*Journal of Infrastructure, Policy and Development* 2024, 8(6), 3072.
https://doi.org/10.24294/jipd.v8i6.3072

Article

# Privacy model for the development and implementation of regulatory technology (RegTech)

**Jawahitha Sarabdeen**

College of Law, Prince Sultan University, Riyadh 11586, Saudi Arabia
*** Corresponding author:** Jawahitha Sarabdeen, jsarabdeen@psu.edu.sa

**CITATION**

Sarabdeen J. (2024). Privacy model for the development and implementation of regulatory technology (RegTech). Journal of Infrastructure, Policy and Development. 8(6): 3072. https://doi.org/10.24294/jipd.v8i6.3072

**ARTICLE INFO**

Received: 23 October 2023
Accepted: 19 February 2024
Available online: 8 July 2024



**Abstract:** An unprecedented demand for accurate information and action moved the industry toward RegTech where computing, big data, and social and mobile technologies could help achieve the demand. With the introduction and adoption of RegTech, regulatory changes were introduced in some countries. Enhanced regulatory changes to ease the barriers to market entry, data protection, and payment systems were also introduced to ensure a smooth transition into RegTech. However, regulatory changes fell short of comprehensiveness to address all the issues related to RegTech's operation. This article is an attempt to devise a Privacy Model for RegTech so industries and regulators can protect the interests of various stakeholders. This model comprises four variables, and each variable consists of many items. The four variables are data protection, accountability, transparency, and organizational design. It is expected that the adoption of this Privacy Model will help industries and regulators embrace standards while being innovative in the development and use of RegTech.

**Keywords:** regulatory technology; privacy model; data privacy; accountability; transparency; organisational model

## 1. Introduction

Regulatory technology which is known as RegTech has been introduced to facilitate better compliance and monitoring of various businesses to meet regulatory requirements. Arner et al. (2017) had defined RegTech as the use of information technology in regulatory monitoring, reporting, and compliance. Clarke (2020) also explained RegTech as the use of technological applications to adopt and monitor regulatory activities. Bolton and Mintrom (2023) stated that RegTech could be considered as the technical solution or aid to manage regulatory issues or to develop and deliver solutions to manage regulatory issues. RegTech has been stretched to cover industries and government efforts to harness technical solutions for regulatory monitoring and enforcement. Hence RegTech could refer to the usage of information technology for monitoring, reporting, and compliance of regulatory requirements (Siering, 2022).

Digitalization of regulatory reporting and compliance provides agility in data connectivity from various technologies and allows quick data generation and configuration. Generally, the regulations establish the economic system vis-a-vis regulating industries and protecting consumers, to deter offences. The pre-RegTech mechanism on compliance and deterrence of crimes yielded less successful results. The efforts to control money laundering failed with less than one percent of financial crime being caught. The main reason for its failure was attributed to the failure to oversee the complex market and understand the data produced by linear old models'

technologies (Konina, 2020). This caused law enforcement and regulators to miss information regarding patterns of crime and failed to deter the commission of crimes or noncompliance and the risk associated with it. With the massive number of documents filed with the regulators and several activities carried out every day, coupled with the current technology, it became impossible to thoroughly eliminate crimes. The UK financial regulators in 2019 received about 65 billion pieces of information annually from the companies it oversaw, and documents were submitted for the different laws, regulations, and standards like financial reporting (e.g., FINREP) and prudential reporting (e.g., BASEL III). If they are not equipped with the appropriate technologies, regulators may overlook nuances from the information collected. With the introduction of RegTech which uses machine-learning and other advanced technologies for analysis, the situation changed for the better. Industries and regulators could better understand the patterns of crime and take necessary preventive measures. If the data shows a trigger, then regulators could unmask the data and act against the individual, or organizations involved. Similarly, it would also be able to prevent banned organizations from mushrooming again with a different identity (Barefoot, 2020). The RegTech is a potential tool for regulators to understand trading or other related behaviors and analyze the potential danger of certain types of behaviors for further regulatory investigation and enforcement. For example, trading activities before a merger or acquisition could be analyzed with available data on all trades to look for unusual trading activity (Eva and Anna Rose, 2019).

On the industry front, the increase in regulatory requirements and demand for operational transparency caused financial institutions to look for innovative technological tools which paved the way for RegTech. RegTech could monitor customer history, and current data along with customer activities using Big Data Analytics that can show insights from structured and unstructured data. These data could prevent suspicious transactions while meeting compliance requirements (Waye, 2019). RegTech could provide automation of operational activities that could compute and interpret results and show unanticipated risks. Big Data Analytics can demonstrate customer behavior and its impact on banks. Robotic Process Automation can help generate regulatory reports on the impact of corporate actions. Artificial Intelligence can display the weaknesses in the current system and help address them. Industries are currently using RegTech to identify relevant regulations, and the regulatory impact on businesses, collect data on business compliances, predict risks, and take measures to control them. RegTech has also been used for reporting. In the health sector, RegTech is used for diagnosing, planning treatment, and understanding the risks associated with the plan, training, and compliance.

RegTech could be used to create internal data from reports and incidents that could help predict the possibility of whistleblowing. Technology-generated whistleblowing is called “whistlebots” which can collect data, analyse, and prepare reports on any violation in the company (Brand, 2020). The automated and mechanized system of whistleblowing would stimulate transparency and accountability. It could be argued that there is a lack of empathy in automated mechanized systems like “whistle-bots” which will result in a lack of trust and cause discomfort among whistle-blowers to disclose serious corporate violations (Brand, 2020). However, the “whistlebots” appear to be the superior method as opposed to

traditional reporting mechanisms as confidentiality and accountability are maintained better.

Due to the advantages that RegTech provides to financial, health, and other industries, regulators in some countries are adopting RegTech. The challenge will be to ensure that the rules applied by the algorithms comply with the law and ethical principles. There should be human intervention in feeding accurate data and validating automated decisions. There should also be human involvement in interpreting and implementing actions based on the algorithm's decisions. The algorithm must be understood by the regulators so that their decision can be rationalized as it could affect the livelihood of individuals and organizations that have no access to data sources of algorithmic decision (Arner et al., 2017) Hence, the industries and the regulator besides complying with the laws, should follow certain privacy principles in the development and the use of RegTech so that individual's and organizations' interest could be protected.

Research gaps in the current literature include a lack of comprehensive studies on the privacy model for Regtech, insufficient exploration of possible models that could be applied for RegTech development and application, and a limited understanding of Regtech use that necessitates the need for the research on possible privacy model for RegTech. Thus, this study contributes to extending the existing theoretical insights to develop a theoretical model for the protection of privacy in RegTech. It further identifies potential themes and variables for a framework for the privacy model. Firstly, with the potential of adopting RegTech in many industries, the privacy model will enhance the protection of data, efficiency, transparency, and accountability as such developing a privacy model as a guideline for development and adoption is timely. Secondly, the use of various technologies and the involvement of many stakeholders, devising or adopting a privacy model could ensure responsibilities and liabilities Hence, this research will assist in understanding the importance of privacy, adopting privacy protection requirements, avoiding associated risks, and addressing challenges.

## 2. Objective and methodology

The objective of this study is to develop a Privacy Model for RegTech development and application so that any privacy issues can be addressed in the early stage of the development of RegTech. The model could also serve as a guideline in meeting the legislative mandate. The Model is developed after analyzing literature on fields like law, ethics, technology, business, and engineering. It is expected that this model will facilitate the effective development and adoption of RegTech Technology that would help in reducing unethical behaviors and decision-making while controlling the unnecessary proliferation of similar models. This Privacy Model provides an overview of the variables and the items within each variable. The variables could be understood easily and adopted in the development and implementation of RegTech.

