# Balancing fraud analytics with legal requirements

## Governance practices and trade-offs in public administrations

Simonofski, Anthony; Tombal, Thomas; De Terwangne, Cécile; Willem, Pauline; Frenay, Benoît; Janssen, Marijn

**DOI**
10.1017/dap.2022.6

**Publication date**
2022

**Document Version**
Final published version

**Published in**
Data and Policy

**Citation (APA)**
Simonofski, A., Tombal, T., De Terwangne, C., Willem, P., Frenay, B., & Janssen, M. (2022). Balancing fraud analytics with legal requirements: Governance practices and trade-offs in public administrations. *Data and Policy*, *4*(1-2), Article e14. https://doi.org/10.1017/dap.2022.6

*Data & Policy* (2022), 4: e14
doi:10.1017/dap.2022.6

RESEARCH ARTICLE

# Balancing fraud analytics with legal requirements: Governance practices and trade-offs in public administrations

Anthony Simonofski[1,*], Thomas Tombal[2], Cécile De Terwangne[1], Pauline Willem[1], Benoît Frenay[1] and Marijn Janssen[3]

[1]University of Namur, Namur Digital Institute, Namur, Belgium
[2]Tilburg University, Tilburg Law School, Tilburg, Netherlands
[3]TU Delft, Faculty of Technology, Policy and Management, Delft, Netherlands
*Corresponding author. E-mail: anthony.simonofski@unamur.be

**Received:** 15 December 2021; **Revised:** 16 March 2022; **Accepted:** 17 March 2022

**Key words:** artificial intelligence; big data; fraud analytics; governance; public administration

## Abstract

Fraud analytics refers to the use of advanced analytics (data mining, big data analysis, or artificial intelligence) to detect fraud. While fraud analytics offers the promise of more efficiency in fighting fraud, it also raises legal challenges related to data protection and administrative law. These legal requirements are well documented but the concrete way in which public administrations have integrated them remains unexplored. Due to the complexity of the techniques applied, it is crucial to understand the current state of practice and the accompanying challenges to develop appropriate governance mechanisms. The use of advanced analytics in organizations without appropriate organizational change can lead to ethical challenges and privacy issues. The goal of this article is to examine how these legal requirements are addressed in public administrations and to identify the challenges that emerge in doing so. For this, we examined two case studies related to fraud analytics from the Belgian Federal administration: the detection of tax frauds and social security infringements. This article details 15 governance practices that have been used in administrations. Furthermore, it highlights the complexity of integrating legal requirements with advanced analytics by identifying six key trade-offs between fraud analytics opportunities and legal requirements.

## Policy Significance Statement

Public administrations consistently use more and more data to deliver their public services. In this regard, they can process a large number of citizens' personal data in order. This key balance between the efficiency allowed by advanced analytics and the legal requirements is at the core of this article. Policy-makers will find guidance to drive their legally compliant advanced analytics projects. More specifically, this article summarizes 15 governance practices observed from the two cases related to the detection of tax fraud and social security fraud. These practices are relevant policy practitioners as they are empirically validated and provide concrete implementation of legal requirements. As a result, they can be used as guidelines for the interested policy-makers.

This research article was awarded an Open Materials badge for transparent practices. See the Data Availability Statement for details.

## 1. Introduction

The use of advanced analytics to detect tax fraud has been examined in previous research (Yu et al., 2003; Van Vlasselaer et al., 2017) and has been labeled as "*fraud analytics*" (Baesens et al., 2015). Fraud analytics refers to a more global approach consisting of using analytics in fraud detection, investigation, confirmation, and ultimately prevention (Baesens et al., 2015; Pencheva et al., 2018). Frauds have five inherent characteristics that make the use of advanced analytics, ranging from data mining, big data analysis to artificial intelligence (AI) and machine learning, valuable (Van Vlasselaer et al., 2017; De Roux et al., 2018). First, as only a limited number of fraud cases are identified, the corresponding data is sporadic in existing datasets. Second, frauds are well-planned and often impact more than one attribute in datasets due to their inherent complexity. Third, fraud is evolving over time, as fraudsters are adaptive and learn from past mistakes. Fourth, frauds are carefully organized as fraudsters have allies and transfer knowledge with each other to commit fraud without being detected. Finally, fraudsters, whether they are organizations or individuals, may have the same characteristics as legitimate companies or individuals. These characteristics all complicate the process of fraud detection and drive the need for the use of advanced analytics, and in consequence, the implementation of legal requirements is challenging.

While fraud analytics offers the promise of more efficiency in fighting fraud, public administrations face additional constraints, such as the need to be trusted by the citizens and to comply with the legal framework. Whether they use traditional or advanced techniques, administrations consistently use more and more data and automatic processing and AI-based techniques to deliver public services. In this regard, they often need to process citizens' personal data, defined by the General Data Protection Regulation (GDPR),[1] as "*any information relating to an identified or identifiable natural person*" (Art. 4.1, GDPR). When processing personal data, organizations have to comply with the citizens' fundamental right to personal data protection,[2] which derives from their right to privacy.[3] As the concrete rules pertaining to these fundamental rights are contained in the GDPR, our analysis will focus on this. Regulation, rather than on more overarching fundamental rights issues. Furthermore, the core principles of administrative law have to be considered as well, since fraud analytics takes place in the context of the administrations' pursuit of their public service missions. As the use of such technologies could have a strong impact on the lives of their citizens, it is fundamental for public administrations to balance the opportunities they offer with the need to comply with these legal requirements.

Previous research showed that several governance mechanisms can be used to balance data analytics opportunities with relevant legal requirements, such as Winter and Davidson (2019) for personal health data. While these legal requirements are well documented (see Section 2.2 for an overview), the concrete way in which they have been integrated with fraud analytics practices of public administrations remains unexplored. This is a key issue as the introduction of analytics in organizations without the introduction of appropriate organizational change and new governance practices can lead to ethical challenges and privacy issues (Gal et al., 2020). Therefore, in this article, we aim to address the following Research Questions (RQ):

- RQ1: How are legal requirements related to data protection law and administrative law addressed in the fraud analytics process of the Belgian Federal administration?
- RQ2: What are the main challenges that emerge when integrating these legal requirements in the fraud analytics process?

[1] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 (General Data Protection Regulation), OJ [2016] L 199/1.

[2] Charter of Fundamental Rights of the European Union, OJ [2012] C 326/391, art. 8.

[3] European Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4 November 1950, art. 8; Charter of Fundamental Rights of the European Union, OJ [2012] C 326/391, art. 7; Belgian Constitution, art. 22.

https://doi.org/10.1017/dap.2022.6 Published online by Cambridge University Press

The remainder of this article is structured as follows. In Section 2, we describe the fraud analytics process, the main legal requirements that constrain the use of fraud analytics techniques; as well as the research gaps. In Section 3, we detail how we collected and analyzed data from the two selected case studies. In Section 4, we describe how the legal requirements have been implemented in the fraud analytics process of the studied administrations; and the main challenges these administrations faced in doing so. In Section 5, we position our findings with the previous findings of the literature and suggest leads for solutions to address the identified challenges. In Section 6, we summarize the main contributions of this work and we present the limitations of this research and further research.

## 2. Background

In this section, we first examine what lies behind the concept of "fraud analytics" (Section 2.1). Then, we present the main data protection law and administrative law requirements that must be factored in by administrations (Section 2.2). Finally, we highlight the research gaps, in terms of the concrete implementation of these legal requirements in the administrations' fraud analytics processes, that this article aims to address (Section 2.3).

### *2.1. Fraud analytics: Advanced analytics for fraud detection*

Before leveraging advanced analytics opportunities, tax authorities tackled tax fraud with two approaches (Castellón González and Velásquez, 2013). The *auditor experience* approach selects a number of tax declarations and audits them based on experience and domain knowledge. The *rule-based system* approach applies "if-then" rules to detect fraud cases. These rules are burdensome to develop as experts have to review and generalize fraud characteristics after having identified them. The main issues with selection techniques are that they exclusively rely on past experiences, lack adaptability to new fraud mechanisms, and are based on the subjective judgment of experts.

Therefore, advanced analytics techniques are needed, as reported in Van Vlasselaer et al., (2017) and De Roux et al. (2018). This call for advanced analytics and digital transformation of the tax administrations have been pushed on the agenda by several countries, under the influence of international organizations (OECD, 2016; IOTA, 2018). Klievink et al. (2017) suggest a usage process for the analysis of advanced analytics. First, there is the *Preprocessing* stage in which data is identified, collected from several sources, combined, and cleansed. Second, there is the *Data Analytics* stage, where several techniques are applied to analyze the data. Third, there is the *Postprocessing* stage, in which the output of the analysis is presented to the relevant stakeholder, interpreted and, in case of governments, has an impact on policy-making.

Recent works in tax fraud detection are based on supervised machine learning techniques with labeled, audit-assisted data. A typical example in a fraud detection setting, using regression techniques, is predicting the fraud amount. In classification techniques, the target is categorical, which means that it can only take on a limited set of predefined values. In binary classification, only two classes are considered (e.g., fraud vs. no-fraud), whereas in multiclass classification, the target can belong to more than two classes (e.g., depending on the severity or the type of fraud). However, the follow-auditing is slow and costly. Several authors argue for the application of unsupervised techniques (De Roux et al., 2018). For instance, unsupervised techniques could be used to find behavior that deviates from normal behavior and to find outliers/anomalies (Baesens et al., 2015). They are unsupervised as they do not need observations to be labeled as fraudulent or nonfraudulent. Anomalies do not necessarily represent fraudulent observations. Hence, the usage of unsupervised learning for fraud detection requires extensive follow-up and validation of the identified, suspicious observations to determine if there is actual fraud. The third type of technique that can be used is social network analysis, where fraudulent activities can be identified within a network of linked entities (Baesens et al., 2015). As fraud is social in nature, the underlying assumption is that the probability of someone committing fraud depends on the people that person is connected to. These

https://doi.org/10.1017/dap.2022.6 Published online by Cambridge University Press

are the so-called guilt-by-associations (Koutra et al., 2011). Fraud detection can make use, in a complementary manner, of these different techniques.

