JOURNAL OF CULTURAL ANALYSIS AND SOCIAL CHANGE

Journal of Cultural Analysis and Social Change,
2025, 10(2), 3599-3607
ISSN: 2589-1316

Negligence and Data Protection in Saudi Arabia: A comparative doctrinal analysis of the GDPR, CCPA, and PDPL with a Sharia-Based Legal Framework

Hanan Alnasser[1*]

[1] *Faculty of Law, Universiti Malaya,* MALAYSIA

***Corresponding Author:** hananalnasser97@gmail.com

Citation: Alnasser, H. (2025). Negligence and Data Protection in Saudi Arabia: A comparative doctrinal analysis of the GDPR, CCPA, and PDPL with a Sharia-Based Legal Framework, *Journal of Cultural Analysis and Social Change*, 10(2), 3599-3607. https://doi.org/10.64753/jcasc.v10i2.2146

Published: November 20, 2025

ABSTRACT

Personal data has become a source of debate recently. Organizations can use these data to be innovative and efficient in accessing individuals. However, the handling of these data varied among organizations making the usage turned from technical error to moral failure. This paper review and compares the legal systems in the European union (General Data Protection Regulation (GDPL), American law (California's consumer privacy act (CCPA), and Saudi Arabia's personal data protection law (PDPL). These laws deals with negligence. The methodology of this study is a qualitative, doctrinal method and the study utilizes the Tort Theory, Accountability Theory, and Shariah Jurisprudence (Fiqh Al-Muamalt) to investigate how laws and ethics works to protect personal data. The findings showed that GDPR and CCPA have pushed negligence far beyond its traditional role in tort theory going beyond compensating for harm to the constant vigilance. On the other hand, in Saudi Arabia, the framework is still being developed and lacks independent system of enforcement. However, the Shariah principles have addressed these the issues of negligence by act such as trust, responsibility and prevention of harm. This makes that protecting data in Saudi Arabia not legal issue alone but ethical and moral expectation.

Keywords: Negligence, Data protection, GDPR, CCPA, PDOL, Tort Law, Shariah Jurisprudence, Saudi Arabia

INTRODUCTION

Personal data is new capital that drives digital innovation, trade, and governance. Digital technologies including AI, big data analytics, blockchain, and cloud computing have transformed data collecting, processing, and usage for governments, companies, and individuals (Dąbrowska et al., 2022; Pimenta Rodrigues et al., 2024). However, societies' rising reliance on digital infrastructure has exacerbated data breaches, privacy violations, and unauthorized disclosures. Organizational negligence-related crisis have created economic losses, reputational damage, and public trust loss (Filler et al., 2022; Tschider, 2024). Thus, industrialized and rising nations prioritize legal accountability for reckless personal data handling.

Tort law defines negligence as a failure to perform appropriately in similar circumstances that harms or loses others (Hylton, 2014; Posner, 2004). Digital duty of care involves protecting personal data against cyberattacks, illegal processing, and disclosure (Balkin, 2016; Jun & Kim, 2024). Data underlies contemporary social and economic activity, therefore neglecting it is a technological mistake and a legal and ethical breach of trust between data controllers and data subjects (Ke & Sudhir, 2023). Politicians and courts must adapt negligent conceptions to data governance as blame shifts from physical to intangible damage (Morrow & Fitzpatrick, 2020; Kesan & Hayes, 2018).

Data protection laws like GDPR and CCPA have negligence standards. Accountability, openness, and individual rights underpin global data protection rules in the 2018 GDPR (Voigt & von dem Bussche, 2017; Quinn & Malgieri, 2021). Data controllers and processors must take "appropriate technological and organizational

measures" to maintain security commensurate with risks under Article 32, which does not define "negligence." Intentional or careless violations can result in administrative fines of 4% of worldwide sales (European Commission, 2018). Responsibility and enforcement make GDPR negligence a functional standard of care, allowing proactive risk management and compliance monitoring (Hamon et al., 2022).

The 2018 California Customer Privacy Act (CCPA) safeguards data and negligence. Customers can sue under California Civil Code Section 1798.150 if a corporation fails to provide proper security. This statutory acknowledgment of negligence moves the burden of evidence from the person to the business, forcing organizations to implement proactive data security measures (Williams, 2020; Koepke & Kaminski, 2020). Thus, the CCPA holds digital economy private sector players accountable for reasonable care neglect. The GDPR and CCPA show how negligence evolved from a reactive tort-based notion to a proactive compliance duty to prevent irresponsible data handling and boost public confidence in digital systems (Masur, 2020; Zhao et al., 2023).

Saudi Arabia, a rapidly digitalizing nation under Vision 2030, is still establishing a data protection and negligence liability policy. Royal Decree No. M/19, revised in 2023, was the Kingdom's first personal data gathering, processing, storage, and transfer law (Sarabdeen & Mohamed Ishak, 2025). PDPL assures data processing fulfils privacy, trust, and accountability criteria, making Saudi Arabia a regional data governance leader. Legal definition, scope, and enforcement of carelessness are ambiguous. Data controllers must "implement required organizational, administrative, and technological measures to secure personal data," however Article 19 of the PDPL does not define "necessary" or "reasonable" care, rendering regulatory interpretation unclear (Alhejaili, 2024). Absence of independent supervisory authority, unambiguous private rights of action, and complete breach notification undermines accountability and enforcement.