### Data extraction and data analysis

For the analysis, the databases were searched extensively till the year 2023 to collect data regarding Regtech and privacy. A systematic search was performed. The

review was conducted in phases (Loosman and Nickel, 2022; Moher et al., 2009; Sarabdeen, 2022). In the first phase, articles were collected from databases like Scopus, Web of Science, Lexis Nexis, and Google Scholar using terms or combinations of terms like "privacy model" "accountability" "privacy", "data protection" "laws", "Privacy" "IT and engineering" "organization design" and "organizational design and privacy model" were searched in all fields and date restrictions were not enforced. This meticulous process yielded the discovery of a total of 370 scholarly publications. The study employed criteria for inclusion, and a comprehensive search was subsequently conducted using the terms "privacy" and "RegTech/regulatory technology". This process yielded a selection of 123 scientific papers. In this process, scholarly literature that offers valuable perspectives was curtailed. The scope was refined to encompass articles published in the English language within the disciplines of law, business, information technology, finance, and management.

As a result, a total of 73 research were identified in the process only filters the researcher applied were "Article" and publication within the timeframe of 2017 to 2023. The search technique and criteria for source selection as mentioned in the literature ensure rigorousness and high quality (Khan et al., 2020). In the second phase of the analysis, the collected research materials were sorted, and abstracts were scanned for relevancy. If it was relevant, then full publications were logged. In the third phase, the relevant articles were read entirely to understand the concept and to include it as a variable or item of the variable.

In the final phase, the four variables: Data protection, accountability, transparency, and organizational design were derived. Along with the variables, the items within each variable were also finalized in this phase. The variables were selected based on a "keyword" search. These keywords, including data protection, accountability, transparency, organizational culture, and design have appeared frequently in the literature, indicating their importance.

Detailed manual reading of all 73 articles suggested that the literature is fixated on the four main themes: 1) Data Protection and RegTech Privacy Model; 2) Accountability and RegTech Privacy Model; 3) Transparency and RegTech Privacy Model; 4) Organisational Design and RegTech Privacy Model. the article discussed in detail the main themes. A few more literatures have been published in 2024 have been added to enhance the quality of the analysis. The process of collection of literature, review, and analysis is provided in **Figure 1**.

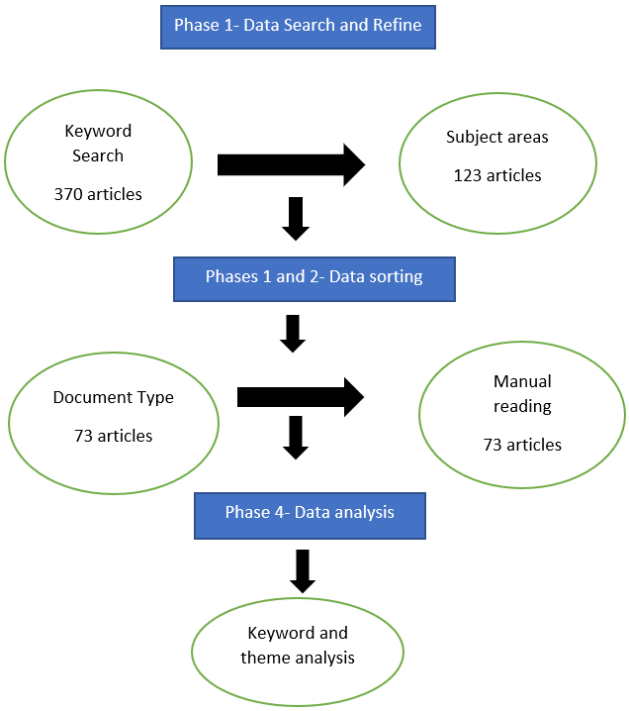


**Figure 1.** Data search and data analysis parameters.

## 3. The need for integrating privacy principles in RegTech

RegTech is currently used to control financial market manipulation and related behaviors, misconduct of insiders and to assess risk accurately (Waye, 2019). It is also used to collect intelligence and predict the occurrence of offense and the risk associated with it (Oswald et al., 2018). RegTech could easily be adopted as a subset of e-government to use for end-to-end approvals and monitoring. This could allow better interaction of personnel and other resources. RegTech can guide regulatory tracking and policy modeling. It could identify the relevant legislative text and its application to products and services. Furthermore, it could be used to scale the importance of provisions to firms, the critical factors in the provision, and predict regulator action or court decision depending on the violation of a specific provision (Fagan, 2016). RegTech provides the opportunity to assess large volumes of materials, with completeness as they are not affected by the capacity limit and are out of range of bias subjectivity by a human analyst. Such a result could provide legitimate motivations and reasoning for regulators to adopt RegTech on a large scale. In RegTech, predictive analysis using available data could interpret the data into various categories and map relationships between categories. The simulation could be drawn to predict behavior under certain conditions or parameters. The RegTech is currently capable of matching the legal text to logical rules for application.

The critics, however, argue that RegTech like any other technology, is not designed to understand the meaning of the data they process, thus they cannot be overly relied upon. The RegTech applications are developed to deal with routine, structured data, and may not be able to count for changes in the environment or capture the nuances of legal and policy intentions in totality (Remus and Levy, 2017). Therefore, they may find it difficult to take account of continuous changes in the environment. Moreover, the RegTech technologies cannot effectively deal with legal

ambiguity as they may not be able to capture the value of the rule of law and, the political and constitutional values of legislation or policy. They further argue that RegTech will not understand the purpose in totality and therefore unable to draw an analysis that will differentiate the importance according to the purpose of the legislation. Though the technology has its drawbacks, it will be able to provide insight into the efficacy of regulator activity, the application of fairness of the law, and the possible outcome of judicial or administrative decisions. However, the analysis of the data feed of RegTech technology is from various data, legal text, decisions, and the judgment of legal experts. There is a likelihood that the data feed provided is based on the needs, and the purpose of the users and may not be considered neutral which could affect the future use of the data. To achieve the best results, the development and adoption of RegTech should consider issues related to data protection, accountability, transparency, elimination of bias, and organizational design for agility.

### 3.1. Data protection as part of RegTech privacy model

In the use of RegTech, it is expected that data protection-related laws and ethical principles should be followed. The collection and processing of data should be done with consent as this practice could create trust and transparency among various stakeholders (Seebacher and Schüritz, 2017). Some users of RegTech use Cryptography in Blockchain to protect information privacy since each blockchain user has a public key and a private key to complete a transaction. The encrypted message sent using the public key is decrypted using the private key. The timestamp in the Blockchain provides the exact time of the transaction, and it is protected against modification (Tschorsch and Scheuermann, 2016). The Blockchain in RegTech, according to Benos et al. (2017) will reduce various costs of reconciliation and data management by creating a distributed, shared, and synchronized database. It could work as an automated clearing house without a middle person to ensure data protection. To use this technology, obtaining the consent of the users will be necessary (Bertino, 2019). The consent to technologies to collect and process personal data should be an informed consent that should include measures to protect the security of the data. In certain circumstances, an individual may not understand fully the consequence of data use or sharing of the data when they first consented. There should be a clear opt-out system in case a data subject wants to withdraw their original consent. The policy of an organization should also make it clear that the institution does not obtain economic advantage by collecting or sharing personal information (Alanazi and Alenezi, 2024; Sarabdeen et al., 2022).

To set up proper standards in data protection, the European Union General Data Protection Regulation (GDPR) could be taken as a guideline. The GDPR gives control of data to the data subjects, Article 6 (1) (a) GDPR clearly states that natural persons have the right to know about collection of their data and the purpose of collection. Following this, the standard could state that the data collection should be consented to, and the data subjects should be informed of the purposes and the way their data are being processed. The data subjects should be given access to data and the opportunity to correct any errors in the data. In this aspect, Article 7(2) GDPR states that consent for data processing should be obtained intelligible and easily accessible form. The

purpose of data collection should be clearly stated. Once the data are collected, there is also a limitation on storage. There should be a nexus between the purpose of data collection and the period of storing the data. Consent should cover all processing. In addition, the data collected cannot be stored forever, it must be deleted within a given timeframe that relates to the objective for which the data was collected.

