http://dx.doi.org/10.18623/rvd.v22.n3.3404

THE CONCEPT OF NEGLIGENCE IN DATA BREACH: A COMPARATIVE DOCTRINAL ANALYSIS OF THE EU, CALIFORNIA, AND SAUDI ARABIA

O CONCEITO DE NEGLIGÊNCIA NA VIOLAÇÃO DE DADOS: UMA ANÁLISE DOUTRINAL COMPARATIVA DA UE, CALIFÓRNIA E ARÁBIA SAUDITA

Article received on: 7/25/2025
Article accepted on: 9/26/2025

Hanan Ali Alnasser*
*Faculty of Law, Universiti Malaya, Kuala Lumpur, Malaysia
hananalnasser97@gmail.com

The authors declare that there is no conflict of interest

Abstract
Data privacy and its safeguarding have become a critical concern for individuals, corporations, and governments worldwide in the swiftly advancing digital era. The concept of negligence has emerged as an important determinant of liability in data breach cases, yet it is disproportionately defined across jurisdictions. This paper undertakes a comparative doctrinal analysis of neg-ligence under the European Union's General Data Protection Regulation (GDPR), California's Consumer Privacy Act (CCPA), and Saudi Arabia's Personal Data Protection Law (PDPL). By examining statutory texts and legal commentary, the study explores how each regime frames the core elements of negligence in tort law (duty of care, accountability, and foreseeability). The research finds that while the GDPR and CCPA incorporate implicit negligence standards through accountability and reasonable security measures, and private rights of action, the PDPL remains underdeveloped both procedurally and doctrinally; It lacks key mechanisms such as private rights of action, an enforcement mechanism, and interpretive guidance. The study uniquely contextualises Saudi's PDPL within its Sharia-based legal tradition, arguing for a culturally rooted reconstruction of negligence arising from moral principles of amanah (trust) and la darar wa la dirar (no harm, no reciprocation of harm). The paper recommends statutory amendments, the formation of an autonomous supervisory body, and the amalgamation of culturally echoed standards of care to enhance legal accountability and data governance in the Kingdom.

Keyword: Data Protection Governance. Negligence Standard. Saudi Arabia. GDPR. CCPA.

Resumo
A privacidade de dados e sua proteção tornaram-se uma preocupação crítica para indivíduos, empresas e governos em todo o mundo na era digital em rápido avanço. O conceito de negligência emergiu como um importante determinante da responsabilidade em casos de violação de dados, embora seja definido de forma desproporcional entre as jurisdições. Este artigo realiza uma análise doutrinária comparativa da negligência sob o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, a Lei de Privacidade do Consumidor da Califórnia (CCPA) e a Lei de Proteção de Dados Pessoais (PDPL) da Arábia Saudita. Examinando textos estatutários e comentários jurídicos, o estudo explora como cada regime enquadra os elementos centrais da negligência no direito civil (dever de cuidado, responsabilização e previsibilidade). A pesquisa conclui que, embora o GDPR e o CCPA incorporem padrões implícitos de negligência por meio de responsabilização e medidas de segurança razoáveis, e direitos privados de ação, o PDPL permanece subdesenvolvido tanto processual quanto doutri-nariamente; carece de mecanismos-chave, como direitos privados de ação, um mecanismo de execução e ori-entação interpretativa. O estudo contextualiza de forma única a Lei de Proteção de Dados Pessoais (PDPL) da Arábia Saudita dentro de sua tradição jurídica baseada na Sharia, defendendo uma reconstrução culturalmente enraizada da negligência, decorrente dos princípios morais de amanah (confiança) e la darar wa la dirar (sem dano, sem reciprocidade de dano). O artigo recomenda emendas estatutárias, a formação de um órgão de supervisão autônomo e a fusão de padrões de cuidado culturalmente ecoados para aprimorar a responsabilização jurídica e a governança de dados no Reino.

Palavras-chave: Governança da Proteção de Dados. Padrão de Negligência. Arábia Saudita. GDPR. CCPA.

1 INTRODUCTION

Information privacy is among the most esteemed human rights in today's digital ecosystem. In the current digital landscape, privacy has emerged as a significant concern, as individuals increasingly share their personal data with internet platforms and services. Technological innovations offer unparalleled ease and connectivity, yet they also present complex challenges related to data security, surveillance, and user permissions. Reconciling the advantages of digital innovation with the imperative to protect individual privacy has emerged as a fundamental concern for governments, technologists, and society as a whole. The interconnection between technological innovation and institutional accountability is equally evident in the financial sector, where digitalisation and financial technology (FinTech) have redefined operational efficiency, profitability, and regulatory risk. Empirical findings from Jordanian commercial banks show that FinTech adoption significantly improves performance while simultaneously intensifying the need for robust governance and compliance systems to mitigate data-related vulnerabilities (Alshehadeh et al., 2022). This insight parallels the broader argument of this paper that legal systems must evolve to balance innovation with accountability, embedding negligence standards within digital governance frameworks.