### *2.2. Data protection and administrative legal requirements*

While fraud analytics offers the promise of more efficiency in fighting fraud, it also raises legal challenges for public administrations. These legal challenges, which fit in the broader context of the legal challenges that must be considered by public administrations when employing analytics and algorithmic processes, are well documented (Hildebrandt, 2019; Council of Europe, 2020).

As for advanced analytics (Mayer-Schönberger and Padova, 2016; Rouvroy, 2016; De Raedt, 2017; Zarsky, 2017; Hildebrandt, 2019), the opportunities offered by fraud analytics must be balanced with the need to protect the citizens' right to privacy and personal data protection (De Raedt, 2017; Scarcella, 2019).[4] While many GDPR provisions and national laws (see Section 4.2) apply to the fraud analytics process, certain legal requirements are especially important to consider.

In terms of data collection, the data must be collected *fairly and transparently* (Art. 5.1.a, GDPR). According to the *purpose limitation principle* (Art. 5.1.b, GDPR), personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. According to the *data minimization principle* (Art. 5.1.c, GDPR), only the adequate, relevant, and necessary data for the fulfillment of the specific purpose of processing shall be processed. Moreover, the *processing of "special categories of data"* (Art. 9, GDPR), such as health-related data, and of *data relating to criminal convictions and offenses* (Art. 10, GDPR) is subjected to stricter rules.

In terms of data analytics, any fraud analytics process must rely on a *lawful basis of processing* (Art. 6, GDPR). In practice, this will often be a law (Art. 6.1.c, GDPR), but this law needs to meet several requirements, such as being very specific regarding the purposes of processing it allows (Art. 6.3, GDPR). For the sake of concision, this requirement will be addressed together with the purpose limitation principle in Section 4.2 as they are intertwined. The GDPR also provides several rights to data subjects, which should be considered when employing data analytics. For instance, the data subjects' *right to information* (Art 12–14, GDPR) mentions that data has to be processed fairly and in a transparent manner (accordingly, this right and the principle of fairness and transparency mentioned above will be addressed together in Section 4.2). Therefore, the public administrations shall take appropriate measures to provide any information to the data subjects about the data analytics in a concise, transparent, intelligible, and easily accessible form, using clear and plain language. Moreover, the data subjects' *right of access* (Art. 15, GDPR) provides that the data subject has the right to obtain, from the public administration, the confirmation as to whether or not it processes personal data concerning her as well as to obtain a copy of the personal data that is processed. Additionally, the data subjects' *right to erasure* (Art. 17, GDPR) provides that the data subject shall have the right to obtain the erasure of personal data concerning her. However, this right can be limited for processing done by administrations (Art. 17.3.b, GDPR). In practice, erasure is difficult as a model has been trained on historical data to produce a result and will use these "learned" results to train on the next batch of data (Villaronga et al., 2018). Furthermore, the data subjects have the *right not to be subject to a decision based solely on automated processing* (Art. 22, GDPR). In this regard, particular attention must be given to the introduction of fictitious or negligible human intervention in the automated decision process, simply in order to avoid (potentially in bad faith) the application of this right. While there are exceptions to this right, such as fully automated processing authorized by a law (Art. 22.2, GDPR), safeguards shall be implemented, such as the right to obtain human intervention (Art. 22.3, GDPR). Finally, it should be mentioned that national laws can nevertheless

[4] Article 29 Working Party, *Guidelines for Member States on the criteria to ensure compliance with data protection requirements in the context of the automatic exchange of personal data for tax purposes*, WP 234, 16 December 2015, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp234_en.pdf; Article 29 Working Party, *Statement of the WP29 on automatic inter-state exchanges of personal data for tax purposes*, WP 230, 4 February 2015, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp230_en.pdf.

https://doi.org/10.1017/dap.2022.6 Published online by Cambridge University Press

restrict the data subjects' rights granted in the GDPR, provided that this restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard an important objective of general public interest (Art. 23, GDPR) (De Raedt, 2017; Scarcella, 2019). In fact, taxation and social security matters are explicitly mentioned as important economic or financial interests of the State (Art. 23.1.e, GDPR).

Moreover, since the fraud analytics process takes place in the context of the pursuit, by public administrations, of their public service missions through the use of some forms of automated processing, the core legal requirements, enshrined in administrative law, identified in the literature pertaining to the automatization of public services (Gérard, 2017) are also fundamental to consider. First, citizens have a *right to a human public service*, which derives from the right to human dignity and states that automated processing should not become the norm, and people are the exception. To some extent, this overlaps with Art. 22 GDPR, although the sources of law are different. They will thus be addressed together in Section 4.2. Second, they have the *right to have equal access to public services.* All public services users should be treated equally and should benefit from the same services and advantages. If applied to fraud analytics, this means that the citizens should be treated equally and that the technologies used (e.g., algorithms) shall not be biased and shall not entail discriminations against some categories of the population. Third, they have the *right to understand (explainability) the administrative decisions* pertaining to them. All unilateral legal acts of individual scope emanating from an administrative authority, whose purpose is to produce legal effects in respect of one or more persons under its jurisdiction, have to be "formerly motivated," which implies that the act must contain the legal and factual conditions that have led to the decision.[5] For decisions taken based on fraud analytics, this should be relatively easy to do if an algorithm simply applies a precise number of rules that it is bound to follow, but it might be more problematic if the public administration is unable to check or explain how the decision was taken (black-box).

### *2.3. Research gaps: Implementation of legal requirements in fraud analytics processes*

Even if previous research has examined fraud analytics techniques as reported in Section 2.1, and extensively describes the Legal Requirements that must be factored by public administrations as reported in Section 2.2, the way these public administrations consider the legal requirements pertaining to fraud analytics, and the way they translate them in their daily work in terms of governance remains relatively undocumented in the existing literature.

Previous research mainly focused on the technical integration of specific legal challenges. For instance, Bibal et al. (2020) focused on the impact of explainability on machine learning. Felzmann et al. (2019) focused on the transparency requirements for AI and concludes that a holistic approach to the integration of legal requirements is needed. Several papers took a broader perspective by developing a legal framework for big data (Kemp, 2014) or by providing data governance recommendations for trustworthy data exploitation (Janssen et al., 2020). Gruschka et al. (2019) examine the impact of the GDPR on two big data analytics processes (security incidents and authentication). For tax fraud, Degrave and Lachapelle (2014) highlighted some friction points between the fraud analytics process and the data subject's right of access to her data (Art. 15, GDPR), while De Raedt (2017) and De Raedt and Lachapelle (2018) highlighted friction points with the data subject's right to information and transparency. Scarcella (2019) focused on profiling and automated decision-making in the use of ICT tools by tax administrations. Lachapelle (2016) also outlined the impact of the use of big data analytics for tax purposes on the citizens' right to privacy. Focusing specifically on the OASIS data warehouse used to detect social security infringements (see Section 4.2), Degrave (2020b) outlines that the concrete functioning of this tool may be in breach of several legal requirements, such as the requirement of transparency.

However, there is a gap in the literature about how public administrations have adapted their government to address the data protection and core administrative law requirements in their fraud

[5] Loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs, *M.B.*, 12 septembre 1991, arts. 1–3.

https://doi.org/10.1017/dap.2022.6 Published online by Cambridge University Press

analytics processes. Due to the complexity of the techniques applied, understanding the current state of practice and the accompanying challenges is essential to design appropriate governance mechanisms and build knowledge. This article aims at filling this gap.

## 3. Methodology

To understand how the legal requirements identified in Section 2.2 are taken into account, in practice, by fraud analytics practitioners (RQ1), we examined two case studies within the Belgian Federal administration: the detection of tax frauds by the Federal Public Service (FPS) Finances and the detection of social security infringements by the Social Security Institutions (SSIs). By analyzing these case studies, clear challenges related to the implementation of legal requirements can be inferred as well (RQ2). Yin (2014) mentions that case study research is relevant to examine a current phenomenon when "how" questions are raised and where the researcher has no intervention in the case. Furthermore, we opted for two, rather than one, case studies as this improves the external validity of the research and allows drawing more general conclusions about the contextual factors in Belgium.

Data from the cases were extracted through semistructured interviews. This qualitative method is effective when covering a complex topic in detail (Baarda et al., 1996; Boyce and Neale, 2006). Moreover, this technique is relevant for our research questions, as it centers around the expertise of the practitioners, and not around the validation of the knowledge of the researchers. In total, 21 interviews were performed online due to the COVID-19 pandemic, from August 2020 to December 2020, with stakeholders from different management levels (strategic, mid-level, and operational) and different backgrounds (legal, IT, and management). In order to be selected for an interview, the participants had to work in the context of fraud analytics and more specifically to detect tax and social frauds. These disparate profiles allowed us to have a complete understanding of the fraud analytics processes, not only at the technical level but also regarding its impact on the organizational structure and the integration of legal requirements, in line with the holistic and contextualized approach suggested for advanced analytics research in Johnson et al. (2019). The IT profiles gave us more understanding about the impact of the requirements on the analytics techniques used, the legal profiles gave us information about the drivers for the changes in processes and the managerial profiles helped us understand the impact on the organizational structure. In that sense, the interviewees did not provide conflicting views about the implementation of legal requirements but rather complementary insights on different steps of the process. The full list of interviewees can be found in Table 1.