The data subject has a right to ask for the removal of data or exercise the right to be forgotten. The right to be forgotten is an important right that could control the processing of data that is outdated, irrelevant or has the potential to cause reputational or financial damage. Any standard should capture this right so that once the data subject requests for removal of data or right to be forgotten, their requests should be implemented within a reasonable timeframe. Article 20 of GDPR grants the right to data portability where data subjects can ask for data transfer from one controller in a commonly structured machine-readable format without any disturbance to the current data controller. This provision will be very useful in national and cross-border data transfer. If meeting the requirement is burdensome or costly, organizations are not expected to meet this request. This could be clearly stated in an organizational policy or standard. Article 3(2) of GDPR restricts the collection of data of a professional or commercial nature for international organizations. They are also obliged to follow all the GDPR requirements in collecting and processing data in EU member countries.

In terms of data management, the GDPR requires specific organizational measures to protect privacy while processing data. The measures include the use of pseudonymization of personal data to secure data from various risks. The privacy standard suggests pseudonymization technology or any other technology to protect privacy. If there is tracking, or profiling involved, the data subject shall be given the right to object to those practices. The standard or policy should allow the data subjects to object to any automated decision-making if it has any negative effects on the individual's interest like denial of rights, incurs in payment, or denial of services. Article 25 of the GDPR requires the introduction of "privacy by design" and "privacy by default" to meet technical standards. The "privacy by design" and "privacy by default" will ensure privacy protection from data collection to disposal of data. There is also a need to conduct data protection impact assessments as explained in Article 35 of GDPR if the processing has the potential to affect individual rights adversely (Almeida et al., 2021). Security measures should be considered as per Article 31 where the controllers and processors must implement technical and organizational measures to protect data, along with risk assessment and mitigation measures. If there is a need to transfer data beyond boundaries due to contractual relations or binding corporate rules, the rules related to Articles 44–47 of GDPR should be followed unless such transfer is required for public security, crime prevention, investigation, public health, or public safety. If any data controller fails to implement GDPR that causes damage to the data subject, the victims will be able to file for damages even if there is no contractual relationship between the parties involved. Besides, the data controller and processors could face a fine of up to 4% of the total worldwide annual turnover of the corporate group. Therefore, it is highly recommended to adopt technical or organizational measures in the development and use of RegTech so that the parties involved in designing or implementing will follow all the rules of acceptable data processing, use, storage, and transfer (Sarabdeen et al., 2022).

Any privacy policy or standard should include the requirement for data protection compliance skills as part of the employees' skill set (Kazim and Koshiyama, 2019). Since the employees need to work with the system, the skills needed should be revised to equip them appropriately for the operation of RegTech so they can provide advice to customers. Continuous education should be introduced as it will help the employees to develop skills and knowledge that are current and relevant. Concurrently, industry-wide design, collaboration, and guidelines should be encouraged in the planning phase of RegTech development or implementation so that an acceptable standard can be drawn. A universal standard among the parties involved will help in adopting a unified industry solution. This will ensure parallel rules related to data protection or localization. This will also assist in avoiding overlapping regulatory requirements that could lead to an inefficient compliance system (Packin, 2018).

Some researchers argue that having a US laissez-faire approach to data protection will be effective for enhancing innovation and promoting technology unlike the approaches adopted by EU countries (Almeida et al., 2021). Initially, the laissez-faire approach in the US facilitated the datafication and acquisition of data combined with analytics. It was the major force in the evolution of RegTech. However, for the seamless adoption of RegTech, the regulators and the organizations should give enough consideration to security, privacy, digital identity, and competition issues. Though the EU member countries implemented the data protection laws, they have also relaxed some of the requirements of data protection regulation. The EU introduced a regulation to ease issues regarding digital identity. In this context, the financial industry adopted the eIDAS Regulation in 2014 to mutually accept digital identity for cross-border dealings among EU countries and corporations. Member states are only required to inform the EU Commission of the adoption of electronic Identification (eID). The eID could ensure a certain level of security and compliance with the Data Protection Regulation (Zetzsche et al., 2019). If a country lacks the proper legislative framework on data protection, having an appropriate privacy guideline on data protection will help in building trust among various stakeholders in the operation of RegTech.

## 3.2. Accountability as part of the RegTech privacy model

Accountability could be defined as the duty to justify and be answerable for the actions taken and the outcome of the action (Leonelli, 2016; Wang, 2024). Accountability, according to Bovens, is based on a relationship between an actor and a forum, and the actor is expected to explain his action, answer all questions, and face the consequences of his action (Bovens, 2007). Accountability is said to be broader than transparency as the latter only requires the disclosure and openness of a working system, agent, or organization and does not require a justification for using a certain system, measure, or method (Wieringa, 2020). However, accountability will require justification for choosing a certain system, measure, or action. Though meeting accountability and transparency in technology applications is becoming challenging as advanced configuration and large amounts of data make it difficult to provide all the step-by-step traceable information, adequate efforts should be implemented to meet the expectation of being accountable and transparent (Burrell, 2016).

The GDPR 'privacy by design' (PbD) and 'privacy by default' are built to protect personal data and provide accountability in data processing (Lmeida, 2022). The requirement of a Data Protection Impact Assessment (DPIA) for high-risk processing of data is one way of achieving PbD. In conducting DPIA, it is necessary to ensure that the justification has been assessed comprehensively and processing measures are fair and lawful. For instance, the Swedish Authority for Privacy Protection requested a school to stop using facial recognition technology as the usage does not come within the requirement of proportionality and necessity. This was attributed to incorrect usage of DPIA and the consent obtained was declared to be invalid. In another incident concerning privacy violation, the IMY fined the Swedish police for failing to conduct DPIA and negligently allowing unauthorized employees to access the software that contained personal data. The police also failed to incorporate appropriate PbD measures in this case (IMY, 2019, 2021). In the case of Bridges v. South Wales Police (2020), Bridges, a civil rights campaigner, inter alia argued that the police DPIA was not performed correctly in the use of facial recognition technology and the court agreed with his argument and decided in his favor. Hence, proper conduct of DPIA is necessary and that requires thorough knowledge and understanding of the technology. Another requirement of the GDPR that could be linked to accountability is the need to have a Data Protection Officer (DPO). If an organization processes data on a large scale regularly or is involved in the monitoring of individuals or processing of data related to criminal offenses or convictions, there is a need to have a DPO. The DPOs should advise the organization on appropriate compliance with data protection measures. If an organization is found to be non-compliant, the DPOs should report to the relevant authority on data protection (Lmeida, 2022).

Auditing schemes could be introduced to ensure accountability in data processing, where the audit system looks at data input, methods, techniques, and assumptions to eliminate bias and incorrect decisions. Interdisciplinary cooperation in this matter is warranted where the legal department could vet the legality of the process, and output of the system along with the intermediate steps. The system experts will devise the data and system according to the legal requirement while the anthropologist and sociologist will assist in data profiling. It should be made compulsory to build an intra-system consistency test so that any discrepancy could be flagged. The fit between the expected and final outcome should be aligned, and the risk-profiling software can provide options to see contradictions. For example, it would allow customer replies to be assessed so that contradictions could be analyzed among different pieces of information provided. Inter-system consistency should also be ensured, where various information from outside could be checked for validity. In the know-your-customer application, the information collected by a bank using RegTech is crosschecked with external information. Periodic system testing and upgrades should be mandated so that any updates and insights can be captured correctly. That will ensure the validity of a decision. A rigorous, systematic method of validation and monitoring will ensure compliance with legislative and privacy standards. According to the UK Information Commissioner's Office (ICO, 2016) guidance on AI auditing and impact assessments, the AI system used for law enforcement should be accurate, reliable, and transparent. It further insisted on data quality and documentation so that individual rights could be safeguarded (Bivins, 2006). The guideline further mentioned the need to have an

oversight on the important aspects of data processing. Though accountability and design documentation are not required by law explicitly, privacy by default under Article 25 requires the technology to be built around data protection that may require being accountable in each step of data processing.