This confusion is noteworthy compared to global best practises, where negligence-based liability is vital to deterrence and victim reparation (Teichmann & Wittmann, 2023; Thomas et al., 2022). In Saudi Arabia, where e-government platforms and financial institutions have suffered data breaches (Almulihi et al., 2022; Juma'h & Alnsour, 2020), the lack of a negligence standard may restrict legal remedies and harm institutional reputation. Thus, the PDPL promotes legal modernity but is immature doctrinally and institutionally, necessitating a comparative and cultural appraisal of negligence.

Saudi Arabia's data protection policy is based on Sharia, which values trust (amanah), damage prevention (la darar wa la dirar), and public benefit. Islamic law views carelessness (taqṣīr) as a moral breach of accountability (mas'ūliyyah), not just a technical error. Gain accounting validates morality and law. Therefore, statutory law and ethical and moral principles that safeguard human dignity and society can punish expected negligence-related data breaches. The Saudi PDPL can integrate digital governance to Sharia-based justice, responsibility, and harm prevention (Alkhamsi & Alqahtani, 2024; Bunyamin, 2021).

This paper restructures GDPR, CCPA, and PDPL data protection negligence into a Sharia-based legal framework utilizing doctrinal, institutional, and ethical elements. Comparisons show how civil, Islamic, and common law define, operationalize, and enforce negligence. This research shows PDPL flaws and proposes legislative change that blends culturally resonant moral obligation and harm reduction notions with globally accepted legal norms of accountability and reasonable care. This research shows that Middle Eastern digital governance reform talks must blend ethical jurisprudence with technological regulation for sustainable digital transformation. This paper claims that a clear and contextually grounded negligence norm will improve the PDPL, raise public trust, align Saudi Arabia with international data protection rules, and strengthen its regional leadership in ethical and effective data governance.

LITERATURE REVIEW

In digital economies, personal data drives innovation, government, and social involvement. Public trust in digital platforms for financial transactions, healthcare access, and communication relies on secure and lawful processing of personal data (Dąbrowska et al., 2022; Pimenta Rodrigues et al., 2024). However, organizational neglect, supervision, or compliance issues can lead to data breaches (Filler et al., 2022; Tschider, 2024). Due to these changes, data protection policymakers and attorneys globally redefined responsibility and accountability. In tort law and digital governance, negligence reveals data protection breach liability (Hylton, 2014; Posner, 2004).

Regulatory philosophy, enforcement culture, and ethics affect data protection negligence legislation by nation. The GDPR and CCPA are the main worldwide negligence-based accountability laws while Saudi PDPL combines Sharia law and international principles (Sarabdeen & Mohamed Ishak, 2025). This section critically examines data protection negligence across regimes and how Sharia-based moral and legal notions may enhance Saudi approach.

The Evolution of Negligence

Posner (2004) defines negligence as doing poorly in similar situations that produce damage. Poor data management costs money, reputation, and information, along with physical suffering (Morrow & Fitzpatrick,

2020). The information economy has created fiduciary connections between data controllers and less powerful and knowledgeable people (Balkin, 2016). Thus, data protection negligence arises when a data controller or processor fails to take necessary technological, administrative, or organisational measures to prevent data breaches, unauthorized access, or misuse (Kesan & Hayes, 2018).

Legal philosophy swings from tort to regulatory negligence. Data privacy laws stress prevention over compensation (Hamon et al., 2022). Being negligent reduces corporate disobedience, encouraging conformity. According to Posner (2004) and Hylton (2014), data governance incorporates the economic rationale for negligence, balancing preventative expenditures against anticipated harm, where ignoring cybersecurity may cost society more than prevention. This indicates data governance and global data protection now accept irresponsibility.

Negligence Lawa in EU, USA, and Saudi Arabia

The GDPR became the most complete and required global data protection standard in 2018. It turns ignorance into responsibility and reactive compliance into proactive compliance (Voigt & von dem Bussche, 2017; Quinn & Malgieri, 2021). Although the regulation does not define "negligence," Articles 24 and 32 require data controllers to adopt "appropriate technical and organizational measures" to limit data processing risk. Disobeying these tasks is reckless. These bans cover controller duty of care violations in risk assessment, encryption, and personnel training (European Commission, 2018; Lim & Oh, 2025). Article 5(2) accountability requires data controllers to comply. Proactivity shifts carelessness from blame to compliance (Hamon et al., 2022). GDPR sanctions of up to 4% of global sales or €20 million discourage disregard. Lloyd v. Google LLC (2021) and Google Spain SL v. AEPD (2014) show the European judiciary's data protection neglect. The GDPR institutionalizes negligence via legal, economic, and ethical accountability (Quinn & Malgieri, 2021; Zhao et al., 2023).