We examined the cases by giving attention to construct validity, internal validity, external validity, and reliability following the recommendations of Yin (2014). We ensured construct validity by using several sources to extract our findings. In addition to the interviews, strategic documents and reports from both cases were identified by browsing the institutional websites of the interviewed organizations or were directly suggested by the interviewees. These documents deal with the technical description of the fraud analytics processes, with its legal construction, and with the fraud detection strategies of the interviewed organizations or internal notes summarizing the main actions related to fraud analytics. Furthermore, this was further ensured by validating, with the interviewees, the main findings from the study. Regarding internal validity, the causal relationship between the legal requirements and how they have been implemented was once again ensured by the triangulation of several sources and the confirmation interviews. Although interviews could have been performed with complementary organizations (e.g., other SSIs or administrations at different government levels) to increase this validity, this was not done here as we had reached code saturation. Regarding external validity, we ensured a replication logic by taking two case studies to study the implementation of legal requirements. Finally, to ensure reliability, we have stored all the interview reports in a case study database in the research data repository of our university.

The analysis of the interviews and documents was performed following the overarching thematic content analysis method described in Mayring (2004) and Anderson (2007), using an inductive approach to infer the fraud analytics process as well as to the legal requirements. The analysis started with

https://doi.org/10.1017/dap.2022.6 Published online by Cambridge University Press

***Table 1.*** *Interviewees*

| Case | Function | Organization |
|---|---|---|
| Tax Fraud | Mid-level—Management | FPS Finances |
| Tax Fraud | Operational—IT | FPS Finances |
| Tax Fraud | Strategic—Management | FPS Finances |
| Tax Fraud | Strategic—IT | FPS Finances |
| Tax Fraud | Mid-level—IT | FPS Finances |
| Tax Fraud | Operational—IT | FPS Finances |
| Tax Fraud | Operational—Legal | FPS Finances |
| Tax Fraud | Operational—Legal | FPS Finances |
| Social Security | Operational—IT | Smals (Private company) |
| Social Security | Operational—IT | Smals (Private company) |
| Social Security | Operational—IT | Smals (Private company) |
| Social Security | Strategic—Management | CBSS (Social Security Database) |
| Social Security | Strategic—Management | CBSS (Social Security Data) |
| Social Security | Strategic—Management | ONEM (Job allocations) |
| Social Security | Strategic—Management | INAMI (Health allocations) |
| Social Security | Strategic—IT | INAMI (Health allocations) |
| Social Security | Strategic—Management | INAMI (Health allocations) |
| Social Security | Operational—Legal | INAMI (Health allocations) |
| Social Security | Operational—Legal | INAMI (Health allocations) |
| Social Security | Operational—IT | ONSS (Social Security coordination) |
| Social Security | Mid-level—IT | ONSS (Social Security coordination) |

summarizing the interviews and the documents in a data memo. In order to code the data, we skim the transcripts and the documents and highlight relevant sentences based on the research questions. Then, we insert the codes into a table divided by the main legal requirements. This method enables us to link similar themes from every interview and document to each other, making it easier to analyze what is being said and how it compares with other findings. We categorize the results from our interviews and documents (textual data) to concrete implementations of legal requirements for their daily work. No contradictions were identified between the data extracted from the documents and the interviews. The documents gave contextual insights about the drivers for implementing the legal requirements. We performed interviews until we reached code saturation, meaning that no new codes were identified after five consecutive interviews (Guest et al., 2006).

## 4. Results

### *4.1. Description of the two cases*

Before presenting how these legal requirements have been included by the FPS Finances and the SSIs in their fraud analytics processes, the general functioning of these two processes (i.e., the detection of tax frauds and the detection of social security infringements), is briefly presented.

Regarding the tax fraud detection process, data is first extracted from several sources and prepared for analysis. Then, data mining is used to signal potentially fraudulent cases that need to be further examined. Data miners perform the two tasks visualized in gray in Figure 1. Then, at the preinvestigation stage, the signals derived from the data mining tasks are enriched with data from other sources, and it is decided whether a proper investigation should be started. Finally, in the investigation stage, some of the potentially fraudulent cases are examined in-depth, with the support of analytics (e.g., text mining) to explore a large

https://doi.org/10.1017/dap.2022.6 Published online by Cambridge University Press

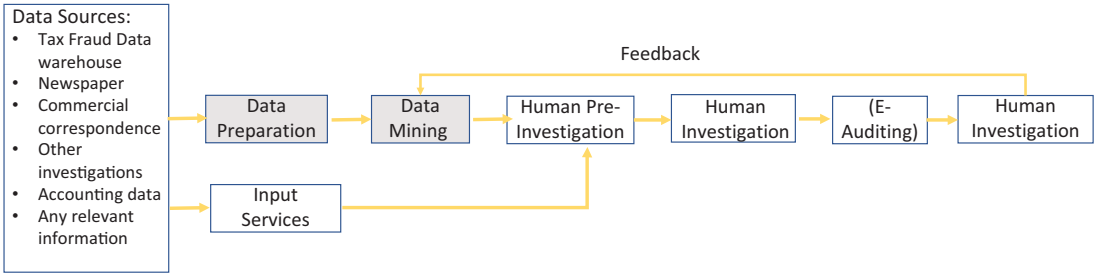


***Figure 1.*** *Fraud analytics process—tax frauds detection.*

quantity of unstructured data. This stage is also referred to as e-auditing. Inspectors perform these inspection tasks. Feedback is then given to data miners about the relevance of the signals. The cases to be investigated are sometimes also suggested by "Input services" that manually detect cases, based on expert knowledge, identified signals, and past experience, to be further investigated. The tax fraud detection process is presented in a simplified version in Figure 1.

For the social security infringement detection process, it is important to understand that a "Social Security Network" was created by the law of 15 January 1990,[6] in which all the Belgian Federal public SSIs are structured around the "Crossroad Bank for Social Security" (CBSS) (Degrave, 2020b). The CBSS acts as the core of the network, and the SSIs are the nodes.[7] While these SSIs remain in control of their authoritative sources of personal social data, the CBSS acts as the central actor for the data sharing between them.[8] The CBSS thus does not itself store any data, but rather acts as a "gatekeeper" that checks that an SSI has the right to access data stored on one of the nodes of the network (another SSI).

Regarding social security fraud, there is a difference between the types of techniques used to detect fraud committed by beneficiaries of social allocations, on the one hand, and employers, health institutions, independent workers, and so forth, on the other hand. For the former, SSIs mainly rely on data matching techniques via bilateral cross-checks from other SSIs' databases to identify incompatibilities in terms of allocations. These are done either before or after the payment of the allocation. For the latter, social security institutions mainly rely on data mining techniques, through the use of the OASIS data warehouse, where larger quantities of pseudonymized data are compiled. Moreover, one SSI is currently developing a big data analytics platform to improve the data governance mechanisms between SSIs, notably to tackle social fraud. The social security infringement detection process is presented in a simplified version in Figure 2.

### *4.2. Integration of legal requirements*

On the basis of the data extracted from the semistructured interviews, we detail how the main legal requirements for fraud analytics presented in Section 2.2 have been included by FPS Finances and the SSIs in their fraud analytics processes. Furthermore, we highlight the challenges identified in the interviews. Our findings are structured, in the following subsections, around the nine legal requirements presented in Section 2.2.

#### *4.2.1. Lawful basis and purpose limitation (LR1)*

Regarding the tax fraud case study, Article 3 of the Law of 3 August 2012[9] states that the FPS Finances can collect and process personal data to execute its legal missions, and that the data cannot be used for other

[6] Loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale, *M.B.*, 22 février 1990.

[7] https://www.ksz-bcss.fgov.be.

[8] Art. 3 of the Law of 15 January 1990.

[9] Loi du 3 août 2012 portant dispositions relatives aux traitements de données à caractère personnel réalisés par le Service public fédéral Finances dans le cadre de ses missions, *M.B.*, 24 août 2012.

https://doi.org/10.1017/dap.2022.6 Published online by Cambridge University Press

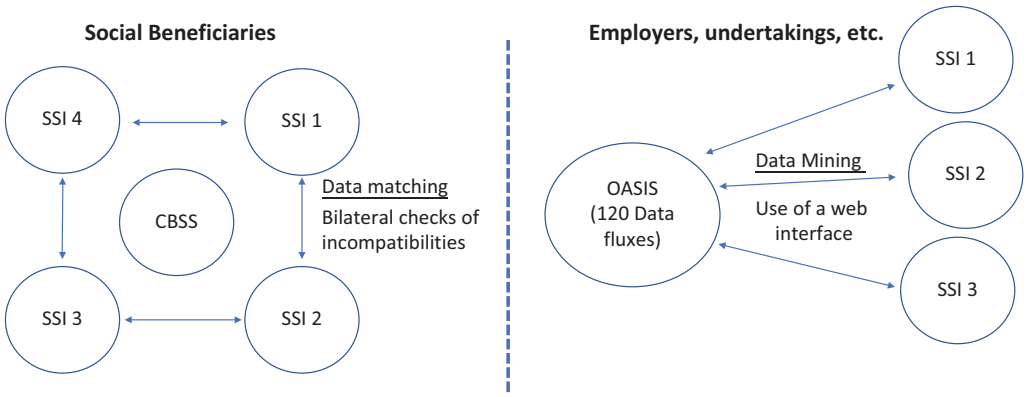


***Figure 2.*** *Fraud analytics process—social security infringements detection.*

purposes.[10] This Law, which constituted the lawful basis for the processing of personal data by the FPS Finances under the regime of the Data Protection Directive,[11] has been maintained and now constitutes the lawful basis of processing required by the GDPR (Art. 6.1.c, GDPR). It should, however, be outlined from the outset that some of the provisions of this Law have been modified in September 2018, in order to adapt it to the entry into force of the GDPR.[12]