Human cross-checking should be made a requirement so that any erroneous output or system errors that are caused due to outliers can be corrected. Supervisors and managers should ensure that they have an efficient and robust system where the possibility of error can be minimized. For instance, the Basel Committee mentions that the supervisors and auditors should have effective communication to collectively identify and understand risks associated with their financial institutions and understand the measures taken to mitigate the risks. In the development stage of RegTech and other technologies, introducing participative, reflexive management will ensure the researchers and designers consider the ethical and privacy implications of their work at every step. The researchers, developers, and others who retrieve information should be trained to consider data history, the significance of the data history, and possible bias before or during collection and during analysis or reanalysis of the data. Accountability should enable understanding of the decision-making process so that the researchers and designers can hold up to the standards that would help to control malpractice (Bovens, 2010; Frauenberger et al., 2016; Israel, 2018). Accountability does not constrain research or prevent innovative research rather it helps to provide a greater acceptable framework from coding data to the research process and the decision-making (Wagner, 2020).

Ongoing training on privacy and participative privacy assessment promotes the exchanging of ideas and understanding the implications of their work. This practice could facilitate better privacy practices among individuals who handle data. The privacy consideration could start from the choice of metadata including data annotations in databases. There should be detailed information about the purpose, if data are collected, the details about how data was collected, how data subjects were chosen, the type of data handled, and the method of data handling. It should also include information about the personnel involved in the project (Leonelli, 2016). Further, the localization of privacy principles will allow scientists, researchers, and designers to assess their practice, and compare and adopt acceptable industry standards on experimentation and reasoning (Leonelli, 2016). This practice will allow them to understand the potential impact of their work while comparing the views of others and ultimately help to improve the quality and reliability of their outputs in RegTech development or application.

### 3.3. Transparency as part of the RegTech privacy model

Transparency could be defined as being open, visible, explainable, or interpretable (Felzmann et al., 2019b). Transparency could mean different things in different disciplines. In politics, it could mean a precondition for participation, and in law, it could mean a precondition for the legality of an administration (Meijer, 2014). Researchers look at transparency in a different dimension- some look at transparency as a virtue while others look at it as a relational notion. A third perspective looks at transparency from a systemic perspective. According to Meijer, transparency as a

virtue does not set standards for evaluating the behavior of public actors (Meijer, 2014), it only requires consistent openness of the system, activities, and agents of an organization. Transparency as a relational notion looks at transparency about an agent and recipient. Thus, transparency is evaluated based on the openness of an agent and how it has been received and understood by the recipient. It also could include the monitoring of transparency by other actors (Felzmann et al., 2020).

Transparency through a systemic perspective looks at transparency in an institutional context, organizational measures, and communication. The organizations should show effective implementation and impact of the transparency measures taken (Felzmann et al., 2020). However, there should be a balance between transparency and nonviolation of privacy. Public pressure for disclosure should not be a reason to release confidential and private information that is available in training data, as such release could violate the law and business interest. Instead, transparency should provide measures to address inequality, bias, and undue influence rather than providing nominal or infringing information. The decision-makers should have all the relevant information, and understand the processes and the outcome of the decisions as part of transparency best practice (Felzmann et al., 2019a). Inspection should be part of the transparency standard where a third party is allowed to investigate the standards of decision-making. Traceability is another component that should be present as part of the transparency standard (Zerilli et al., 2019).

It is argued that the algorithms could provide better clarity and transparency in selecting the variables and the reasoning behind decisions which in turn will control discrimination. For example, if the algorithm is used in court, the court could utilize the algorithm's risk prediction and make decisions based on risk factors like ordering detention for high-risk defendants and releasing multiple low-risk inmates. However, inherent biases in algorithm use could be seen in employment, search and arrest, immigration, and other related algorithms (Howard and Borenstein, 2018). The software can be biased, for instance, a gender-neutral advertisement may turn out to be biased against certain groups as the creator of the software may contain bias in building the software. Biases in the existing data set could affect the algorithms as they would bring biased outcomes. Since algorithms affect user behavior, any bias in algorithms would hurt user behavior. Measurement bias could also occur depending on the way data has been categorized, used, and measured (Mustard, 2003). Historical socio-political bias could affect data sampling and the subsequent result of the analysis (d'Alessandro et al., 2017). Similarly, discrimination could lead to unfairness, and it could be the cause of prejudice and likewise affect data collection and analysis. Some types of discrimination are allowed as justifiable discrimination and it is considered legal (Kamiran and Zliobaite, 2013). For example, giving priority to Aboriginal people in certain types of employment hiring is considered justifiable discrimination to offset historical barriers i.e., racism, and negative attitudes passed down by settlers, they have faced to enter the workforce. Discrimination based on gender, and marital status is illegal and unacceptable. This kind of discrimination could cause unfair treatment or unfavorable outcomes (Kleinberg et al., 2018).

Since bias and discrimination are prohibited by law, algorithms should be designed to avoid this. In designing the algorithm, designers may choose the most common approach and have a comprehensive record for transparency so

discrimination can be weeded out (Bertino, 2019). Introducing a policy on transparency is as crucial as changes made to privacy-related issues. The policy should request all the components of an algorithm including the data set, screening, and training algorithms be available for examination. The policy should require the disclosure of data selection rationale and ultimate decision. The output based on the algorithm depends on the input from the data set so, ensuring proper input of data will help eliminate bias and provide transparency (Barocas and Selbst, 2016). There should be a prohibition regarding disparate treatment, disparate impact on certain groups, and using of data produced based on past discriminatory results. There should be enough representation from certain subgroups and the variable used should directly relate to the outcome.

Transparency in the use of RegTech requires the disclosure of information that includes details about the system, scope, limitation of the systems, application, and any exceptions. An organization should come up with a transparency policy that is clear and concise. It should allow capture of the changes in processes and systems even if the system is complex. The process and system should be transparent to supervisors so that they can understand and correct any errors and try to apply best practices (Felzmann et al., 2020). The regulators should also be transparent towards the market and disclose the RegTech system, the model they use, the pitfalls of the model, and changes that they introduced to the system. This will create trust in the operation and show the accuracy of the model. The introduction of transparency initiatives will allow customers to make informed decisions.

Researchers have suggested to incorporate Transparency by Design (TbD) and coined it with PbD (Cavoukian, 2006). While TbD could help achieve privacy, it would also allow a more careful appreciation of transparency. The TbD offers a framework as a reflection tool to implement transparency like PbD. Though PbD is mandated by law TbD is a self-regulatory initiative. Zarsky (2013) came up with a taxonomy for the transparency of predictive analytics. This taxonomy included stages of transparency: designing, data processing, analysis, and accountability. In designing transparency measures, careful thought should be given from the initiation of design rather than being reactive (Cavoukian, 2006). The design should consider transparency as an integrative process where it is incorporated from data collection, data labeling, and algorithms used in the decision-making process. The TbD should consider audience needs and the way they interpret the data. The transparency requirements and information may vary and depend on the recipient and the data being shared (Zarsky, 2013). It should be noted that explanations of certain processes could be challenging in technologically loaded data and data processing (The European Commission's HLEG AI, 2019). In this situation, a reasonable explanation of the data used, the steps involved in selecting data, and in which stage of data processing human intervention took place should be explained. The regulators can insist on having certain models or standards that are to be periodically reviewed as part of organizational policy. The EU Commission's Delegated Regulation on regulatory technical standards for investment firms states that organizations must implement measures like governance, tests, and assessments concerning algorithms so that accountability and transparency can be maintained.