The CCPA protects consumers through statutory negligence, whereas the GDPR employs rights-based administrative approaches. The CCPA requires "reasonable security measures and practices" for data in 2018. California Civil Code 1798.150 allows private security data breaches lawsuits. Corporate responsibility protects consumers through CCPA negligence. Data protection bodies execute the GDPR administratively, while the CCPA permits anybody to sue, democratising enforcement and extending negligence-based liability (Masur, 2020). The Equifax Data Breach Settlement (2020) established statutory negligence for failing to maintain basic encryption and risk management (Tarra & Mittapelly, 2024), supporting this approach. Although beneficial, US federal consistency has slowed CCPA implementation (Crepax, 2024). It disregards consumer rights over regulations. The GDPR and CCPA stress institutional responsibility and individual empowerment, respectively, and organize data protection law around negligence.

Saudi Arabia's first comprehensive data gathering, processing, and transfer rule was M/19 in 2021 and changed in 2023. The law encourages digital transformation and sustainable governance within Vision 2030 (Sarabdeen & Mohamed Ishak, 2025). Saudi Data and Artificial Intelligence Authority (SDAIA) keeps the PDPL secure. Although wide, the PDPL lacks clarity and enforcement (Alhejaili, 2024; Abobaker, 2024a). Article 19 compels firms to "implement key organizational, administrative, and technical measures" to protect personal data, but it does not specify the care or foreseeability conditions that cause negligence in other systems. SDAIA administers the PDPL's data management lawsuit ban. Due to private enforcement and deterrent constraints, Saudi courts seldom punish negligence (Alkhamsi & Alqahtani, 2024). Regulated overlap and supervisory independence are lower than the European Data Protection Board (Kanojia, 2023). Saudi Arabia follows Sharia law, therefore neglect must balance morals and process.

In Islamic jurisprudence (fiqh), negligence (taqṣīr or ta'addī) is more extensive than in Western law. This involves legal and moral negligence in preventing harm (dar' al-mafāsid) (Bunyamin, 2021). Trust (amanah) encourages care, as Qur'an 4:58 indicates, "Allah requires you to render trusts to whom they are due". Therefore, misusing personal data is illegal and untrustworthy. GDPR preventive liability and Sharia's no hurt, no reciprocation (la darar wa la dirar) emphasize damage prevention. Islamic law recognizes liability for both intentional and unintentional negligence (Alhejaili, 2024). These ideas establish a culturally consistent framework for combating data carelessness in Saudi law when combined with data protection rules. By making compliance moral and legal, they encourage Islamic responsibility and international governance.

Theories of Negligence

Despite greater data protection awareness in Saudi Arabia, intellectual and policy discourse is lacking. Compliance processes, not legal negligence, are most researched (Alhejaili, 2024; Alkhamsi & Alqahtani, 2024). Few scholars have explored incorporating Sharia ideas like amanah and taqṣīr within negligence frameworks. In addition, GDPR and CCPA-PDPL comparisons are few, making it hard for Saudi Arabia to embrace worldwide best practices. Finally, the PDPL's recent adoption hinders enforcement and court interpretation research. These

problems need conceptual comparison of the Saudi PDPL to global regulatory trends and Islamic law. Integration increases Kingdom data protection law clarity, enforcement, and ethics.

Data protection negligence is shifting from harm compensation to institutional responsibility. CCPA, GDPR redefine digital duty of care. Although sophisticated, the Saudi PDPL needs a theoretical definition of negligence and stronger enforcement. Trust, responsibility, and harm prevention distinguish Sharia division. Western regulations and Islamic beliefs form a composite philosophy. PDPL negligence as a fiduciary trust violation (amanah) rather than a procedural failure links legal and moral blame.

RESEARCH METHOD

This Sharia-based qualitative doctrinal and comparative study assesses GDPR, CCPA, and Saudi PDPL. This research examines legal norms, conceptions, and legislative interpretation, not assessment. Doctrinal legal theory examines the law as written, interpreted, and applied, whereas comparative legal theory examines parallels, divergences, and lessons from other regimes that may impact Saudi law. Specified, culturally consistent, and internationally standardized data protection negligence.

This exploratory, qualitative research examines legislation, judicial judgments, and academic opinions. Qualitative research prioritizes legal reasoning, normative meaning, and conceptual clarity above numbers. Given Saudi law's lack of PDPL negligence research, it is crucial. The PDPL is evolving, but the GDPR and CCPA are global. PDPL can meet Saudi Arabia's Vision 2030 goals for sustainable digital transformation and regulatory modernization by evaluating these frameworks' weaknesses.

Every study data is secondary, including legal. To discover interpretation patterns, we investigated GDPR (EU Regulation 2016/679), CCPA (California Civil Code §1798.100–1798.199), and PDPL (Royal Decree No. M/19, 2021, and 2023), court decisions and regulation documents. This study examined Islamic legal principles, such as, trust, responsibility, accountability, and harm avoidance using primary sources from the Qur'an, Hadith, and classical jurisprudential literature (fiqh al-muamlat). Scopus, Web of Science, and HeinOnline provide peer-reviewed books, policy papers, and research on negligence, data protection, and comparative legal reform that influence Islamic philosophy. Post-GDPR analysis requires only 2018-published documents.