Personal data processed by the FPS Finances can originate from the administration on the one hand (article 4 of the Law of 3 August 2012) or from external partners (e.g., other regional governments, foreign countries, and private parties) on the other hand (article 5, §2 of the Law of 3 August 2012). The safeguards are different in each hypothesis. Within the FPS Finances, the various administrations and/or services of the FPS can exchange personal data, provided that they have the authorization from the President of the Executive Committee.[13] The President can ask an opinion from the Information Security Committee (ISC) in this regard.[14] If personal data come from external parties, their integration in the data warehouse shall be subject to prior deliberation of the ISC (except in certain cases).[15] Moreover, if possible, those personal data must be pseudonymized (depseudonymization can only take place if there is a risk of an infringement of a law or regulation whose application falls within the tasks of the FPS Finances).[16]

Regarding, more specifically, the use of big data to fight tax fraud, Article 5.1, which was modified in September 2018,[17] provides that the FPS Finances may aggregate data, collected to execute its legal missions, in a "data warehouse" enabling "data mining" and "data matching" operations, including profiling. This can only be done to carry out, in the context of its legal missions, targeted controls on the basis of "risk indicators" and of analyses on data coming from different administrations and/or services of the FPS Finances. Although this Article constitutes the lawful basis for such processing (Art. 6.1.c, GDPR), such law must clearly determine the specific purposes of processing that are allowed (Art. 6.3, GDPR). Yet, the critique formulated by Degrave and Lachapelle (2014) regarding the previous version of

[10] Art. 3, al.1 and 2 of the Law of 3 August 2012.

[11] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ [1995] L 281/31, art. 7.c.

[12] Loi du 5 septembre 2018 instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en oeuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, *M.B.*, 10 septembre 2018, arts. 70–85.

[13] Art. 4, al.1 of the Law of 3 August 2012, as modified by Art. 70 of the Law of 5 September 2018.

[14] Art. 4, al.4 of the Law of 3 August 2012, as modified by Art. 70 of the Law of 5 September 2018.

[15] Art. 5, §2, al.1 and 3 of the Law of 3 August 2012, as modified by Art. 71 of the Law of 5 September 2018.

[16] Art. 5, §2, al. 2 of the Law of 3 August 2012, as modified by Art. 71 of the Law of 5 September 2018.

[17] Modified by art. 71 of the Law of 5 September 2018.

https://doi.org/10.1017/dap.2022.6 Published online by Cambridge University Press

Article 5, namely that the purposes of data processing were defined too broadly in the Law, as they simply referred to the execution of the FPS Finances' "legal missions," have not been addressed in the 2018 modification, as the same terminology is used. This might thus be problematic in terms of the validity of this Law as lawful basis for the processing, as well as in terms of compliance with the purpose limitation principle (Art. 5.1.b, GDPR)

However, this concern is somewhat alleviated as the data miners have to fill in a Data Access Management (DAM) fiche, which has to be validated by the President of the Executive Committee of the SPF Finances.[18] In this DAM fiche, they have to state the objectives and purposes of the data mining and explain how it fits the organization's mission. The purpose limitation principle is thus implemented at the process level, but in a way that is not ideal from a democratic perspective (as Parliament does not define the concrete purposes of processing) nor from a legal perspective (as according to Article 8 of the European Convention on Human Rights,[19] Article 22 of the Belgian Constitution and Art. 6.3 GDPR, the key elements of personal data processing by public administrations, such as the processing purposes, must be clearly defined by law).

The Law adds that personal data resulting from processing operations in the data warehouse shall be kept for no longer than is necessary for the purposes for which they are processed, with a maximal retention period of 1 year after the prescription of all actions falling within the competence of the controller.[20] In practice, a relevance check is performed every 3 months by the head of the data miners to see if the data are used in conformity with the DAM fiche and if the project is still relevant and advancing. If it is not, the data access ceases and the data must be deleted.

Regarding the social security fraud case study, the use of data matching techniques relying on bilateral cross-checks, aimed at identifying incompatibilities in terms of allocations, must be subject to a data transfer protocol, as provided in Article 20.1 of the Law of 30 July 2018,[21] unless provided otherwise in specific laws (e.g., in Article 15 of the Law of 15 January 1990, as modified in September 2018,[22] which requires, in some cases, a prior deliberation of the ISC). The protocol, which must notably contain the purposes of the data processing, must be submitted to the Data Protection Officers of the SSIs involved in the sharing.[23] However, they are not subject to a prior validation by the Data Protection Authority, which would bring more certainty in terms of the legitimacy of the purpose of processing. Once this purpose is achieved, the data must be deleted.

SSIs also use data mining techniques. According to Article 5*bis* of the Law of 15 January 1990, which has been inserted in September 2018,[24] they may aggregate and process data in a data warehouse, enabling them to carry out data mining operations to prevent, establish, prosecute, and punish offenses against social legislations which fall within their respective powers. This data warehouse is known as OASIS and has existed since 2005. According to De Raedt (2017) and Degrave (2020b), the purposes of processing in OASIS that are authorized by the law are not clearly defined, which could, here as well, be problematic in terms of the validity of this Law as lawful basis for the processing, as well as in terms of compliance with the purpose limitation principle. However, this concern is somewhat alleviated, although not optimally either from a democratic and legal perspective (see above), in the hypotheses contained in Articles 5*bis*, al.7 and 15 of the Law of 15 January 1990, as the authorization to process data from the data warehouse must be subject to a prior deliberation by ISC, which will evaluate the purposes of processing.[25] It must nevertheless be underlined here that the ISC should, in theory, be independent of the administrations (including the SSIs) to which it grants authorizations to process the data, which implies that its members

[18] Art. 4, al.1 of the Law of 3 August 2012, as modified by Art. 70 of the Law of 5 September 2018.

[19] European Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4 November 1950.

[20] Art. 5.1, al.3 of the Law of 3 August 2012, as modified by Art. 71 of the Law of 5 September 2018.

[21] Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018.

[22] Modified by art. 18 of the Law of 5 September 2018.

[23] Art. 20.2 of the Law of 30 July 2018.

[24] Inserted by art. 12 of the Law of 5 September 2018.

[25] Art. 5bis, al. 1 of the Law of 15 January 1990, inserted by art. 12 of the Law of 5 September 2018.

https://doi.org/10.1017/dap.2022.6 Published online by Cambridge University Press

should not also exercise mandates within these administrations.[26] This is currently not the case, which creates independence issues as some members of the CSI are both players and referees, and this has led to the launch of an infringement procedure by the European Commission against Belgium.[27] This situation will need to be remedied as soon as possible.

Moreover, if such a deliberation is not imposed, then the data controllers taking part in the fraud detection processing will nevertheless have to conclude a data transfer protocol, notably specifying the desired processing purposes, as this is the standard for any exchange of personal data between administrations, in light of the accountability principle of the GDPR (Art. 5.2, GDPR).[28] In any case, personal data resulting from processing operations in the data warehouse shall be kept for no longer than is necessary for the purposes for which they are processed, with a maximal retention period not exceeding 1 year after the prescription of all actions falling within the competence of the data controller.[29]

The purpose limitation principle is thus also implemented at the process level in the social security case study, as the purposes of the data matching or data mining operations have to be defined in advance, either in a protocol or in the file to be submitted to the ISC.

The mechanisms mentioned above, introduced to address purpose limitation, can be in conflict with the need for reactivity in fraud analytics. In some cases, such as customs tax fraud detection, administrations have to react very quickly, and getting the authorizations is time-consuming. Furthermore, it can be challenging to precisely define the exact type of fraud that they are investigating in advance, as this is sometimes broadly defined at the start and needs to be further refined with time. This is the first challenge: "*Challenge 1: Ensuring reactivity to frauds while respecting purpose limitation.*"

#### *4.2.2. Data minimization (LR2)*

Regarding the tax fraud case study, one may distinguish the application of the data minimization principle with regard to data collection, data mining, and e-auditing phase (those two last points are two specific forms or data processing).

Concerning data collection, personal data exchange between the various administrations and/or services of the FPS Finances must be authorized by the President of the Executive Committee.[30] The President decides which types of personal data can be exchanged, on a systematic or ad hoc basis and for specific purposes, after having verified their adequacy, relevance, and nonexcessiveness.[31] This is a materialization of the data minimization principle.

When it comes to personal data furnished by third parties, the data minimization principle is enshrined in the fact that the integration of such data in the data warehouse is subject to a prior deliberation by the ISC. Moreover, if possible, the processing of those data should be pseudonymized and depseudonymized only if a risk of infringement to a law or a regulation that falls within the tasks of the FPS Finance exists.[32]

Regarding data mining operations in the data warehouse, Article 5 of the Law of 3 August 2012 provides that the FPS Finance can use "data collected to execute its legal missions." These are notably data collected from people's and undertakings' tax declarations, from the newspapers, from their own

[26] Art. 52 of the GDPR; Loi du 5 septembre 2018 instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, *M.B.*, 10 septembre 2018, arts. 3 and 5.