Since automated decision-making would harm individuals, the transparency practice should explain when and how human intervention takes place. In making decisions, the criteria utilized and justification for the decision could be explained. (Wachter and Mittelstadt, 2019). The justification should include the level of privacy breaches, the countermeasures taken, the purpose of processing, the impact of processing, and the reliability of the inference of the result. The TbD or Transparency standard should include the possible risk and the risk mitigation mechanism so that informed consent can be attained (Beauchamp and Childress 2001). Allowing audit of the system, process, data, risk, and risk management will meet the requirement of inspectability of the transparency principle (Felzmann et al., 2019a; Zerilli et al., 2019). This audit will allow experts to test and verify the system and processes. Transparency requires organizations and actors to be responsive to the questions of the stakeholders. Whether the data controllers or the users are in compliance or noncompliance with the rules and norms, they should be open to answer any questions and criticisms. That includes a critical assessment of their performance on transparency and meeting any legal consequences and sanctions. Periodical reporting of the use of AI or other technologies for data collection should be carried out. The report could give descriptive and aggregate information about where the data processing happened what types of data had been used, how the decision had been made, and the outcome of the decision. The format might differ depending on the purpose and the audience.

In devising appropriate transparency and accountability standards, coordination among various regulators will assist in a cross-border cooperation framework. For instance, Kenya, Singapore, the UK, and the Canadian province of Ontario signed an agreement to allow access to new markets with cooperation agreements to receive informal assistance on the regulatory environment they may face in the banking business (Konina, 2020). Additionally, this type of cooperation could also help compliance and develop a common standard. They could also share best-practice guidelines and code of conduct as this will help in building regulations for RegTech. The use of technology will become safe and effective if cross-border agreements can be reached on operational and resolution matters considering economic, legal, and other factors. For instance, machine learning algorithms could be directed for sharing data and reconciling them for different authorities locally and internationally. This could be achieved by creating a common taxonomy, standard, and resolution mechanisms. For instance, the cross-border Crisis Management Group (CMG) of the banking sector works closely based on informal agreements to supervise banks and a similar setup could be devised concerning technological cooperation in RegTech (Loiacono and Rull, 2022). Currently, transparency is not legally mandated as privacy, and it would be advisable to include transparency as a legal requirement. However, consideration should be given not to violate privacy while being transparent about the data. To mitigate this, the transparency policy should include a clause on privacy protection. A transparency score could be introduced which displays a scalar to assess the risk of privacy violation while exercising transparency.

### 3.4. Organisational design as part of RegTech privacy model

The organizational design could be considered a blueprint for the formal structures of organizations that explain the hierarchy, labor, and distribution of authority among other things (Mintzberg, 1979; Triandis, 1966; Thompson, 1967). Historically, the organizational structure is an important part of controlling organizational behavior (Mintzberg, 1979). The classical approach to organizational design does not give enough consideration to informal structure or organizational culture which plays a crucial role in organizational success (Schein, 1985). Its concentration is on upper management and the organizational design ensures that employees work according to what upper management thinks is productive and workers are not a core part of the design (Rittel, 1972).

The new approach to organizational design is called developmental design where design and development are intertwined. According to Burnes (1996), developmental approaches are more suitable for turbulent environments whereas the classical approach suits a stable environment. Since the adoption of technology will require changes in the creation of an ethical culture, the new approach to organizational design will facilitate the adoption. The new design was not created to control people's behavior but rather, to address uncertainty and unexpected situations (Nystrom and Starbuck, 1981). The new generation of organizational design is realistic and more relevant to practitioners. The industry could follow a few developmental designs: reflection-in-action, co-construction, and bricolage. According to Schon (1987), reflection-in-action could be considered as one of the developmental approaches. In reflection-in-action, a designer or a group of designers come up with a model, a concept, or a point of view then, explore its consequences and conditions and finally, reflect on its feasibility and productivity. This design involves various actors and introduces a testable design. If it suits the circumstances, it can be adopted by an organization. Co-construction is another design concept that allows progressive adjustment of organizational design depending on the complexity and uncertainty of the environment. Further development happens during the design process (Monge 1993). The design focuses on activities and their (temporary) closure. It can cover parallel and open-ended processes unlike the phase-related processes (Visscher, 2006). Bricolage is another theory where situational tinkering with the resources at hand are important feature (Weick, 1993). The designer as a bricoleur shall improvise a design with the tools and materials he has at hand. The bricoleur is problem-driven and has a structured way of working with the resources. Designing in the new generation does not emphasize the blueprints and their subsequent implementation, rather it focuses on an integral process of bringing a new organization into being.

For the regulators, the organizational structure should facilitate the update of the technology consistently. It is possible to follow either the government agency model, the government corporation model, the self-regulatory organization model, or the delegated gatekeeper model as mentioned by Yang and Tsang (2019) to regulate the industry. The model should be unbiased in regulating all the parties. Though the motivation of the current regulatory model may not be associated with profit, regulators fail in the current regulatory model to keep up with technological advances in the industry. Hence, it is recommended to move away from the current model of

regulation. The Government Agency model is the current popular model. According to this model, the regulators are assigned responsibility through legislation and the legislation provides a monopoly in the regulation of the market, where a single regulator regulates the assigned industry. Though the monopoly provides the advantage of lack of insight between various regulators within the same industry, the competition that fuels efficiency and innovation is absent. There may be potential for the influence of bigger industries at the expense of smaller industry players. The current model fails in adopting the fast-paced changing technological environment (Jabotinsky, 2017; Levitin, 2013).

Non-Profit Orientation is another model that allows the regulators to operate within the assigned budget without the motivation for a profit with revenue generated spent on organizational activities (Carnell et al., 2017). The current model involves bureaucracy and a rigorous decision-making process that requires compliance with the laws and regulations in terms of notice, hearing, etc. All these regulatory requirements could delay the process innovation similar to the Government Agency model. The other prevalent model is the Government Corporation model. This model is followed by most financial regulators. The regulators operate as a government corporation that is owned by the government (Froomki, 1995). For instance, the FDIC of the USA and FCA of the UK operate under this model while maintaining a monopoly in regulation and maintaining a self-sufficient budget. The regulators under this model do not pursue profit either. They operate as quasi-agencies and share many similarities like the Government Agency model in decision-making, innovation, monopoly, and non-profitable nature (Yang and Tsang, 2019).

The Self-Regulatory Organization model could also be adopted. Under this model, the regulators act as a non-governmental organization that operates according to the regulations and standards it creates (Sanders, 2017) The security regulators and real estate market regulators in some countries operate under this model. The issue of monopoly will not arise in this model as there could be many regulators in each market. The regulators under this model are concerned about public interest and tend to protect the interest of the regulated industries in comparison to the previous two Models. Moreover, they do not rely on budget allocation rather, generate their income and are not subject to the government's monitoring. However, regulators who operate under this model may be subjected to criticism for the possibility of compromising quality in regulating the industry (Yang and Tsang, 2019)

The next model followed by regulators is the Delegated Gatekeeper model. Under this model, the regulators delegate their powers to private parties to function as gatekeepers (Masciandaro and Romelli, 2016). The regulated industries could be allowed to select the gatekeepers. Since many gatekeepers are involved, the regulators do not maintain the monopolistic approach to regulation, the decision processes are less rigorous, and it helps to maintain flexibility in operation. This model provides the advantage of formulating an efficient compliance process that involves many industries with vast amounts of information. However, there exist disadvantages of industry influence and dominance in regulatory compliance. To avoid this pitfall, government regulators should impose requirements, standards, and sanctions for violation by gatekeepers and industry players. Though the government regulators are more accountable to the public, the operational inefficiency caused by monopoly, non-

profit operation, and strict adherence to due process disrupts the regulation of various industries. It is suggested that the adoption of more profit-oriented and flexible models will create an effective system of regulation, with rightly rigorous accountability (Yang and Tsang, 2019).