Second, normative comparison evaluates duty of care, negligent non-compliance liability, data subject redress, and compliance supervision institutions. Third, doctrinal synthesis links Saudi Sharia to GDPR and CCPA to create a contextually tailored legal paradigm that incorporates morality. The research examines doctrine and topics. Doctrinal interpretation identifies concepts, purposes, and relationships in legal works by analyzing coherence and ambiguity. Thematic content analysis clusters accountability, sufficient care, harm reduction, and comparative synthesis ethics.

Triangulation, cross-jurisdictional comparison, and interpretation consistency give this research academic rigor, validity, and dependability. We research legal and academic literature from several authoritative jurisdictions to avoid contextual gaps. Systematic purposive and contextual interpretation analysis is reliable (Hutchinson & Duncan, 2012). Jurisprudential integration of Sharia-based materials from ancient Islamic academics and current legal theorists provides theological truth and normative coherence. Doctrinal rigor and comparative breadth boost academic and policy credibility and transferability.

COPE-based research promotes legal interpretation integrity, transparency, and intellectual honesty. It uses public secondary data without harming anybody or requiring ethics. Scholars must interpret religious texts ethically and politely. Research allows objective interpretation that respects legal traditions. Though effective, this method has drawbacks. The PDPL lacks carelessness data and legal precedents since its founding. Both theoretical and normative methods use similar systems and textual interpretation. Study subjects combine policy and law. As PDPL enforcement increases, expert interviews or case studies may improve this doctrinal study.

The paper examines data protection negligence using rigor, comparative understanding, and normative synthesis. The paper reviews the GDPR, CCPA, and PDPL within a Sharia-based ethical framework to address doctrinal issues and establish Saudi Arabian data governance theory. This technique provides academically sound, culturally grounded, and practically applicable study results, setting the framework for aligning global data protection laws with Saudi moral and legal values.

FINDINGS

The GDPR and CCPA have strict data protection laws, while the PDPL is under preparation, according to this article. Comparative studies show regulatory philosophy, enforcement techniques, and legal culture affect negligent liability. Since carelessness exceeds Sharia law's responsibilities, data protection is a legal and ethical trust. Deep understanding ensures PDPL normative consistency and worldwide compatibility. Initial conclusion: data

protection regulations characterize negligence. GDPR/CCPA negligence requires compliance, transparency, and prevention. GDPR Articles 24 and 32 hold the controller accountable for not implementing "appropriate technical and organizational measures". This notion makes carelessness a proactive compliance principle that holds parties liable for direct harm and data-related risk management failure. CCPA punishes corporations for not having "reasonable security systems and practices." Consumers can sue without fees, empowering and discouraging. These efforts demonstrate universal consensus that data protection negligence is systemic, not a tort.

Structure and scope are similar to the GDPR, although the Saudi PDPL does not mention carelessness or data breach culpability. Article 19 of the PDPL requires "necessary organizational, administrative, and technical measures" but does not define "reasonable" care. The ambiguity makes intentional misconduct, extreme negligence, and regular oversight difficult to identify. The PDPL limits victims' remedies to administrative agencies like the Saudi Data and AI Authority without private rights. DPAs and CPPA can prosecute negligence, but SDAIA cannot. Uncertainty surrounds implied PDPL carelessness.

Third, compare enforcement and accountability. Two-tiered GDPR charges of up to €20 million or 4% of worldwide sales discourage and promote proactive compliance. CCPA administrative oversight and private enforcement enable regulators and consumers to hold data controllers responsible. PDPL fines are administrative, not based on organization size or violation severity. The PDPL struggles to address global service provider transnational data breaches without international judicial participation. The PDPL presume negligence, unlike the GDPR and CCPA.

Cultural and moral philosophy parallels on legal culpability are insightful. Negligence is legally defined by risk management and consumer rights in Europe and California. In Saudi Arabia, negligence analysis is based on Sharia jurisprudence, which relates legal blame (mas'ūliyyah) to moral obligation (takl Islamic legal notions like la darar wa la dirār (no harm, no reciprocation) and darʾ al-mafasid (damage prevention) enhance GDPR's preventive negligence framework. Trust (amanah) moralizes corporations' data protection duty. This intersection of Islamic ethics and modern accountability theory reveals that Saudi Arabia has a unique jurisprudential foundation for a hybrid legal paradigm with global and local values.

Islamic data protection law redefines negligence. Sharia punishes disobedience and obligations. Data controllers that fail to secure data are untrustworthy. A second component supports PDPL negligence interpretation fiduciary obligation. Research links GDPR's risk-based preventative measures to Sharia's taqṣīr standard (fault by omission). Integrating these frameworks would allow Saudi law to define negligence as a moral-legal continuum where data protection is ethical and compliant.