In a data-centric environment, a significant percentage of business operations are carried out online, utilising personal data. Personal data has emerged as a cornerstone of contemporary governance, commerce, and public administration (Dąbrowska et al., 2022). Presently, while cyberspace is extensively used for the creation and management of online accounts, it also entails other legal challenges, such as identity theft, intellectual property violations, data breaches, and jurisdictional uncertainty; The convergence of physical and digital identities increasingly challenges legal frameworks, which often fail to adapt to the complexities of online interactions, underscoring the necessity for resilient and flexible legislation (Islam, 2022; Mirshekari et al., 2020). Information privacy has emerged as a significant problem on the worldwide political agenda (Islam, 2018). Within such an environment, ordinary citizens, as private individuals or customers, seek

sufficient protection. As a result, the global discourse on privacy issues has become evident. Organisations which mishandle personal information, due to “negligence”, i.e., failure to exercise “reasonable care” in data governance, thus expose individuals to “harms” ranging from identity theft to unlawful surveillance (Filler et al., 2022; Tschider, 2024).

In response to data privacy concerns, global legal regimes, such as the European Union’s General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), have responded by implementing principles of transparency, accountability, and liability into statutory directives, together with devices that associate deficient data management with legal negligence. Nevertheless, jurisdictions such as Saudi Arabia are still in the nascent phases of legislative development in the field of data privacy (Abobaker, 2024a; Kanojia, 2023). The Saudi Personal Data Protection Law (PDPL) represents an introductory step toward proclaiming data control and user protection. Nonetheless, the legislation has numerous substantive and procedural shortcomings. The issues encompass ambiguous definitions of critical categories, such as “personal data” and “sensitive data,” insufficient guidance on data subject rights, and a lack of clarity concerning the extent of extraterritorial applicability. Furthermore, the PDPL lacks an autonomous supervisory authority, which raises concerns regarding enforcement and accountability. In contrast to the extensive data protection frameworks in Western jurisdictions, such as the EU’s General Data Protection Regulation (GDPR), the PDPL's doctrinal clarity, implementation strategies, and interpretive guidance are underdeveloped, indicating a need for further legislative refinement and institutional support. (Sarabdeen & Mohamed Ishak, 2025).

The GDPR is widely acknowledged for its intricate legal framework, highlighting responsibility, data minimisation, breach notification, and privacy by design (Pimenta Rodrigues et al., 2024; Quinn & Malgieri, 2021). Although the GDPR does not explicitly mention the term "negligence," researchers concur that its compliance mandates effectively implement a legal norm similar to negligence by necessitating firms to address risks proactively (Filler et al., 2022). The CCPA, although less comprehensive, offers a consumer-centric framework that prioritises user empowerment and transparency. It significantly establishes statutory damages and reduces evidentiary burdens for plaintiffs, hence improving private enforcement alternatives (Williams, 2020). Notwithstanding these advancements, the literature indicates significant deficiencies in data privacy and

protection. The normative and theological aspects of negligence are inadequately established; Discussions predominantly concentrate on technological compliance or organisational vulnerability, neglecting the circumstances under which legal liability emerges from inadequate data governance (Masur, 2020; Zhao et al., 2023). In the context of Saudi Arabia, researchers like Kanojia (2023) and Alhejaili (2024) recognise the constraints of the PDPL, which include stringent restrictions on cross-border data transfers and a pronounced focus on data localisation, hindering multinational operations.

But do not theorise how negligence might be construed through Sharia law and contemporary data governance concepts.

The literature increasingly characterises organisational data mishandling not a separate technical failure, but as a systematic legal concern stemming from incompetence and insufficient accountability; Scholars advocate for legal reforms that establish a duty to safeguard personal data and include frameworks for negligence and restitution, so providing preventive measures and appropriate compensation for victims of data misuse (Bunyamin, 2021; Chandler, 2007; Claudia & Gunadi, 2023; Jun & Kim, 2024; Pemuli & Barkatullah, 2024; Setyawan et al., 2024; Sinaga, 2023; Weitzman, 2023). However, mainly due to the lack of explicit standards, the research also indicates persistent uncertainty in legal criteria for organisational negligence regarding data breaches (Teichmann & Wittmann, 2023; Thomas et al., 2022). Although negligence liability serves as a crucial deterrent against irresponsible activities, delineating "reasonable" security poses significant challenges. Major data breaches are frequently attributable to systemic organisational problems rather than single incidents, highlighting the need for legislative and regulatory mechanisms that can resolve the aim of successful deterrence against such data breaches and risk management (Juma’h & Alnsour, 2020; Jun & Kim, 2024; Khan et al., 2022; Schlackl et al., 2022).