The organizational design should allow the RegTech developers and users to foster a privacy culture. The privacy culture should ensure the behavior of customer protection. There should be continuous monitoring of e-mails, conversations, and other interactions with customers so that the nuances of communication can be understood and addressed. Additionally, it may be difficult to comprehend the type of data, their associations, and factors in the algorithmic predictions to normal users, so the employees should be trained to understand the opacity involved in data use to avoid bias, discrimination, or other unfavorable results.

## 4. RegTech privacy model

Based on the discussion in section 3 above, the Privacy Model which should be part of the RegTech policy comprises four variables: data protection, accountability, transparency, and organization design. The four variables are made of various items. The 'Data protection' variable is comprised of consent as the crown of data processing, and it should be informed consent (Bertino, 2019; Sarabdeen et al., 2022). Disclosure of purpose as a component is linked to consent where the entire purpose of data processing should be disclosed. Allowing access to data to the data subject during any time of data processing is pertinent (Arner et al., 2017; GDPR, 2018). The possibility of correction of data should also be part of the Model. If the data subject requests for correction or erasure of data, the correction should be done within a reasonable timeframe. If the request cannot be entertained due to valid justification, the data subject should be informed. Disclosure of automated processing is an important item. The details about the automated processing of data and decision-making should be informed in advance so that the data subject can decide if they want to opt-out. Human intervention is one of the mandates in any automated decision-making (Wachter and Mittelstadt, 2019). The data subjects or consumers should be informed at which stage of the data processing the human intervention has taken place and the impact on decision-making. The consumer information collected during any transaction process should be stored for a limited time only. Data storage should be restricted to a reasonable time, where the time frame may differ from ordinary data to sensitive data. Technical and organization measures should be part of the Ethical Model where technical measures like privacy by design (PbD) and 'privacy by default' and any risk avoidance measures are incorporated. Training and cooperation with experts and regulators should be ongoing so that any update can be implemented in due time (Almeida et al., 2021; GDPR, 2018).

The 'Accountability' variable will include appropriate disclosure of the system, process, and people involved in RegTech (Wieringa, 2020). Justification for decisions, actions, and the selection of various systems is another item in the accountability variable (Burrell, 2016). Continuous monitoring of all components of RegTech activities, and audit are also part of the Model (Lmeida, 2022). Audits should be carried out periodically and look at data input, methods, techniques, and assumptions

to eliminate bias and wrong decisions. Interdisciplinary cooperation in this matter is warranted among various departments (Felzmann et al., 2019). In the case of automated decisions, the disclosure of human intervention and how human intervention played a role in the overall decision-making should be disclosed (Wachter and Mittelstadt, 2019). Ongoing training should be mandated to keep tabs on all the changes that may cause liability in the operation of RegTech.

'Transparency' as a variable includes many items and openness is one of them. The openness of the system, activities, and agents of an organization is necessary. Clarity about all the relevant information, algorithms, processes, and outcomes of decisions is also important in the Model (Felzmann et al., 2019). Inspect ability should be part of transparency where a third party is allowed to investigate the standards of decision-making. Traceability is another item that should be present as part of the transparency variable (Zerilli et al., 2019). The algorithms used in RegTech should provide improved transparency in controlling bias, inequality, and discrimination. Human intervention should be part of the RegTech Privacy Model so that stakeholders can understand the rationale behind decisions and the effect of decisions. Similar to an accountability audit, there should be a transparency audit where experts can test and verify the system, processes, and procedures (Lmeida, 2022). Transparency requires organizations and actors to be responsive to the questions of the stakeholders. Coordination with various stakeholders is also part of the Model as it creates an opportunity for sharing of best-practice guidelines and code of conduct. The use of technology will eventually become safe and effective if cross-border agreements can be reached on operational and resolution matters.

The development and implementation of RegTech require flexible and innovative organizational design so that challenges can be overcome. The informal organizational structure that the developmental designs offer will be the right fit for the challenging environment. The development organizational designs that are included in the 'Organisational Design' variable are reflection-in-action, co-construction, or bricoleur. They give the flexibility of operation, emphasize the importance of all workers, and value their feedback. Which organizational design is adopted depends on the problem, risk, and the resources at hand (Schön, 1987; Monge, 1993; Weick, 1993). While the industry could adopt the developmental design as part of the Privacy Model, regulators could look into other organizational designs that suit their operation and mandate. The possible designs are the government agency model, the government corporation model, the self-regulatory organization model, or the delegated gatekeeper model (Yang and Tsang, 2019). Organizational culture should fit the organizational model. The organizational design should allow the workers, system, and procedures to be flexible and informal so that the appropriate culture could be developed to protect consumers and be innovative in product development and operation (Triandis, 1966; Thompson, 1967; Mintzberg, 1979). All important items of each variable should be incorporated into the Privacy Model. This Privacy Model should be a part of the privacy policy or standard in an organization. The Privacy Model could work as a guideline and a blueprint in decision-making during RegTech Development or Implementation. **Figure 2** below shows the Privacy Model for RegTech.

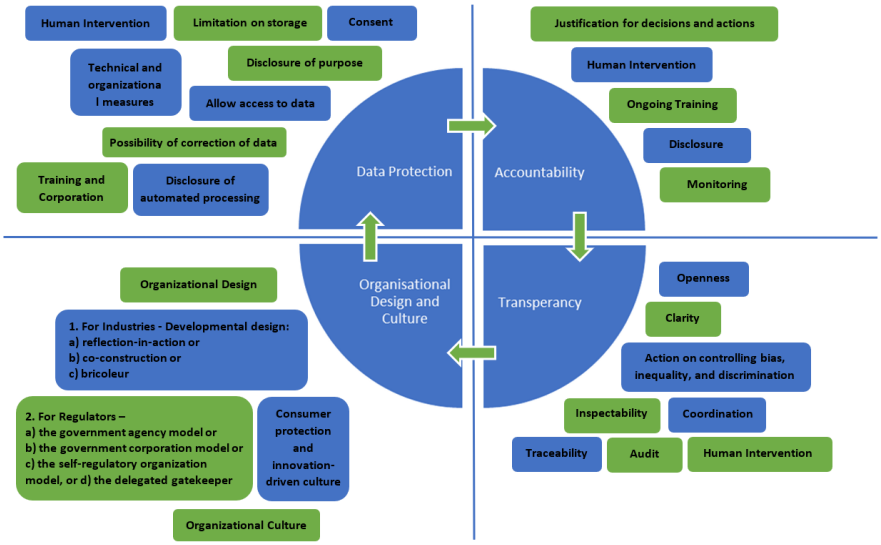


**Figure 2.** Ethics model for RegTech.

## 5. Conclusion: Implication of the RegTech privacy model and future research

RegTech involves complex data processing and movement of data handled by various parties. The processing and movement will raise different privacy questions that have significant consequences. Each processer of the data in RegTech should look at the aspect along with the legal impact of data processing and decisions made based on the processing. This approach to the privacy oversight of data could help in the quality and reliability of data-derived decisions and can be integrated as part of best practices. Considering privacy protection as an integral part of the use of RegTech could assist in maintaining the interest of all the stakeholders. The Privacy Model allows the integration of privacy protection in the RegTech application. It allows better protection of data, algorithms, and system use. It also ensures greater accountability (Haraway, 1988; Harding, 1992) and compliance with the GDPR principle of accountability and privacy by design duty. Transparency as part of the Model goes far beyond issues of data protection and accountability. The inclusion of transparency and organizational design in the Privacy Model allows broader considerations of equality, bias, discrimination, organizational design, and culture. In addition to privacy by design and privacy by default, the involvement of DPO is also part of the requirement of the Model. The involvement of global regulators and other industry players is considered for cooperation and training.