Another discovery is that global and Saudi views may match. GDPR, CCPA, and PDPL seek to manage personal data correctly and publicly despite simple variances. All three systems agree on data transparency, technology security, and institutional accountability. Saudi Arabia must define negligence, create independent monitoring, and add severity-based PDPL fines to harmonize. Saudi Arabia's internal credibility and global leadership in culturally based data governance will increase due to Islam's trust and harm prohibition in legal interpretation. Data protection policies lack conceptual clarity and enforcement. GDPR and CCPA function because they have defined criteria and institutional capacity to monitor and punish carelessness. Table 1 shows a summary and comparison of three laws.

Table 1: Summary and Comparison of Negligence Law

Dimension of Analysis	GDPR (European Union)	CCPA (California, USA)	PDPL (Saudi Arabia)	Sharia-Based Theoretical Synthesis	Implications for Saudi Legal Reform
Legal Philosophy	Rights-based framework emphasizing accountability and proportionality; negligence embedded in the duty of preventive care (Art. 24, 32).	Consumer-centric framework; negligence codified as statutory liability linked to "reasonable security practices."	Compliance-oriented with limited articulation of negligence; focuses on organizational obligations without defining "reasonable care."	Sharia emphasizes *amanah* (trust), *mas'uliyyah* (responsibility), and *la darar wa la dirar* (no harm) — aligning with preventive accountability.	Integrate ethical accountability with legal compliance by explicitly linking negligence to *amanah* and duty of care.
Definition of Negligence	Implicit; defined through omission of adequate technical and organizational safeguards.	Explicit; failure to implement reasonable security measures triggers liability.	Absent; Article 19 mandates protective measures but lacks clarity on what constitutes "negligence."	Negligence (*taqṣir*) in Sharia is both moral and legal failure to fulfill entrusted responsibility.	Include a statutory definition of negligence referencing both legal omission and ethical dereliction of duty.
Enforcement Mechanism	Independent supervisory authorities (DPAs); fines up to €20 million or 4% of global turnover.	Dual enforcement: Attorney General oversight and private right of action for consumers.	Centralized under SDAIA with limited independence and no private right of action.	Emphasizes communal oversight (*hisbah*) and institutional responsibility under *maqaṣid al-shari'ah* (objectives of Sharia).	Establish an independent oversight authority and enable partial citizen redress mechanisms consistent with Sharia's justice principles.

Accountability Framework	Proactive accountability: data controllers must demonstrate compliance (Art. 5(2)).	Reactive accountability: liability established post-breach through civil litigation.	Procedural accountability: organizations required to comply, but evidentiary burden unclear.	Accountability (*muḥāsabah*) viewed as both divine and legal obligation; aligns with preventive legal ethics.	Shift toward demonstrable accountability (e.g., audits, compliance reports) grounded in Islamic ethical reasoning.
Scope of Liability	Applies to all controllers/processors within and outside EU processing EU citizens' data.	Applies to for-profit entities meeting data volume thresholds; limited to California residents.	Applies to data collected in the Kingdom; limited cross-border scope.	Sharia recognizes transboundary ethical responsibility for harm (*dar' al-mafāsid*).	Expand PDPL's extraterritorial application and align with global cross-border data principles.
Remedies and Sanctions	Strong financial penalties and corrective orders; negligence attracts administrative fines.	Statutory damages (USD 100–750 per consumer per incident) for negligent breaches.	Sanctions administrative and monetary but not proportionate to severity or size.	Sharia prioritizes restitution (*diya*) and restoration of harm (*iṣlāḥ*).	Introduce tiered penalties linked to severity, harm, and organizational scale.
Cultural and Ethical Foundations	Secular, rights-driven legal culture emphasizing transparency and risk mitigation.	Market-driven model emphasizing consumer autonomy and private enforcement.	Emerging compliance culture; evolving awareness of privacy as a human right.	Rooted in divine trust, moral restraint, and public welfare (*maṣlaḥah*).	Institutionalize ethics training and awareness programs promoting trust (*amanah*) and privacy culture.
Theoretical Integration	Based on preventive liability and proportional accountability.	Based on consumer empowerment and deterrence.	Based on administrative control and compliance without moral codification.	Integrates moral-legal duty, harm prevention, and trust preservation.	Develop a hybrid model blending preventive accountability with Sharia-derived ethical governance.
Overall Assessment	Mature system embedding negligence in accountability structures.	Evolving but strong consumer-driven enforcement model.	Foundational law with limited doctrinal clarity on negligence and weak enforcement independence.	Offers moral and jurisprudential depth aligning with preventive ethics.	Codify negligence explicitly, strengthen enforcement institutions, and embed Sharia-based moral accountability for sustainable digital governance.