[27] See https://ec.europa.eu/commission/presscorner/detail/en/inf_21_2743; https://www.archyde.com/european-commission-gives-belgium-two-months-to-restore-independence-to-oda/; https://www.archyde.com/mathieu-michel-invites-the-federal-parliament-to-assume-its-responsibilities-in-the-apd-file-a-highly-problematic-situation/; https://plus.lesoir.be/376968/article/2021-06-08/vie-privee-la-commission-lance-une-procedure-dinfraction-au-rgpd-contre-la.

[28] Article 20.1 of the Law of 30 July 2018.

[29] Art. 5bis, al. 4 of the Law of 15 January 1990, inserted by art. 12 of the Law of 5 September 2018.

[30] Art. 4, al.1 of the Law of 3 August 2012, as modified by Art. 70 of the Law of 5 September 2018.

[31] Art. 4, al.2 of the Law of 3 August 2012, as modified by Art. 70 of the Law of 5 September 2018.

[32] Art. 5, §2, al. 1 and 2 of the Law of 3 August 2012, as modified by Art. 71 of the Law of 5 September 2018.

https://doi.org/10.1017/dap.2022.6 Published online by Cambridge University Press

experience, from whistle-blowers and from outputs of investigations. In fact, the Tax Code mentions that investigators can collect "any books and documents,"[33] which includes the commercial correspondence (such as emails, etc.), and that the information that is discovered through that means may be invoked for the tracing of any sum due under the tax laws.[34] However, when e-mails boxes are concerned, this must be balanced with the right to protection of correspondence.

Once again, the critique formulated by Degrave and Lachapelle (2014) and De Raedt (2017) regarding the previous version of Article 5, namely that the types of data that could be used were defined too broadly, as it provided that the FPS Finance can use, via the data warehouse, any "data collected in order to execute its legal missions," have not been addressed in the 2018 modification either, as the same terminology has been kept. This might be problematic from a data minimization perspective. However, this concern is somewhat alleviated by the fact that, as outlined above, a DAM fiche must be completed and submitted to the President of the Executive Committee. This constrains the data that data miners can access for a specific project. This is a pragmatic solution, as it would be very difficult for the legislator to pre-define all the types of data that could be processed in this regard. Moreover, the technical access to the data warehouse is built in such a way that the agents of the FPS Finances can only access the electronic records, data, or applications that are adequate, relevant, and nonexcessive in light of the execution of the tasks that fall within their legal missions,[35] and this can be checked through access logs. These logs are necessary to allow third-party auditing (e.g., by the Data Protection Authority) of the process.

Data minimization requirements are also important at the e-auditing phase (i.e., during the concrete investigation). The inspectors can only collect data related to the tax issue from the suspect's computer, and have to avoid collecting any data pertaining to the suspect's private life. Making this selection is time-consuming and this is an issue as they often have a limited time to collect these data. In cases where investigators run out of time and have to copy data whose relevance could not be verified on the spot, they will self-censure themselves later on and refrain from using data that are irrelevant for the investigation regarding the suspect's right to privacy. Furthermore, they face privacy limitations in accessing suspects' data stored in the cloud or on their smartphones and accessing potentially useful data held by third parties such as SSIs. As regarding jurisdictional limitations, the Belgian Income Tax Code states that the administration has the right to request the communication of data digitally located in Belgium or abroad.[36]

Whether at the data collection, data mining, or at the e-auditing stage, the key is thus to be proportionate in the types of data collected and used. Even if they could potentially have access to troves of data, a balance must be found with the citizens' privacy and data protection, but also with commercial and professional secrecy requirements. This creates internal discussions about how much data they capture and how much data they may ask for in a timely manner. This is the second challenge: "*Challenge 2: Balancing data minimization with timely access to relevant data sources.*"

Regarding data matching operations to fight against social security infringements, they must be subject to a data transfer protocol or to a prior deliberation of the ISC. In this regard, the SSIs must identify the data that are necessary and adequate for the data matching purpose they pursue. The key is to be proportionate. For instance, one SSI entered a request to obtain the IP addresses of the people applying for an allowance to determine whether they were in Belgium or abroad (in which case they are not entitled to receive it, because they have to live in Belgium), but this was refused as it was disproportionate.

Regarding the data mining operations conducted in the OASIS database, Art 5*bis* of the Law of 15 January 1990, inserted in 2018, provides that "all the necessary data for the purposes of applying the labor law and social security legislation" can be used. According to Degrave (2020b), this definition may be too broad as it does not allow the citizens to know exactly which types of data are (or can be) processed. However, this concern is somewhat alleviated by the fact that access to data from the data warehouse must

[33] C.I.R. 92, art. 318.
[34] C.I.R. 92, art. 336.
[35] Art. 10.1 of the Law of 3 August 2012.
[36] C.I.R. 92, art. 315*bis*, al. 6.

https://doi.org/10.1017/dap.2022.6 Published online by Cambridge University Press

be subject to a data transfer protocol[37] or to a prior deliberation of the ISC,[38] in which the necessary and proportionate nature of the accessed data will be controlled (see Section 4.2.1).

Moreover, the data minimization principle is enshrined in the fact that the data warehouse solely contains pseudonymized data and that it can only be accessed by a limited number of data miners/investigators. Importantly, the people who pseudonymize the data to be uploaded in the data warehouse and suggest fraud indicators are not the same as those who use the data warehouse in order to spot fraudulent patterns based on those indicators. In practice, the SSIs shall draw up a list of the categories of persons having access to the personal data in the data warehouse, with a description of their role in relation to the data processing in question, and this list shall be kept at the disposal of the Data Protection Authority.[39] It is only once these data miners/investigators have identified a potential fraudulent case on the basis of determined indicators that the data at hand is depseudonymized, following a risk analysis, and extracted from the data warehouse, in order to start an investigation assessing whether there is a fraud or not.

#### *4.2.3. Special categories of data and data relating to criminal convictions and offenses (LR3)*

The processing of "special categories of data" (Art. 9, GDPR), such as health-related data, and of data relating to criminal convictions and offenses (Art. 10, GDPR) is subjected to stricter rules. Importantly, some forms of fraud analytics might blur the lines between "special categories of data" and "regular" personal data (De Raedt, 2017. An analysis merely relying on and addressing "regular" data can quite quickly end up pertaining to "special categories of data" (Rouvroy, 2016). Moreover, some fraud analytics data can be considered as data relating to criminal convictions and offenses (but it must also be noted that even without this fraud analytics, tax authorities have access to those data (De Raedt, 2017).

In practice, these specificities will be addressed either in the DAM fiche or in the authorization request to the President of the Executive Committee of the FPS Finance, for the tax fraud case study; and either in the request for a prior deliberation of the ISC or in the data transfer protocol for the social security infringements case study.

#### *4.2.4. Right to information, fairness, and transparency (LR4)*

As a rule of thumb, any fraud analytics processing must be fair and transparent, and the data subjects must be informed about it. Fairness implies that, as mentioned in Section 2.2, the laws on which this processing is based must be sufficiently explicit and understandable for the data subjects. They cannot be taken by surprise. For both case studies, citizens are generally informed about the existence of data matching and data mining operations through the laws mentioned above. Yet, according to Degrave and Lachapelle (2014), De Raedt (2017), and Degrave (2020b), these laws do not provide sufficiently clear information to the citizens, notably in terms of the concrete processing that will be conducted and in terms of the types of data that will be used (see Sections 4.2.1 and 4.2.2).

To some extent, this lack of transparency is reduced by the fact that these concrete data processing will be subject to a DAM fiche, to an authorization from the President of the Executive Committee of the FPS Finance, to a prior deliberation of the ISC or to the conclusion of a data transfer protocol, which will provide more specific information. However, citizens do not have access to the DAM fiches or to the authorizations of the President of the Executive Committee. Moreover, while the deliberations of the ISC are published on the website of the CBSS,[40] it is hard to obtain information about specific processing, as the search tool is quite basic. In a similar vein, as the data transfer protocols have to be published on the websites of the relevant data controllers,[41] this leads to a diluted publication on a wide variety of websites,

[37] Art. 20.1 of the Law of 30 July 2018.
[38] Arts. 5*bis*, al.7 (inserted by art. 12 of the Law of 5 September 2018) and 15 of the Law of 15 January 1990.
[39] Art. 5*bis*, al. 5 of the Law of 15 January 1990, inserted by art. 12 of the Law of 5 September 2018.
[40] https://www.ksz-bcss.fgov.be/fr/deliberations-csi-list?term_node_tid_depth=51.
[41] Art. 20.3 of the Law of 30 July 2018.

https://doi.org/10.1017/dap.2022.6 Published online by Cambridge University Press

whose quality can strongly vary. This makes it almost impossible for citizens to have a good overview of the types of processing conducted with their data. This constitutes the third challenge: "*Challenge 3: Facilitating the access to information about fraud analytics for citizens.*"

Regarding the tax fraud case study, it is also worth mentioning that this right to information, as well as the other data subject rights, can be delayed, limited, or excluded, with regard to the processing of personal data for which the FPS Finances is the data controller, to guarantee public interest objectives in the budgetary, monetary and fiscal field.[42] This is an application of Article 23 of the GDPR, mentioned above (see Section 2.2). The goal is to avoid a citizen suspected of committing tax fraud using this information in order to prejudice the investigation and to escape a sentence.

Finally, it should be outlined that, for both case studies, a person or an undertaking will not be informed that it has been flagged as being a potential fraudster following data mining operations conducted in the data warehouse, if the follow-up investigation did not result in the finding of fraud. Consequently, this person/undertaking might repeatedly be flagged as "suspicious," although erroneously, without being able to do anything about it, since it is not aware of it. However, since the investigators give feedback to data miners on the "fraud signals" that were the result of the data mining, false signals should rapidly be discarded.