The implication of adopting the Privacy Model is that before the use of RegTech, users will understand the purpose of the data processing, the context of processing, the appropriateness of the notices given, the need for consent, and measures to be implemented in controlling bias and discrimination. Users also can explore the limitations of RegTech capacities and mitigation measures. The user can check how accountability and transparency are exercised and explained and the ways they are audited. The RegTech users can also assess the complaint management mechanism and the challenges in implementing them. There is a policy implication too, where the privacy Model will be adopted as part of the organizational policy and the managers

can act upon it for better compliance with law, ethics, and stakeholder expectations (Almeida et al., 2021). Future directions could involve regulators suggesting new laws to better regulate the RegTech. Laws like the Modernizing Government Technology Act of 2017 (MGT Act) enable the government to move forward in the modernization and adoption of technological infrastructure and the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank) to practice transparency in business and created supervisory agencies (Packin, 2018). This in turn will help to contribute to accountable and fair institutions as stated by United Nation's Sustainable Development Goals.

Future research in this domain can contribute to testing the model in various organizations. Studies could also use various mythologies to assess the effectiveness of monitoring, reporting, and compliance in various cultures.

**Acknowledgments:** The author would like to acknowledge the support of Prince Sultan University (PSU) for the research and for paying the Article Processing Charges (APC) of this publication. The author would like to record the support provided by the Governance and Policy Research Lab too.

**Conflict of interest:** The author declares no conflict of interest.

## References

Almeida, D., Shmarko, K., & Lomas, E. (2021). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. AI and Ethics, 2(3), 377–387. https://doi.org/10.1007/s43681-021-00077-w

Ara, A., Sharma, A., & Yadav, D. (2022). An efficient privacy-preserving user authentication scheme using image processing and blockchain technologies. Journal of Discrete Mathematical Sciences and Cryptography, 25(4), 1137–1155. https://doi.org/10.1080/09720529.2022.2075089

Alanazi, F., Alenezi, M. (2024). Driving the future: Leveraging digital transformation for sustainable transportation. Journal of Infrastructure, Policy and Development, 8(3), 3085. https://doi.org/10.24294/jipd.v8i3.3085

Arner, D.W., Barberis, J., Buckley, P.R. (2017). FinTech, RegTech, and the Reconceptualization of Financial Regulation. Northwestern Journal of International Law and Business, 37, 371-413.

Barefoot, J.A. (2020). Digitalizing Financial Regulation: RegTech as a Solution for Regulatory Inefficiency and Ineffectiveness. Available online: https://www.hks.harvard.edu/centers/mrcbg/publications/awp/awp150 (accessed on 5 December 2023).

Beauchamp, T.L. (2001). Childress JF Principles of biomedical ethics, 7th ed. Oxford University Press.

Bertino, E., Kundu, A., & Sura, Z. (2019). Data Transparency with Blockchain and AI Ethics. Journal of Data and Information Quality, 11(4), 1–8. https://doi.org/10.1145/3312750

Bivins, T. H. (2006). Responsibility and Accountability. Ethics in Public Relations: Responsible Advocacy, 19–38. https://doi.org/10.4135/9781452204208.n2

Bolton, M., & Mintrom, M. (2023). RegTech and creating public value: opportunities and challenges. Policy Design and Practice, 6(3), 266–282. https://doi.org/10.1080/25741292.2023.2213059

Bovens, M. (2010). Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism. West European Politics, 33(5), 946–967. https://doi.org/10.1080/01402382.2010.486119

Brand, V. (2020). Corporate Whistleblowing, Smart Regulation and Regtech: The Coming of the Whistlebot? SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3698446

Bridges, R. (On the Application Of) v South Wales Police. (2020). EWCA Civ 1058. Available online: https://www.bailii.org/ew/cases/EWCA/Civ/2020/1058.Html (accessed on 5 December 2023).

Burnes, B. (1996). Managing change. In: A strategic approach to organizational dynamics, 2nd ed. Pitman Publishing.

Burrell, J. (2016). How the machine 'thinks': Understanding opacity in machine learning algorithms. Big Data & Society, 3(1), 205395171562251. https://doi.org/10.1177/2053951715622512

Carnell, R.S., Macey, J.R., Miller, G.P., Conti-Brown, P. (2021). The Law of Financial Institutions, 7th ed. Aspen.

Cavoukian, A. (2006). Privacy by design: The 7 foundational principles. Available online: /iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf (accessed on 5 December 2023).

Clarke, R. (2020). RegTech Opportunities in the Platform-Based Business Sector.

d'Alessandro, B., O'Neil, C., & LaGatta, T. (2017). Conscientious Classification: A Data Scientist's Guide to Discrimination-Aware Classification. Big Data, 5(2), 120–134. https://doi.org/10.1089/big.2016.0048

European Commission. (2016). Open innovation, open science, open to the World. Brussels, Belgium: European Union Publication. Available online: http://bookshop.europa.eu/en/open-innovationopen-science-open-to-the-world-pbKI0416263/ (accessed on 5 December 2023).

Eva, M., Anna Rose, W. (2019). Regulatory technology: Replacing law with computer code. European Business Organization Law Review. pp. 1-29.

Fagan, F. (2016). Big Data Legal Scholarship: Toward a Research Program and Practitioner's Guide. Virginia Journal of Law & Technology, 20(1): 1-81.

Felzmann, H., Villaronga, E. F., Lutz, C., et al. (2019a). Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns. Big Data & Society, 6(1), 205395171986054. https://doi.org/10.1177/2053951719860542

Felzmann, H., Fosch-Villaronga, E., Lutz, C., et al. (2019b). Robots and Transparency: The Multiple Dimensions of Transparency in the Context of Robot Technologies. IEEE Robotics & Automation Magazine, 26(2), 71–78. https://doi.org/10.1109/mra.2019.2904644

Felzmann, H., Fosch-Villaronga, E., Lutz, C., et al. (2020). Towards Transparency by Design for Artificial Intelligence. Science and Engineering Ethics, 26(6), 3333–3361. https://doi.org/10.1007/s11948-020-00276-4

Frauenberger, C., Rauhala, M., & Fitzpatrick, G. (2016). In-action ethics: Interact Computing System. Available online: 10.1093/iwc/iww024 (accessed on 5 December 2023).

Froomkin, A.M. (1995). Reinventing the Government Corporation. University of Illinois Law Review.

Google Spain decision of the Court of Justice of EU. (2014). Available online: https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf (accessed on 5 December 2023).

Howard, A., & Borenstein, J. (2018). The Ugly Truth About Ourselves and Our Robot Creations: The Problem of Bias and Social Inequity. Science and Engineering Ethics, 24(5), 1521–1536. https://doi.org/10.1007/s11948-017-9975-2

Haraway, D. (1988). Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective. Feminist Studies, 14(3), 575. https://doi.org/10.2307/3178066

Harding, S. (1992). After the neutrality ideal: science, politics, and strong objectivity. Soc Res, 59, 67-587.

IMY. (2019). Supervision pursuant to the General Data Protection Regulation (EU) 2016/679—facial recognition used to monitor the attendance of students. Stockholm.

IMY. (2021). Police unlawfully used facial recognition app. Available online: https://www.imy.se/nyheter/police-unlawfully-used-facialrecognition-app/ (accessed on 5 December 2023).