GDPR and CCPA involve negligence in responsibilities (Table 1). Both systems combine legal, technical, and organizational reasonable care to make carelessness a proactive compliance responsibility. Although comparable, the PDPL lacks definitional accuracy, procedural enforcement independence, and negligence as a legal standard. The Saudi Arabian PDPL needs conceptual clarity and institutional growth to be accountable. Sharia improves Saudi law. Islamic ideals of amanah (trust) and mas'ūliyyah (responsibility) integrate morality into legal compliance, complementing modern accountability. Sharia-based negligence goes beyond procedural failure to moral breach, emphasizing the legal and ethical need to preserve personal data. La darar wa la dirar supports GDPR's data protection and preventative logic. Comparative research shows ethical jurisprudence enhances Saudi data privacy. PDPL hybrid governance may be current, culturally real, and globally credible due to global regulatory systems and Islamic moral philosophy. Law and ethics build public trust and realize Vision 2030's responsible digital transformation and good governance based on Saudi religion and culture.

DISCUSSION

This study indicates intellectual traditions hamper data protection negligence law and ethics. Accountability Theory drives regulation, whereas Tort Law shapes negligence in Western legal systems. Saudi Arabia and Islamic law need trust, damage avoidance, and Sharia, making negligence moral and jurisprudential. Saudi Arabia's culturally based legal system requires a multifaceted view of negligence that goes beyond civil responsibility and includes ethical stewardship to justify and improve data security.

Not taking due care is tortious negligence. Agents must prevent projected harm (Prosser, 1971). GDPR and CCPA preventive architecture require data controllers to anticipate and manage risks. Lack of planning produces carelessness, not devastation. Reactive liability versus proactive risk management advises avoidance above compensation. Damage assessments, breach reports, and data audits make vigilance GDPR negligence. The CCPA's "reasonable security measures and practices" regulation holds digital enterprises accountable.

It appears PDPL is administrative regulation, not tort responsibility. Although it requires "necessary measures," it does not define reasonableness or data subject duty. Lack of a standard of care separates negligence from quantitative rules, weakening tort law. PDPL needs court precedence and responsibility to deter. To hold PDPL accountable, the report offers a tort-like duty of care that defines negligence as a failure to exert "reasonable preventive diligence".

Tort Theory defends carelessness, but Accountability Theory illustrates how it developed a systemic governance model. Beyond individual liability, modern regulatory systems need institutional responsibility, openness, and accountability (Bovens, 2007; Mulgan, 2014). Data controllers must follow GDPR. Future proof, documentation, and monitoring, not retrospective blame, of institutions' actions. Through legislation and private action, CCPA multi-level accountability democratizes data governance.

A Saudi Data and AI Authority monitors PDPL accountability. Saudi Arabia's state-led administration lacks GDPR and CCPA pluralized accountability. Without independent control and limited court review, irresponsible interpretation is limited. Accountability Theory prioritizes government over citizens in vertical accountability. While simplifying law, this paradigm diminishes digital legitimacy's openness and confidence. Integrating Sharia's muhāsabah concept can improve the PDPL's accountability system in a culturally appropriate manner. Islamic governance demands moral, spiritual, institutional, and procedural responsibility. The dual strategy meets GDPR transparency and accountability. Data governance as amanah (entrustment) may enable Saudi firms view accountability as moral rather than regulatory. The paper proposes a hybrid PDPL accountability model based on institutional monitoring and internalized ethical obligation, combining modern regulatory logic with Islamic ethics.

Reinterpreting negligence via Sharia jurisprudence (Fiqh al-Muʿāmalāt) is critical. Islamic law considers carelessness (taqṣīr or ihmāl) a moral and social obligation infringement, not only a technical failure. The Quran's "Do not betray your trusts" and "everyone of you is a shepherd, and everyone of you is responsible for his flock" promote ethical accountability. Data controllers are moral and legal custodians of personal data. Poor data security breaks trust and law. Harm prevention (la darar wa la dirar) mitigates GDPR risk. Islam's maslahah (public welfare) emphasizes that the collective good above individual accountability, supporting data protection's social aspect These theories give an ethical framework for modern administration that addresses PDPL normative issues. Sharia-based data ethics is spiritual-moral since carelessness affects justice, trust, and human dignity, unlike secular techniques that consider it as procedural failure. Islamic duty and legitimacy underpin Saudi law.

Accountability Theory, Tort Theory, and Sharia law combine legal and ethical accountability. Under these theories, negligence is systematic legal, ethical, and social failure. Organizations must manage digital trust legally and morally. Negligence ranges from individual omission to institutional weakness, requiring multi-tiered supervision. Saudi Arabia's PDPL may encourage incorporation. Clear laws defining negligence as failure to exercise legal and ethical care. Therefore, regulators are advised to integrate ethical principles (amanah and mas'ūliyyah) with data governance guidelines. Public responsibility that followed Islamic justice limited individual remedies. The reform will defend Sharia and connect Saudi Arabia's data governance with global best practices. It would promote Vision 2030's integrity-, innovation-, and trust-based knowledge economy. This hybrid strategy shows Sharia promotes ethical legal change.