#### *4.2.5. Right of access (LR5)*

For both case studies, interviewees mentioned that they very rarely receive access requests from data subjects. However, in the context of our interviews relating to the upcoming big data analytics platform in the field of social security, it was outlined that it would be built in a way to anticipate the answer to access requests by data subjects. The platform will keep detailed logs about data access with related persons requesting the access, concerned SSI, and related purpose. Moreover, this right of access can be delayed, limited, or excluded from the tax fraud case study (see Section 4.2.4).[43]

#### *4.2.6. Right to erasure (LR6)*

For both case studies, personal data resulting from processing operations in the data warehouse shall be kept for no longer than is necessary for the purposes for which they are processed, with a maximal retention period defined by law (see Section 4.2.1). Once this purpose is achieved, the data must be deleted. In parallel, citizens also have a right to erasure (Art. 17, GDPR), but, for the tax fraud case study, this right can be delayed, limited, or excluded (see Section 4.2.4).[44]

#### *4.2.7. Right to nonsolely automated decision-making and right to human public services (LR7)*

For the tax fraud case study, humans play an important role in the preinvestigation and investigation stages. For instance, human controllers have first established a set of typologies (types of suspicious profiles they want to detect) and use analytics to support detecting them. The indicators used to identify these typologies are either proposed by humans or by the machine, which will propose a predictive shortlist of profiles that strongly correspond to the typology that the investigators are looking for. To this effect, the machine will identify the most effective factors to detect these typologies, but the final decision to investigate (or not) a profile remains in the hand of the human controller. In fact, the investigators will often not investigate all suspicious cases identified in the preinvestigation. Rather, they will test some of these and will provide feedback on the usefulness of the signals at the end of the investigation. If the signals are relevant, they will investigate more cases from the suggested list. Data mining is thus just the

[42] Arts. 11.1, al.1; 11/1.1, al.1; 11/2.1, al.1; and 11/3.1, al.1 of the Law of 3 August 2012, as modified by Art. 81 of the Law of 5 September 2018.

[43] Arts. 11.1, al.1; 11/1.1, al.1; 11/2.1, al.1; and 11/3.1, al.1 of the Law of 3 August 2012, as modified by Art. 81 of the Law of 5 September 2018.

[44] Arts. 11.1, al.1; 11/1.1, al.1; 11/2.1, al.1; and 11/3.1, al.1 of the Law of 3 August 2012, as modified by Art. 81 of the Law of 5 September 2018.

https://doi.org/10.1017/dap.2022.6 Published online by Cambridge University Press

very beginning of the process, and does not suffice on its own to establish fraud. Additionally, for some types of frauds such as those linked to "direct income taxes," the cases that are investigated following a data mining recommendation are relatively small compared to the cases that controllers investigate on their own initiatives (about 20%). Data mining is, however, extremely important for, and well suited to, other specific types of frauds (such as VAT fraud where about 80% of the cases derive from data mining).

Regarding the social security infringements case study, a distinction must be made between bilateral cross-checks relying on data matching, and data mining operations conducted in the OASIS data warehouse. For the former, some forms of ex ante data matching cross-checks (e.g., checks before the social allocation is paid) do not imply a human intervention and are fully automated. This is because they are used to identify objective obstacles to the payment of the allowances (e.g., no unemployment benefit if a person has a professional income). It is thus not a matter of interpretation, as there is no flexibility for the machine. This could easily be reviewed by a human, if requested by a data subject. Ex post data matching cross-checks, on the other hand, always imply human verification. It is necessary for them to hear the person and ensure the rights of defense before taking a decision. This makes it possible to find cases that have escaped the ex ante cross-checks. All these ex post cross-checks are justified by a decision in due form with legal and factual justification, which can give rise to complaints to the ombudsman and appeals. A machine never takes final decisions and there is always human control. There is no total automaticity or blind trust in the results of the data mining for data mining operations. With its greater calculation power, the machine allows to browse the broad quantities of data faster to identify fraud indicators, but these are merely suggestions of cases to investigate. The concrete investigation, on the other hand, will always be done by a human. Moreover, the indicators integrated in OASIS have, in fact, been suggested by humans, namely inspectors on the field, who translate their experience of the cases they investigated in indicators. The machine simply looks for those indicators in a large amount of data.

It thus seems that humans have an important role in the two case studies. However, there is no transparency on that from public authorities toward the public and this is a real problem. As a consequence, one must be careful with the hereabove statements. Moreover, even if humans are involved in the process, the extent of involvement must be questioned. The introduction of negligible human intervention should not be such as to avoid the application of the guarantees contained in Article 22 GDPR.

For both case studies, as also underlined by De Raedt (2017), Scarcella (2019), and Degrave (2020b), even if the machine does not itself decide that a person is a fraudster, the decision to identify a person as "suspicious" could, in and of itself, be qualified as a solely automated decision producing legal effects for this person (i.e., the opening of an investigation). If this interpretation is followed, this would require implementing appropriate safeguards, such as the right to obtain a human intervention (Art. 22.3, GDPR), but also the right to obtain an explanation on how the decision was reached. This right is intrinsically included in the data subject's right to information as well as his or her right of access (art. 13–15 GDPR).[45]

Moreover, questions could be raised about whether the human intervention remains sufficient, especially if the controllers do not question the fraud inspection suggestions they receive, as they completely rely on the machines to determine the cases to be investigated. For instance, in the specific field of customs frauds, while some fraud indicators result from human knowledge, there is also an automated model that analyses all of the feedback from the controllers on a continuous basis and updates itself every day. Based on these updates, it will produce hundreds of updated selection rules every day to determine which goods/undertakings should be controlled. Therefore, only the feedbacks are provided by

[45] According to Wachter et al. (2017), a right to obtain explanation of automated decision-making does not exist in the GDPR. However, we tend not to agree with this position because such a right is derived from articles 13 to 15 GDPR. According to those articles, the data subjects have the right to access and receive information about the logic involved as well as the significance and the envisaged consequences of the processing for them. Additionally, as long as the explanation of the logic must be given to a data subject having regard to a decision concerning him or her, the level of the explanation should not be general, but individualized. Therefore, it is not necessary to make a distinction between the "decision" and the "logic involved": such difference exists per se regarding the context in which the explanation must be given (i.e., toward a decision concerning a data subject).

https://doi.org/10.1017/dap.2022.6 Published online by Cambridge University Press

humans, not the rules inferred from them. In such cases, it is fundamental to ensure that the inspectors keep collaborating by giving feedback on those newly suggested indicators, rather than simply applying what the AI suggests, without any critical thinking. For instance, in the customs frauds example, feedback will be provided by the controllers, which implies that a human will assess the recommendations made by the machine, putting back human control in the process. Yet, looking toward the future, it is possible that, in light of the constant budget cuts and reductions of personnel, there is a risk that the few inspectors left will simply end up trusting the machine without any critical thinking, because they have to meet their control quotas, and no longer have time to check the relevance of the indicators suggested by the machine. Such a scenario must be avoided. This constitutes the fourth challenge: "*Challenge 4: Ensuring a truly critical human check of quasi-automated decisions.*"

#### *4.2.8. Equal access to public services (LR8)*

For the tax fraud case study, data quality checks are performed in the data warehouse, in order to ensure that the data is not biased at the application level and does not lead to discrimination. Several data mining projects pursued by the data miners solely aim at improving and ensuring data quality.

For the social security case study, it was highlighted that regular bias detection checks will need to be taken in the building of the data mining models to ensure fairness and the use of nonbiased and relevant data. We can only assume that any risk of inequality is discarded at the stage of the drafting of the data transfer protocol or at the stage of the obtention of the prior authorization from the ISC. However, due to the relative opacity in this regard, the existence of inequalities and discriminations cannot be excluded.

#### *4.2.9. Explainability (LR9)*

For the tax fraud case study, interviewees mentioned that they do not work with black-boxes, because they need to be able to explain their path and why a certain person or company is suspected of tax fraud.[46] For each case, the data miners are able to explain the reasoning behind the detection (indicators, techniques applied, etc.). As a consequence, the analytics used are qualified as "simple but effective" by data miners as the queries to detect fraud typologies are developed by controllers. Even most advanced techniques, such as social network analysis, used to detect more complex fraud types (e.g., "domino bankruptcies") are designed by the data miners. However, it should be mentioned that, when investigating a specific case, controllers can rely on AI techniques delivered by private software companies. The functioning of this AI software is somewhat of a black box for the tax investigators, but, according to them, they can solicit an explanation from the private company and the latter will likely reply, as they want to keep them as customers. However, it cannot be excluded that these private companies might hide behind commercial secrecy to refuse to provide such an explanation, and this should be a key point of attention when dealing with those software providers.

