPR and Beyond: A European Legal Framework on Automated Decision-Making. *30 Fordham Intellectual Property and Entertainment Law Journal* 91. Available online: https://ir.lawnet.fordham.edu/iplj/vol30/iss1/ (accessed on 9 April 2021). [CrossRef]

Chen, Ligong, Lijun Yang, Zhaohui Zhang, and Meng Ying. 2019. A Method for Online Transaction Fraud Detection Based on Individual Behavior. In *ACM TURC '19: Proceedings of the ACM Turing Celebration Conference—China*. New York: ACM, pp. 1–8. [CrossRef]

Chen, Keqin, Yadav Amit, and Zhu Kun. 2020. Credit Fraud Detection Based on Hybrid Credit Scoring Model. *Procedia Computer Science* 167: 2–8. [CrossRef]

Citron, Danielle Keats, Solove Daniel, and Privacy Harms. 2021. *GWU Legal Studies Research Paper No. 2021-11*. Washington, DC: GWU Law School Public. [CrossRef]

Clifford, Damian, and Ausloos Jef. 2018. Data Protection and the Role of Fairness. *Yearbook of European Law* 37: 130–87. [CrossRef]

Clifford, Damian, and Jef Ausloos. 2017. *Data Protection and the Role of Fairness*. CiTiP Working Paper 29/2017. Cham: Springer. [CrossRef]

CNIL. 2018. PIA Knowledge Base. Available online: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf (accessed on 9 April 2021).

Cormack, Andrew. 2020. Processing Data to Protect Data: Resolving the Breach Detection Paradox. *Journal of Law, Technology & Society* 17: 2. [CrossRef]

Council of Europe. 2019. *Artificial Intelligence and Data Protection: Challenges and Possible Remedies*. Strasbourg: Council of Europe.

Datatilsynet. 2018. The Norwegian Data Protection Authority. Artificial Intelligence and Privacy. Report. Available online: https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf (accessed on 9 April 2021).

Dong, Feng, Haoyu Wang, Li Li, Yao Guo, Tegawendé F. Bissyandé, Tianming Liu, Guoai Xu, and Jacques Klein. 2018. FraudDroid: Automated Ad Fraud Detection for Android Apps. In *ESEC/FSE 2018: Proceedings of the 2018 26th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*. New York: Association for Computing Machinery, pp. 257–68.

Dornadula, Vaishnavi, and Nath S Geetha. 2019. Credit Card Fraud Detection using Machine Learning Algorithms. *Procedia Computer Science* 165: 631–41. [CrossRef]

Dwork, Cynthia, Moritz Hardt, Toniann Pitassi, Omer Reingold, and Richard Zemel. 2012. Fairness through awareness. In *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference (ITCS '12)*. New York: Association for Computing Machinery, pp. 214–26. [CrossRef]

European Banking Authority (EBA). 2018. *Opinion of the European Banking Authority on the Implementation of the RTS on SCA and CSC*. Paris: EBA.

European Banking Authority (EBA). 2019. *Opinion of the European Banking Authority on the Elements of Strong Customer Authentication under PSD2*. Paris: EBA.

ECJ. 2014. *Cases C293/12 and C594/12. Digital Rights Ireland*. Luxembourg: ECJ.

European Data Protection Board (EDPB). 2020. *Guidelines 05/2020 on Consent under Regulation 2016/679*. Brussels: EDPB.

Edwards, L., and M. Veale. 2017. Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for. *Duke Law & Technology Review* 16: 18–84.

European Parliamentary Research Service (EPRS). 2020. *The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence*. EPRS. Available online: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf (accessed on 9 April 2021).

Eurobarometer. 2015. *Special Eurobarometer 423, Cybersecurity*. Eurobarometer. Available online: https://www.adepp.info/wp-content/uploads/2016/07/studio-su-cybercrime.pdf (accessed on 9 April 2021).

European Payments Council. 2019. *Payment Threats and Fraud Trends Report*. Brussels: European Payments Council.

Eurostat. 2020. *ICT Usage in Households and by Individuals*. Eurostat. Available online: https://ec.europa.eu/eurostat/cache/metadata/en/isoc_i_esms.htm (accessed on 9 April 2021).

Finck, Michèle, and Biega Asia. 2021. Reviving Purpose Limitation and Data Minimisation in Personalisation, Profiling and Decision-Making Systems. *Max Planck Institute for Innovation & Competition Research*, 21–24. [CrossRef]

Floridi, L., S. Wachter, and B. Mittelstadt. 2017. Transparent, explainable, and accountable AI for robotics. *Science Robotics* 2. [CrossRef]

Forgó, Nikolaus, Stefanie Hänold, and Benjamin Schütze. 2017. The principle of purpose limitation and Big Data. In *New Technology, Big Data and the Law*. Edited by Marcelo Corrales, Mark Fenwick and Nikolaus Forgó. Singapore: Springer. [CrossRef]

Galhotra, Sainyam, Yuriy Brun, and Alexandra Meliou. 2017. Fairness testing: Testing software for discrimination. In *Proceedings of the 2017 11th Joint Meeting on Foundations of Software Engineering (ESEC/FSE 2017)*. New York: Association for Computing Machinery, pp. 498–510. [CrossRef]

Ginart, Antonio A., Melody Y. Guan, Gregory Valiant, and James Zou. 2019. Data Deletion in Machine Learning. Paper presented at the 33rd Conference on Neural Information Processing Systems (NeurIPS 2019), Vancouver, BC, Canada, December 8–14.