IMPLICATIONS

The study indicates that positive laws increase negligence. Comparative legal study is easier with Sharia and Western legal systems' normative, spiritual, procedural, and moral requirements. These findings imply Saudi officials must enact laws and rules for reducing negligence. Digital economy enforcement and citizen trust would improve by punishing negligence with fines. Data protection laws neglect the evaluation of ethics, innovation, human dignity, autonomy, accountability, and efficiency in existing law. Saudi Arabia's strict data protection law influences global digital ethics issues. A hybrid legal-ethical paradigm that combines tradition and modernity, law and morality, government control and private trust may enable the Kingdom reconcile Western law's correctness with Islamic morality.

This work intellectually and practically enhances Western and Islamic data protection and negligence literature. The study enriches literature by expanding negligence beyond tort law. Classic tort theory treats negligence as reactive harm healing based on the "reasonable person" criterion. Modern data protection methods intentionally and purposefully require laws for negligence, supporting accountability theory. Institutions need openness, attentiveness, and prevention, but this is risky. Make negligence an anticipatory governance principle that protects data subjects from recognized threats in a digitalized world to increase accountability theory. Another theoretical contribution is incorporating Shariah law (Fiqh al-Muʿāmalāt) into global data governance discussions. Trust, accountability, and non-retaliation make legal duties spiritual and ethical. This moral component ties exterior accountability to inside moral consciousness, making neglect a legal and ethical paradigm beyond positivist interpretations.

The research creates a hybrid jurisprudence that combines Western reasoning and Islamic norms. Islamic morality and public benefit (maslahah) strengthen regulatory systems, according to this theory. The report impacts Saudi Arabia's Personal Data Protection Law amendments and institutions. The findings imply codifying negligence as failing to exercise reasonable preventative measures will clarify and enforce the PDPL. Second, the paper emphasises the need for an independent supervisory body like the European Data Protection Authorities to

guarantee institutional autonomy and impartiality. Third, amanah-based corporate codes of conduct strengthen business trust and compliance by linking legal and moral obligations. Realistic and graded punishments for data breaches align with Sharia concepts of justice (ʿadl) and damage avoidance, according to research.

Saudi Vision 2030 seeks to lead digital innovation while protecting culture and morals. The PDPL can show regulatory sophistication and cultural authenticity by implementing Sharia-based data protection. Islamic and developing nations may match global data protection rules with their moral and legal systems using this hybrid technique. This study modernizes ethics in the digital era utilizing normative theory and policy design.

CONCLUSION

This study investigated data protection negligence in the GDPR, CCPA, and PDPL. Comparative and normative study demonstrated that the GDPR and CCPA operationalized negligence as proactive accountability, whereas the PDPL is still emerging with definitional uncertainties and insufficient enforcement. Global best practices and Shariah ethics may help PDPL. According to Tort Theory, Accountability Theory, and Islamic law, data management negligence violates trust. Integrating ethics into legislative interpretation gives the PDPL moral-legal obligations beyond procedural compliance. The analysis reveals that Saudi Arabia's legal modernization offers a rare potential to blend global and indigenous rules. This will improve the Kingdom's data administration and demonstrate how Islamic law may benefit global law. Shariah balances innovation, justice, and social welfare in modern government, research finds. The proposed hybrid paradigm prioritizes amanah, mas'ūliyyah, and ʿadl as ethical standards for digital economy administration.

Despite theoretical and comparative value, the research has major limitations. The study included only law, research, and policy inform doctrinal, qualitative analysis. Insufficient evidence and legal precedent make irresponsible interpretation and implementation of the PDPL difficult to prove. Second, Saudi Arabia's new data protection system's Shariah compliance and implementation are unclear. Third, the research prioritizes legal and ethical negligence above enforcement-related technology and cybersecurity challenges. Further studies are recommended to examine UAE, Malaysia, Saudi Arabia, and other Western nations.

Future research should employ empirical and transdisciplinary methodologies to validate and broaden this study's conceptual framework. Saudi legal experts, politicians, and data protection officials may disclose important knowledge and practice in qualitative interviews or focus groups. Future study may examine Shariah-based nations' jurisprudential analysis to understand how Islamic principles impact data governance in different socio-legal contexts. Through business ethics and compliance, quantitative research can quantify data protection morality.

Research should study how AI, blockchain, and cross-border data migration effect Islamic negligence and duty. International data ecosystems need ethical governance that balances local and global laws. Lastly, a Shariah-based digital ethics paradigm based on Quranic and jurisprudential sources may boost worldwide debates on digital trust, privacy, and morality This study found that data protection negligence symbolizes digital societies' trust, duty, and justice, not compliance. Islamic law adds morality to obligation, while Western law is procedural. Saudi Arabia may lead a new ethical digital governance paradigm that combines international and Islamic law.

REFERENCES

Abobaker, A. (2024a). Data protection and privacy governance in Saudi Arabia: Evaluating the Personal Data Protection Law (PDPL) in context. *Arab Law Quarterly*, 38(2), 145–168.

Alhejaili, M. (2024). Data privacy and Sharia law: Reassessing personal data protection in Saudi Arabia under Vision 2030. *Journal of Law and Digital Governance*, 12(1), 33–57.