Regarding the social security infringements case study, even if the bilateral ex ante cross-checks relying on data matching are fully automated, they remain explainable because they are used to identify objective obstacles to the payment of the allowances. The machine thus does not have any margin of interpretation. Regarding bilateral ex post cross-checks relying on data matching, their results are also explainable, since they always imply a human verification. Similarly, the results of the data mining operations conducted in the data warehouse are also explainable, since the indicators that are used to pinpoint suspicious cases have, in fact, been suggested by humans (the data miners). In the future, as the frauds become more and more complex, the use of simpler algorithms with explainable business rules can become an issue, especially if there is a lack of in-house advanced analytics solutions, leading to the need to resort to private sector providers. This is the fifth challenge: "*Challenge 5: Develop in-house explainable advanced analytics solutions to detect complex frauds.*"

Finally, it should be reminded that, for both case studies, a person or undertaking will not receive an explanation about why it has been flagged as "suspicious" if the following investigation does not lead to the finding of fraud. In the same vein, it appeared from the interviews pertaining to tax fraud that, for cases

[46] However, as there is no transparency on that from public authorities, one must be careful with this declaration.

https://doi.org/10.1017/dap.2022.6 Published online by Cambridge University Press

that are investigated following a data mining recommendation, the "suspects" rarely ask for explanations as to why they have been flagged by the data mining process in the first place, but rather ask explanations about how the tax administration has established the concrete amount of tax that they are claiming on the basis of their e-auditing (e.g., text mining of the data and files collected during the investigation). However, this could change in the future and it is important for the tax administration to anticipate this need to explain the results of the data mining process. Similarly, in the social security case study, it was highlighted that it is complex to find a balance between being fully transparent and explaining the data mining processes and models used, and the need to not disclose their fraud analytics processes, as otherwise the fraudsters will adapt and avoid being detected. So even if they can explain their decision, the challenge is to determine when and how they should do it. This is the sixth challenge: "*Challenge 6: Balancing explainability with the need to ensure the confidentiality of fraud analytics process.*"

## 5. Discussion: Theoretical and Practical Implications

Table 2 summarizes the governance practices observed from the two cases for legally compliant governance of fraud analytics. These practices are relevant for researchers and policy practitioners as they are empirically validated and also provide concrete implementation of legal requirements. Furthermore, Table 2 highlights the theoretical contributions of this study by presenting the new findings elicited through the cases.

These practices are also consistent with previous research examining the impact of the GDPR and other legal requirements on advanced analytics (big data analytics, AI-based techniques, etc.) such as Kemp (2014), Gruschka et al. (2019), Bibal et al. (2020), Degrave (2020a), and Janssen et al. (2020), which we integrate and extend in this article. However, some elements in this study provide new insights and concrete implementations of general good practice simply mentioned in the cited papers. Hence, our research has resulted in a more detailed and comprehensive overview. For instance, the network structure for data sharing between the SSIs can be considered as a concrete illustration of the distributed governance advocated by Janssen et al. (2020). Another example resides in the simpler analytics used by data miners to ensure the need for explainability, studied from a technical perspective in Bibal et al. (2020). A final example relates to the generic risk analysis principle suggested by Kemp (2014), which is implemented, here, at the process (limitation of access, depseudonymization risk analysis) and organizational (Privacy committee) levels. We can thus argue that these practices can be useful for any organization wishing to engage in fraud analytics and to consider these legal requirements.

These findings also have direct practical implications as diverse solution directions can be identified to overcome the aforementioned challenges. We hereunder suggest examples of ways forward for three challenges:

- Challenge 1: to ensure reactivity to frauds while respecting purpose limitation (LR1), the data processing authorization request could be slightly broader at first, and then refined continuously throughout the process, via close collaboration between legal services and data miners following agile analytics principles as suggested in Earley (2014). Another solution direction would be to anonymize, or at least pseudonymize, the data warehouse data on which the data mining analysis is done, and to only allow the reidentification of the data subjects in the context of a concrete human-led investigation. This would ensure privacy-by-design and privacy-by-default (Art. 25, GDPR) and can prevent data processing mistakes.
- Challenge 3: for the facilitation of access to information (LR4), a solution would be to centralize the publication of all of the data transfer protocols in a single source, such as the Data Protection Authority's website, as suggested in Degrave (2020a). A good example of this is the city of Amsterdam's "Algorithm register."[47] Moreover, it should be possible to search through this single

[47] https://algoritmeregister.amsterdam.nl/en/ai-register/.

https://doi.org/10.1017/dap.2022.6 Published online by Cambridge University Press

***Table 2.*** *Summary of practices identified in the cases for Legally Compliant Governance of fraud analytics*

| Observed governance practices for Legally Compliant fraud analytics | Case 1 (Tax Fraud) | Case 2 (Social Security Fraud) | Related Legal Requirements (LR) | Related challenges | Related literature |
|---|---|---|---|---|---|
| 1. Perform continuous data relevance checks | X | | LR1 | Challenge 1 | New finding |
| 2. Limit the access to data before analytics phase | | X | LR1, LR2, LR3 | Challenges 1 and 2 | Janssen et al. (2020) |
| 3. Create a Privacy Committee to authorize access | X | X | LR1, LR2, LR3 | Challenges 1 and 2 | Kemp (2014) |
| 4. Establish maximal retention period in data warehouse | X | X | LR1, LR6 | Challenge 1 | Gruschka et al. (2019) |
| 5. Pseudonymize the data in data warehouse before analytics | | X | LR2 | Challenge 2 | Gruschka et al. (2019) |
| 6. Perform risk analysis before depseudonymization | | X | LR2 | Challenge 2 | Kemp (2014) |
| 7. Monitor the access to the data warehouse manually or through Text Mining | X | X | LR2 | Challenge 2 | New finding |
| 8. Organize and request audits by external organizations | X | | LR2 | Challenge 2 | New finding |
| 9. Create a network structure for data sharing | | X | LR2 | Challenge 2 | Janssen et al. (2020) |
| 10. Limit the possible data sources | X | X | LR2, LR3 | Challenge 2 | Janssen et al. (2020) |
| 11. Centralize publications of authorizations for fraud analytics and allow detailed search | X | X | LR4 | Challenge 3 | Degrave (2020a) |
| 12. Anticipate and prepare access requests | X | X | LR5 | / | Janssen et al. (2020) |
| 13. Keep humans in the loop and ensure critical human checks | X | X | LR7 | Challenge 4 | Bibal et al. (2020) |
| 14. Perform continuous data quality and biases checks | | X | LR8 | / | Janssen et al. (2020) |
| 15. Use simpler and effective analytics to ensure explainability | X | X | LR9 | Challenges 5 and 6 | New finding |

source, as well as through the ISC's deliberations on the CBSS website, on the basis of several criteria, such as the types of purposes or of data concerned.
– Challenge 5: to ensure explainability (LR9) with advanced analytics, the use of open-source software providers should be examined. Another solution would be to resort to explainable AI techniques in the fraud detection domain which is currently underinvestigated (Gade et al., 2019). A final solution direction resides in the use of heterogeneous techniques to ensure the explainability about the detection of cases to investigate, while experimenting with more advanced techniques for the investigation of a specific case.

## 6. Conclusion, Limitations, and Future Research

Fraud analytics refers to the use of advanced analytics, based on big data or AI-based techniques, to detect fraud. However, the concrete way in which public administrations have integrated legal requirements and adapted their governance remains unexplored. Our study has two main contributions in that regard. First, through the extensive examination of two case studies, this article shows the complexity of this implementation by examining how the Belgian tax and social security public administrations have implemented, in practice, the main data protection law and administrative law requirements in their fraud analytics processes. The findings are summarized as 15 governance practices. Second, it has clearly outlined the main challenges for a legally compliant fraud analytics process, and opens avenues for practitioners and future researchers to tackle them in the future. These challenges highlight the necessary trade-offs to balance advanced analytics with legal requirements and are the following:

1. Ensuring reactivity to frauds while respecting purpose limitation;
2. Balancing data minimization with timely access to relevant data sources;
3. Facilitating the access to information about fraud analytics for citizens;
4. Ensuring a truly critical human check of quasi-automated decisions;
5. Develop in-house explainable advanced analytics solutions to detect complex frauds;
6. Balancing explainability with the need to ensure the confidentiality of fraud analytics process.

This research has some inherent limitations that introduce avenues for further research. First, in order to improve the internal validity of our case study approach, onsite examination of the processes was impossible but would have delivered complementary insights. Focus groups are also a complementary data collection method, which would deliver more fine-grained insights about the identified challenges and elicit innovative leads for solutions. We recommend that the interested future researchers organize focus groups to elicit those leads for solutions. Moreover, we recommend that creativity techniques are used to foster the elicitation of ideas from practitioners (Mahaux et al., 2013). Second, in order to improve the external validity of our approach, we strongly encourage future researchers to use the legal requirements of this study as a theoretical lens to examine the fraud analytics process in other countries. Ultimately, this further research can lead to the formalization of a fraud analytics process considering the legal requirements, with several alternative solutions for practitioners to select from depending on several factors (analytics used, organizational structure, etc.). Third, to improve our external validity, we recommend extending our case study database and developing a user interface to extract relevant insights from it, linked to the suggested formalized process. This would constitute an innovative research data management that would be valuable for researchers and practitioners wanting to access information.

**Acknowledgments.** This article is an extended version of the "Artificial Intelligence and Big Data in Fraud Analytics: Identifying the Main Data Protection Challenges for Public Administrations," paper presented at the 2021 Data for Policy conference (DOI:10.5281/zenodo.5205519).

**Funding Statement.** We would like to acknowledge the Belgian Federal Science Policy Office (BELSPO) for their support. The research pertaining to these results received financial aid from the Federal Science Policy according to the agreement of subsidy no. B2/191/P3/DIGI4FED.

**Competing Interests.** The authors declare no competing interests exist.

**Author Contributions.** Conceptualization: A.S., T.T., M.J.; Investigation: T.T.; Methodology: A.S., T.T.; Project administration: A.S., C.D.T., B.F.; Supervision: C.D.T., B.F., M.J.; Writing—original draft: A.S., T.T.; Writing—review and editing: A.S., T.T., C.D.T., P.W., B.F., M.J.