Goldsteen, A., G. Ezov, R. Shmelkin, M. Moffie, and A. Farkash. 2020. Data Minimization for GDPR Compliance in Machine Learning Models. *arXiv* arXiv:2008.04113.

González, Gil E., and P. de Hert. 2019. Understanding the legal provisions that allow processing and profiling of personal data—An analysis of GDPR provisions and principles. *ERA Forum* 19: 597–621. [CrossRef]

Green, B, and S. Viljoen. 2020. Algorithmic Realism: Expanding the Boundaries of Algorithmic Thought. In *Proceedings of the ACM Conference on Fairness, Accountability, and Transparency (FAT*)*. New York: Association for Computing Machinery.

Gruschka, N., V. Mavroeidis, K. Vishi, and M. Jensen. 2018. Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR. Paper presented at the 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, December 10–13; pp. 5027–33. [CrossRef]

Hacker, P., and B. Petkovka. 2017. Reining in the big promise of Big Data: Transparency, inequality, and new regulatory frontiers. *Northwestern Journal of Technology and Intellectual Property* 15: 1–42. [CrossRef]

Hajian, Sara, and Josep Domingo-Ferrer. 2013. A Methodology for Direct and Indirect Discrimination Prevention in Data Mining. *IEEE Transactions on Knowledge and Data Engineering* 25: 1445–59. [CrossRef]

Hawash, R., and G. Lang. 2020. Does the digital gap matter? Estimating the impact of ICT on productivity in developing countries. *Eurasian Economic Review* 10: 189–209. [CrossRef]

Hoffmann, A. O. I., and C. Birnbrich. 2012. The impact of fraud prevention on bank-customer relationships: An empirical investigation in retail banking. *International Journal of Bank Marketing* 30: 390–407. [CrossRef]

Horak, Martin, Václav Stupka, and Martin Husák. 2019. GDPR Compliance in Cybersecurity Software: A Case Study of DPIA in Information Sharing Platform. In *ARES '19: Proceedings of the 14th International Conference on Availability, Reliability and Security*. New York: Association for Computing Machinery. [CrossRef]

ICO. 2017. *Big Data, Artificial Intelligence, Machine Learning and Data Protection*. Cheshire: ICO.

Jha, Sanjeev, Montserrat Guillen, and J. Christopher Westland. 2012. Employing transaction aggregation strategy to detect credit card fraud. *Expert Systems with Applications* 39: 12650–57. [CrossRef]

Jiang, C. J., G. Song, L. Liu, and W. Luan. 2018. Credit Card Fraud Detection: A Novel Approach Using Aggregation Strategy and Feedback Mechanism. *IEEE Internet of Things Journal* 5: 3637–47. [CrossRef]

Kaltheuner, F., and E. Bietti. 2018. Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR. *Journal of Information Rights, Policy and Practice* 2. [CrossRef]

Kaminski, Margot E., and Gianclaudio Malgieri. 2020. Multi-layered explanations from algorithmic impact assessments in the GDPR. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (FAT* '20)*. New York: Association for Computing Machinery, pp. 68–79. [CrossRef]

Kamiran, F., I. Zliobaite, and T. Calders. 2013. Quantifying explainable discrimination and removing illegal discrimination in automated decision making. *Knowledge and Information Systems* 35: 613–44. [CrossRef]

Li, Zhenchuan, Huang Mian, and Jiang Changjun. 2021. A hybrid method with dynamic weighted entropy for handling the problem of class imbalance with overlap in credit card fraud detection. *Expert Systems with Applications* 175: 114750. [CrossRef]

Malgieri, Gianclaudio. 2018. Automated Decision-Making in the EU Member States: The Right to Explanation and Other 'Suitable Safeguards' for Algorithmic Decisions in the EU National Legislations. *Computer Law & Security Review*. [CrossRef]

Malgieri, Gianclaudio. 2020. The concept of fairness in the GDPR: A linguistic and contextual interpretation. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (FAT* '20)*. New York: Association for Computing Machinery, pp. 154–66. [CrossRef]

Malgieri, G., and G. Comandé. 2017. Why a right to legibility of automated decision-making exists in the general data protection regulation. *International Data Privacy Law* 7: 243–65. [CrossRef]

Mehmet, Huseyin Bilgin, Chi Keung, Marco Lau, and Ender Demir. 2012. *Technology Transfer, Finance Channels, and SME Performance: New Evidence from Developing Countries, The Singapore Economic Review (SER)*. Singapore: World Scientific Publishing Co. Pte. Ltd., vol. 57, pp. 1–20.