Alkhamsi, R., & Alqahtani, M. (2024). Personal data protection in Saudi Arabia: Challenges and opportunities under the PDPL framework. *International Review of Law, Computers & Technology*, 38(3), 201–223.

Almulihi, A., Alghamdi, S., & Alharbi, H. (2022). Cybersecurity awareness and data breach incidents in Saudi Arabia: An empirical analysis. *Information & Computer Security*, 30(4), 512–533.

Balkin, J. M. (2016). Information fiduciaries and the First Amendment. *UC Davis Law Review*, 49(4), 1183–1234.

Bunyamin, M. (2021). Negligence and moral responsibility in Islamic jurisprudence: Revisiting the concept of taqṣīr. *Islamic Law Review*, 15(1), 77–95.

Crepax, N. (2024). Fragmented privacy: The limits of consumer protection under the California Consumer Privacy Act (CCPA). *Yale Journal of Regulation*, 41(2), 327–354.

Dąbrowska, J., Pérez, M., & Silva, R. (2022). The value of personal data in the digital economy: Challenges for governance and policy. *Telecommunications Policy*, 46(3), 102–118.

European Commission. (2018). General Data Protection Regulation (GDPR): Regulation (EU) 2016/679. *Official Journal of the European Union*.

Filler, T., Becker, K., & Wiese, M. (2022). Corporate negligence in data governance: Organizational risk and accountability. *Journal of Business Ethics*, 179(2), 409–426.

Hamon, R., Junklewitz, H., & Sanchez, I. (2022). The concept of accountability in the GDPR and its transformative effect on compliance. *Computer Law & Security Review*, 44, 105626. https://doi.org/10.1016/j.clsr.2022.105626

Hylton, K. N. (2014). *Tort law: A modern perspective*. Cambridge University Press.

Juma'h, A., & Alnsour, Y. (2020). Cyber threats and data breaches in GCC countries: Legal and institutional responses. *Middle East Policy*, 27(4), 82–99.

Jun, H., & Kim, D. (2024). Digital negligence: Corporate liability in the era of data-driven risk. *Journal of Cybersecurity Studies*, 10(2), 111–135.

Kanojia, R. (2023). Emerging data protection frameworks in the GCC: Comparative analysis of PDPL, DIFC, and ADGM laws. *Journal of International Privacy and Data Law*, 9(1), 45–68.

Ke, T., & Sudhir, K. (2023). Trust, negligence, and data responsibility in digital markets. *Journal of Marketing Research*, 60(1), 92–112.

Kesan, J. P., & Hayes, C. (2018). Mitigating cyber risk: Data breach, negligence, and the role of regulation. *Iowa Law Review*, 103(2), 117–159.

Koepke, L., & Kaminski, M. (2020). Consumer privacy and negligence under the CCPA: Lessons from early enforcement. *California Law Review Online*, 11(1), 51–68.

Lim, S., & Oh, J. (2025). GDPR enforcement and corporate accountability: Trends in EU data protection jurisprudence. *European Law Journal*, 31(1), 55–73.

Masur, J. S. (2020). Privacy, deterrence, and negligence in digital regulation. *Harvard Law Review*, 133(6), 1885–1932.

Morrow, K., & Fitzpatrick, R. (2020). Data protection and the law of negligence: Rethinking harm in the information age. *Legal Studies*, 40(3), 355–374.

Pimenta Rodrigues, F., Chen, Y., & Soares, A. (2024). Digital transformation, data governance, and public trust: A global review. *Government Information Quarterly*, 41(2), 101–125.

Posner, R. A. (2004). *Economic analysis of law* (7th ed.). Aspen Publishers.

Quinn, P., & Malgieri, G. (2021). Accountability and risk in the GDPR: A doctrinal and normative analysis. *International Data Privacy Law*, 11(3), 233–249.

Sarabdeen, J., & Mohamed Ishak, N. (2025). Data protection, Sharia, and regulatory convergence: Saudi Arabia's Personal Data Protection Law in comparative perspective. *Arab Law Quarterly*, 39(1), 75–99.

Tarra, M., & Mittapelly, R. (2024). Corporate negligence and liability in major data breach settlements: Lessons from Equifax and beyond. *Journal of Cyber Law & Policy*, 18(2), 144–168.

Teichmann, F., & Wittmann, M. (2023). Negligence and accountability in data governance: Comparative insights from the EU and MENA regions. *Computer Law Review International*, 24(1), 9–24.

Thomas, D., Patel, R., & Ahmed, S. (2022). Negligence and liability in cross-border data transfers. International Journal of Law and Information Technology, 30(4), 315–338.

Tschider, C. (2024). Data governance failures and the problem of organizational negligence. *Minnesota Journal of Law, Science & Technology*, 25(2), 231–274.

Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer.

Williams, S. (2020). Negligence and accountability under the California Consumer Privacy Act (CCPA). *Stanford Technology Law Review*, 23(1), 1–28.

Zhao, X., Li, J., & Nguyen, H. (2023). Data protection and negligence liability: Comparative evidence from the EU and Asia-Pacific. *Journal of Comparative Law & Technology*, 19(4), 455–478.