**Data Availability Statement.** The methodological material that was used to derive the findings of this study is openly available in Zenodo at the following link: https://zenodo.org/record/4572708#.YbDKd9DMI2w.

## References

**Anderson R** (2007) *Thematic Content Analysis (TCA): Descriptive Presentation of Qualitative Data Using Microsoft Word.* Descriptive Presentation of Qualitative Data, pp. 1–4.

**Baarda B**, **Dirk B**, **Goede MPM**, **de Matthëus PM and van der Meer-Middelburg AGE** (1996) *Basisboek Open Interviewen: Praktische Handleiding voor het Voorbereiden en Afnemen Van Open Interviews [Book about Basics Open Interviewing: A Practical Guidance for Preparing and Conducting Open Interviews]*. Groningen: Stenfert Kroese.

**Baesens B**, **Van Vlasselaer V and Verbeke W** (2015) *Fraud Analytics Using Descriptive, Predictive, and Social Network Techniques*. Hoboken, NJ: Wiley. http://doi.org/10.1002/9781119146841

**Bibal A**, **Lognoul M**, **de Streel A and Frénay B** (2020) Legal requirements on explainability in machine learning. *Artificial Intelligence and Law 29*, 149–169. http://doi.org/10.1007/s10506-020-09270-4

**Boyce C and Neale P** (2006) Conducting in-depth interviews: A guide for designing and conducting in-depth interviews. *Evaluation 2*, 1–16.

**Castellón González P and Velásquez JD** (2013) Characterization and detection of taxpayers with false invoices using data mining techniques. *Expert Systems with Applications 40*, 1427–1436. https://doi.org/10.1016/j.eswa.2012.08.051

**Council of Europe** (2020) *Recommendation CM/Rec(2020)1 of the Committee of Ministers to Member States on the Human Rights Impacts of Algorithmic Systems.* Available at https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154. (accessed 10th of Ferbruary 2022).

**De Raedt S** (2017) *The Impact of the GDPR for Tax Authorities*. Gent: R.D.T.I, pp. 66–67.

**De Raedt S and Lachapelle A** (2018) *National Report of Belgium: EATLP Annual Congress – Tax Transparency.* Available at http://www.crid.be/pdf/public/8235.pdf (accessed 10 Ferbruary 2022).

**De Roux D**, **Pérez B**, **Moreno A**, **Del Pilar Villamil M and Figueroa C** (2018) Tax fraud detection for under-reporting declarations using an unsupervised machine learning approach. In *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. New York, USA: Association for Computing Machinery. http://doi.org/10.1145/3219819.3219878

**Degrave E** (2020a) Le R.G.P.D., les lois belges et le secteur public: Les traitements de données dans l'administration en réseaux et l'Autorité de protection des données. *Le Règlement Général Sur La Protection Des Données (R.G.P.D./G.D.P.R.): Premières Applications et Analyse Sectorielle 195*, 299.

**Degrave E** (2020b) The use of secret algorithms to combat social fraud in Belgium. *European Review of Digital Administration & Law 1*(1–2), 167–177.

**Degrave E and Lachapelle A** (2014) *Le droit d'accès du contribuable à ses données à caractère personnel et la lutte contre la fraude fiscale. Note Sous C.C., 27 Mars 2014, N°2014/28, R.G.F.C., 2014/5*, pp. 322–335.

**Earley S** (2014) Agile analytics in the age of big data. *IT Professional 16*(4), 18–20.

**Felzmann H**, **Villaronga EF**, **Lutz C and Tamò-Larrieux A** (2019) Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns. *Big Data and Society 6*, 1–14. http://doi.org/10.1177/2053951719860542

**Gade K**, **Geyik SC**, **Kenthapadi K**, **Mithal V and Taly A** (2019) Explainable AI in industry. In *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, New York, USA: Association for Computing Machinery pp. 3203–3204.

**Gal U**, **Jensen TB and Stein MK** (2020) Breaking the vicious cycle of algorithmic management: A virtue ethics approach to people analytics. *Information and Organization 30*(2), 100301. http://doi.org/10.1016/j.infoandorg.2020.100301

**Gérard L** (2017) Robotisation des services publics: l'intelligence artificielle peut-elle s'immiscer sans heurt dans nos administrations. In *L'Intelligence Artificielle et le Droit*. Namur: Larcier.

**Gruschka N**, **Mavroeidis V**, **Vishi K and Jensen M** (2019) Privacy issues and data protection in big data: A case study analysis under GDPR. In *Proceedings - 2018 IEEE International Conference on Big Data, Big Data 2018*. Seattle, USA: IEEE http://doi.org/10.1109/BigData.2018.8622621

**Guest G**, **Bunce A and Johnson L** (2006) How many interviews are enough?: An experiment with data saturation and variability. *Field Methods 18*(1), 59–82.

**Hildebrandt M** (2019) Privacy as protection of the incomputable self: From agnostic to agonistic machine learning. *Theoretical Inquiries in Law 20*(1), 83–121.

**IOTA** (2018) *Impact of Digitalisation on the Transformation of Tax Administrations.* Available at https://www.iota-tax.org/sites/default/files/publications/public_files/impact-of-digitalisation-online-final.pdf (accessed 10 Ferbruary 2022).

**Janssen M**, **Brous P**, **Estevez E**, **Barbosa LS and Janowski T** (2020) Data governance: Organizing data for trustworthy artificial intelligence. *Government Information Quarterly 37*, 101493. http://doi.org/10.1016/j.giq.2020.101493

**Johnson SL**, **Gray P and Sarker S** (2019) Revisiting IS research practice in the era of big data. *Information and Organization 29*(1), 41–56.

**Kemp R** (2014) Legal aspects of managing big data. *Computer Law and Security Review 30*, 482–491. http://doi.org/10.1016/j.clsr.2014.07.006

**Klievink B**, **Romijn BJ**, **Cunningham S and de Bruijn H** (2017) Big data in the public sector: Uncertainties and readiness. *Information Systems Frontiers 19*(2), 267–283.

**Koutra D**, **Ke TY**, **Kang U**, **Chau DH**, **Pao HKK and Faloutsos C** (2011) Unifying guilt-by-association approaches: Theorems and fast algorithms. In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. http://doi.org/10.1007/978-3-642-23783-6_16

**Lachapelle A** (2016) Le respect du droit à la vie privée dans les traitements d'informations à des fins fiscales: état des lieux de la jurisprudence européenne. *R.G.F.C.P., 2016/9*, pp. 24–37, 44–65.

**Mahaux M**, **Nguyen L**, **Gotel O**, **Mich L**, **Mavin A and Schmid K** (2013) Collaborative creativity in requirements engineering: Analysis and practical advice. In *Proceedings - International Conference on Research Challenges in Information Science*, Paris, France: IEEE pp. 1–10.

**Mayer-Schönberger V and Padova Y** (2016) Regime change? Enabling big data through Europe's new data protection regulation. *Columbia Science & Technology Law Review 17*, 315.

**Mayring P** (2004) Qualitative content analysis. *A Companion to Qualitative Research 1*(2), 159–176.

**OECD** (2016) *Advanced Analytics for Better Tax Administration: Putting Data to Work.* Available at https://read.oecd-ilibrary.org/taxation/advanced-analytics-for-better-tax-administration_9789264256453-en (accessed 10 Ferbruary 2022)

**Pencheva I**, **Esteve M and Mikhaylov SJ** (2018) Big data and AI – A transformational shift for government: So, what next for research? *Public Policy and Administration 35*, 24–44. http://doi.org/10.1177/0952076718780537

**Rouvroy A** (2016) *Of Data and Men: Fundamental Rights and Freedoms in a World of Big Data*. Strasbourg: Council of Europe. Available at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a6020 (accessed 10 Ferbruary 2022).

**Scarcella L** (2019) Tax compliance and privacy rights in profiling and automated decision making. *Internet Policy Review 8*(4), 1–19.

**Van Vlasselaer V**, **Eliassi-Rad T**, **Akoglu L**, **Snoeck M and Baesens B** (2017) GOTCHA! Network-based fraud detection for social security fraud. *Management Science 63*, 2773–3145. http://doi.org/10.1287/mnsc.2016.2489

**Villaronga EF**, **Kieseberg P and Li T** (2018) Humans forget, machines remember: Artificial intelligence and the right to be forgotten. *Computer Law and Security Review 34*, 304–313.

**Wachter, S.**, **Mittelstadt, B.**, & **Floridi, L.** (2017). Why a right to explanation of automated decision-making does not exist in the general data protection regulation. *International Data Privacy Law*, *7*(2), 76–99.

**Winter JS and Davidson E** (2019) Big data governance of personal health information and challenges to contextual integrity. *Information Society 35*(1), 36–51.

**Yin RK** (2014) *Case Study Research: Design and Methods*, Vol. *26*. Thousand Oaks, CA: Sage. http://doi.org/10.1097/FCH.0b013e31822dda9e

**Yu F**, **Qin Z and Jia XL** (2003) Data mining application issues in fraudulent tax declaration detection. In *International Conference on Machine Learning and Cybernetics*. Xi'an, China: IEEE. http://doi.org/10.1109/icmlc.2003.1259872

**Zarsky T** (2017) Incompatible: The GDPR in the age of big data. *Seton Hall Law Review 47*, 995–1020.

**Cite this article: Simonofski A, Tombal T, De Terwangne C, Willem P, Frenay B and Janssen M** (2022). Balancing fraud analytics with legal requirements: Governance practices and trade-offs in public administrations. *Data & Policy*, 4: e14. doi:10.1017/dap.2022.6