Misra, Sumit, Thakur Soumyadeep, Ghosh Manosij, and Saha Sanjoy Kumar. 2020. An Autoencoder Based Model for Detecting Fraudulent Credit Card Transaction. *Procedia Computer Science* 167: 254–62. [CrossRef]

Nathan, R.J., V. Victor, and C. L. Gan. 2019. Electronic commerce for home-based businesses in emerging and developed economy. *Eurasian Business Review* 9: 463–83. [CrossRef]

Nilson Report. 2020. Issue 1187-December 2020. Available online: https://nilsonreport.com/publication_newsletter_archive_issue.php?issue=1187 (accessed on 9 April 2021).

Öğrek, Mahmut, Öğrek Eyüp, and Bahtiyar Şerif. 2019. A deep learning method for fraud detection in financial systems: Poster. In *WiSec '19: Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*. New York: Association for Computing Machinery, pp. 298–99. [CrossRef]

Olowookere, Toluwase, Ayobami Adewale, and Olumide Sunday. 2020. A framework for detecting credit card fraud with cost-sensitive meta-learning ensemble approach. *Scientific African* 8: e00464. [CrossRef]

Perera, H. W., D. Hussain, R. A. Mougouei, A. Shams Nurwidyantoro, and J. Whittle. 2019. Towards Integrating Human Values into Software: Mapping Principles and Rights of GDPR to Values. Paper presented at the IEEE 27th International Requirements Engineering Conference (RE), Jeju, Korea, September 23–27; pp. 404–9. [CrossRef]

Politou, Eugenia, Efthimios Alepis, and Constantinos Patsakis. 2019. Profiling tax and financial behaviour with big data under the GDPR. *Computer Law & Security Review* 35: 306–29. [CrossRef]

Reidenberg, J., N. Russell, A. Callen, S. Qasir, and T. Norton. 2014. Privacy harms and the effectiveness of the notice and choice framework. Paper presented at 2014 TPRC Conference, Washington, DC, USA, September 11–14. Fordham Law Legal Studies Research Paper No. 2418247.

Rojas, Lopez, Edgar Alonso, Gultemen Dincer, and Zoto Erjon. 2018. On the GDPR Introduction in EU and Its Impact on Financial Fraud Research. In *European Modeling and Simulation Symposium, EMSS*. New York: Fordham Center on Law and Information Policy.

Romei, A., and S. Ruggieri. 2014. A multidisciplinary survey on discrimination analysis. *The Knowledge Engineering Review* 29: 582–638. [CrossRef]

Stalla-Bourdillon, Sophie, Pearce Henry, and Tsakalakis Niko. 2018. The GDPR: A game changer for electronic identification schemes? The case study of Gov.UK Verify. *Computer Law & Security Review* 34: 784–805. [CrossRef]

Sudharsan, K., D. Ambeth Kumar, R. Venkatesan, V. Sathyapreiya, and G. Saranya. 2019. Two Three Step Authentication in ATM Machine to Transfer Money and for Voting Application. *Procedia Computer Science* 165: 300–6. [CrossRef]

Șcheau, Mircea Cosntantin, Viorel Nicolae Gaftea, Monica Violeta Achim, and Corina-Narcisa Cotoc. 2020. Cyber Security Reactivity in Crisis Times and Critical Infrastructures. Paper presented at 24th International Conference on System Theory, Control and Computing (ICSTCC), Sinaia, Romania, October 8–10; pp. 691–98. [CrossRef]

Vedder, A., and L. Naudts. 2017. Accountability for the use of algorithms in a Big Data environment. International Review of Law. *Computers & Technology* 31: 206–24.

Wachter, Sandra, and Mittelstadt Brent. 2019. A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review*. [CrossRef]

Wachter, S., B. Mittelstadt, and L. Floridi. 2017. Why a right to explanation of automated decision-making does not exist in the general data protection regulation. *International Data Privacy Law* 7: 76–99. [CrossRef]

Wachter, Sandra, Mittelstadt Brent, and Russell Chris. 2020. Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI. *Computer Law & Security Review*. [CrossRef]

Wang, Yuan, and Liming Wang. 2019. Bot-like Behavior Detection in Online Banking. In *ICBDC 2019: Proceedings of the 2019 4th International Conference on Big Data and Computing*. New York: Association for Computing Machinery, pp. 140–44. [CrossRef]

Whitrow, C., D. J. Hand, and P. Juszczak. 2009. Transaction aggregation as a strategy for credit card fraud detection. *Data Mining and Knowledge Discovery* 18: 30–55. [CrossRef]

Yang, Bao, Hilary Gilles, and Ke Bin. 2020. Artificial Intelligence and Fraud Detection. Innovative Technology at the interface of Finance and Operations. Springer Series in Supply Chain Management. *Springer Nature*. [CrossRef]

Yu, S. 2016. Big Privacy: Challenges and Opportunities of Privacy Study in the Age of Big Data. *IEEE Access* 4: 2751–63. [CrossRef]