Israel, M. (2018). Ethical Imperialism? Exporting Research Ethics to the Global South. The SAGE Handbook of Qualitative Research Ethics, 89–100. https://doi.org/10.4135/9781526435446.n6

Jabotinsky, Y.H., Jabotinsky, Y.H. (2017). The Federal Structure of Financial Supervision: A Story of Information-Flow. Stanford Journal of Law, Business & Finance, 22(1), 52-92.

Kazim, E., & Koshiyama, A. (2019). Data Ethics Principles: A Comment on the House of Lords Report 'Regulating in a Digital World.' SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3581754

Kamiran, F., Žliobaite, I. (2013). Explainable and Non-explainable Discrimination in Classification. Springer.

Khan, A., Hassan, M. K., Paltrinieri, A., et al. (2020). A bibliometric review of takaful literature. International Review of Economics & Finance, 69, 389–405. https://doi.org/10.1016/j.iref.2020.05.013

Kleinberg, J., Ludwig, J., Mullainathan, S., et al. (2018). Discrimination in the Age of Algorithms. Journal of Legal Analysis, 10, 113–174. https://doi.org/10.1093/jla/laz001

Konina, A. (2020). Regulating Regtech: The Benefits of a Globalized Approach. Lex Electronica. Available online: https://ssrn.com/abstract=3914215 (accessed on 5 December 2023).

Levitin, A. J. (2013). The Consumer Financial Protection Bureau: An Introduction. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2199678

Leonelli, S. (2016). Locating ethics in data science: responsibility and accountability in global and distributed knowledge production systems. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 374(2083), 20160122. https://doi.org/10.1098/rsta.2016.0122

Lmeida, D., Shmarko, K., Lomas, E. (2022). The Ethics of Facial Recognition Technologies, Surveillance and Accountability in an Age of Artificial Intelligence: A Comparative Analysis of USA, EU and UK Regulatory Frameworks. AI and Ethics, 2, 377–387.

Loiacono, G., & Rulli, E. (2022). ResTech: innovative technologies for crisis resolution. Journal of Banking Regulation, 23(3), 227–243. https://doi.org/10.1057/s41261-021-00154-4

Loosman, I., & Nickel, P. J. (2022). Towards a Design Toolkit of Informed Consent Models Across Fields: A Systematic Review. Science and Engineering Ethics, 28(5). https://doi.org/10.1007/s11948-022-00398-x

Maglaras, L., Almomani, I. (2023). Digitization of healthcare sector: A study on privacy and security concerns. Korean Institute of Communications Information Sciences.

Masciandaro, D., & Romelli, D. (2016). Banking Supervision and External Auditors: What Works Best? SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2895999

Mehrabi, N., Morstatter, F., Saxena, N., et al. (2022). A Survey on Bias and Fairness in Machine Learning. ACM Computing Surveys, 54(6), 1–35. https://doi.org/10.1145/3457607

Meijer, A. (2014). Transparency. In: Bovens, M., Goodin, R.E., Schillemans, T. (editors). The Oxford handbook of public accountability. Oxford University Press.

Moher, D., Liberati, A., Tetzlaff, J., Altman, D.G. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. BMJ, 339(7716), 332–336. https://doi.org/10.1136/bmj.b2535

Mintzberg, H. (1979). The structuring of organizations. Prentice-Hall.

Monge, P.R. (1993). (Re)designing dynamic organizations. in: Huber GP, Glick WH. eds. Organizational change and redesign; Ideas and insights for improving performance. Oxford University Press. pp. 323-345.

Mustard, D. B. (2003). Reexamining Criminal Behavior: The Importance of Omitted Variable Bias. Review of Economics and Statistics, 85(1), 205–211. https://doi.org/10.1162/rest.2003.85.1.205

Nystrom, P.C., Starbuck, W.H. (1981). Handbook of organizational design. In: Adapting organizations to their environments. Oxford University Press.

Oswald, M., Grace, J., Urwin, S., et al. (2018). Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality. Information & Communications Technology Law, 27(2), 223–250. https://doi.org/10.1080/13600834.2018.1458455

Packin, G.N. (2018). RegTech, compliance and Technology Judgement Rule. Chicago-Kent Law Review, 93(1), 193-218.

Remus, D., Levy, F.S. (2017). Can Robots be Lawyers? Computers, Lawyers and the Practice of Law. Georgetown Journal of Legal Ethics, 30(3), 501–511.

Rittel, H. (1972). On the planning crisis; Systems analysis of the first and second generation. Bedrifts Okonomen, 8, 309-396.

Sanders, J. (2017). Break from Tradition: Questioning the Primacy of Self-Regulation in American Securities Law. Michigan Business & Entrepreneurial Law Review, 7.1, 93. https://doi.org/10.36639/mbelr.7.1.break

Sarabdeen, J. (2022). Protection of the rights of the individual when using facial recognition technology. Heliyon, 8(3), e09086. https://doi.org/10.1016/j.heliyon.2022.e09086

Schein, E. (1987). Organizational culture and leadership. Jossey-Bass.

Schön, D.A. (1987). Educating the reflective practitioner; Toward a new design for teaching and learning in the professions. Jossey-Bass Publishers.

Siering, M. (2022). Explainability and fairness of RegTech for regulatory enforcement: Automated monitoring of consumer complaints. Decision Support Systems, 158, 113782. https://doi.org/10.1016/j.dss.2022.113782

The EU General Data Protection Regulation (GDPR). (2018). Available online: https://eugdpr.org/ (accessed on 5 December 2023).

Thompson, J.D. (1967). Organizations in action. McGraw.

Triandis, H.C. (1966). Notes on the design of organizations. In: Approaches to organizational design. University of Pittsburg Press.

Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. IEEE Communications Surveys & Tutorials, 18(3), 2084–2123. https://doi.org/10.1109/comst.2016.2535718

Visscher, K. (2006). Capturing the competence of management consulting work. Journal of Workplace Learning, 18(4), 248–260. https://doi.org/10.1108/13665620610665845

Visscher, K., Fisscher, O.A.M. (2012). Towards a new generation of organizational design. University of Twente, Enschede.

Wachter, S., Mittelstadt, B. (2019). A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI. Columbia Business Law Review, 7(2), 494–620.

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. https://doi.org/10.1093/idpl/ipx005

Wagner, B. (2020). Accountability by design in technology research. Computer Law & Security Review, 37, 105398. https://doi.org/10.1016/j.clsr.2020.105398

Wang, X.L. (2024). Managing third party accountability in human services contracting: Contract accountability in human services. Journal of Infrastructure, Policy and Development, 8(2), 2622. https://doi.org/10.24294/jipd.v8i2.2622

Waye, V.C. (2019). Regtech: A New Frontier in Legal Scholarship. Adelaide Law Review, 40(1), 363–386.

Weick, K.E. (1993). Organizational redesign as improvisation. In: Organizational change and redesign; Ideas and insights for improving performance. Oxford University Press.

Wieringa, M. (2020). What to account for when accounting for algorithms. A systematic literature review on algorithmic accountability. In: Proceedings of the 2020 conference on fairness, accountability, and transparency.

Yang, Y.P.A, Tsang, C.Y. (2019). RegTech and the New Era of Financial Regulators: Envisaging More Public-Private Partnership Models of Financial Regulators. University of Pennsylvania Journal of Business Law, 21(2), 1-51.

Zarsky, T.Z. (2013). Transparent predictions. University of Illinois Law Review, 4, 1503–1570.

Zerilli, J., Knott, A., Maclaurin, J., et al. (2019). Transparency in Algorithmic and Human Decision-Making: Is There a Double Standard? Philosophy & Technology, 32(4), 661–683. https://doi.org/10.1007/s13347-018-0330-6

Zetzsche, D. A., Arner, D. W., Buckley, R. P., et al. (2019). The Future of Data-Driven Finance and RegTech: Lessons from EU Big Bang II. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3359399