Comparative studies of data protection regulations across jurisdictions (e.g., Malaysia, EU, Singapore, China) indicate that non-Western legal systems frequently do not meet international standards, especially regarding preventive and remedial actions for data breaches (Ikram, 2024; Sarabdeen & Mohamed Ishak, 2025). Although limited studies explicitly focus on data protection in Saudi Arabia, the existing literature predominantly emphasises the formulation and execution of data protection measures (Alkhamsi & Alqahtani, 2024; Kanojia, 2023; Nusairat, 2024). To the best of the author's knowledge, the extant scholarship appears to be deficient in terms of legal reasoning and

negligence liability from the lens of moral or religious "duties," rather than the duty prescribed under common or civil law systems. Therefore, this study attempts to relate to Saudi Arabia's legal system, which is rooted in alternative normative traditions, i.e., Sharia-based civil law. Since the intersection of legal negligence with cultural and spiritual factors remains insufficiently explored, the Saudi Arab's legal principles, grounded in fiqh al-muamalat and ethical precepts such as la darar wa la dirar (no harm, no reciprocation of damage), establish a unique normative framework for alleviating avoidable injury. Contrary to the Western legal systems, which characteristically explain the "negligence concept" through common law theories such as the "reasonable person" standard, Sharia-based principles emphasise the "moral duty" to prevent harm and to promote public interest. In this perspective, negligence liability arises not merely from breached legal duties but from failing to uphold ethical obligations that preserve the welfare (maslahah) of individuals and the community. These principles offer that harm arising from data breaches, where there is/was foreseeability or preventability, may establish an actionable negligence even in the absence of precise statutory language.

Therefore, this study argues that the concept of individual or organisational negligence in data protection can be re-explained within Saudi Arabia's Sharia-based legal framework, which requires moral and ethical duties such as the duty to prevent harm and maintain public welfare instead of relying exclusively on statutory standards.

The organisation of this article is as follows: The initial section delineates the research gap, objectives, and methodological framework, underscoring the importance of neglect in the context of data protection discourse. The second portion offers a comprehensive doctrinal examination of the formulation and implementation of negligence under the GDPR, CCPA, and Saudi Arabia's PDPL. A comparative review follows, highlighting convergences and divergences among the three legal systems, with an emphasis on duty of care, liability standards, and enforcement mechanisms. The fourth section rigorously analyses the normative and cultural aspects of the PDPL, emphasising the lack of interpretive guidance and the possible incorporation of Islamic legal ideas. The last section integrates the findings to recommend practical legal improvements for the Saudi data protection system, ending in a conclusion that emphasises the necessity for a strong, contextually relevant negligence rule.

This paper has three objectives: Analyses the legislative texts, judicial precedents, and regulatory structures in each country to comprehend the conception and enforcement

of negligence within the realm of data protection; Conducts a comparative legal analysis of the treatment of "carelessness" as a violation of data protection requirements under the GDPR (General Data Protection Regulation), the CCPA (California Consumer Privacy Act), and the Saudi Arabian Personal Data Protection Law (PDPL); and assess the efficacy of negligence-based enforcement methods in protecting personal data rights.

2 LITERATURE REVIEW

2.1 Theoretical foundations of negligence in data protection

"Negligence" in classical tort theory is liability for breaching a duty of care that causes harm, measured against what a "reasonable person" would do in similar circumstances. In digital environments, this standard has evolved to guide the conduct of data controllers and processors as breach risks rise (Jun & Kim, 2024). This study adopts a conceptual model in which the standard of care functions as the independent variable (IV), capturing diligence in safeguarding personal data; harm/injury (financial loss, reputational damage, privacy violations) is the dependent variable (DV); and organizational safeguards (policies, risk awareness, institutional practices, technical controls) operate as intervening variables that strengthen or weaken the IV→DV pathway (Hylton, 2014). The economic rationale is consistent with Posner (2004): negligence reflects failure to implement cost-justified precautions against foreseeable risks. Because data subjects entrust organisations with intimate information, the relationship is often framed through fiduciary duty, trust, and vulnerability (Balkin, 2016; 2020; Ke & Sudhir, 2023). Negligence in data governance thus straddles tort theory (duty/breach/causation/damage) and regulatory compliance, connecting trust violations to legal culpability.

2.2 From physical injury to non-physical harms

Digital harms extend beyond bodily or purely pecuniary injury to include privacy invasion, loss of autonomy, emotional distress, and time/monitoring costs (Kesan & Hayes, 2018; Morrow & Fitzpatrick, 2020; Vaka, 2020). Contemporary regimes increasingly recognise that failure to perform routine duties may ground negligence even

absent easily quantifiable loss (Hamon et al., 2022). This underpins the policy shift from reactive enforcement to proactive risk mitigation.

2.3 From duty of care to compliance: GDPR and CCPA

Although the GDPR does not use the word "negligence," it embeds its core elements:

Accountability (Art. 5(2)) and appropriate technical and organisational measures (Art. 32) operationalise reasonableness and foreseeability (Hamdani et al., 2021; Kaminski & Malgieri, 2020). DPIAs institutionalise anticipatory risk management, aligning with modern negligence theory. Non-implementation of adequate measures maps onto breach, with Art. 82 (compensation) and Art. 83 (fines) provide remedies and deterrence (Rogers, 2010; Terry, 2012; Voigt & Von dem Bussche, 2017; Giliker, 2010; Lim & Oh, 2025).

The CCPA/CPRA takes a consumer-centric route:

Transparency and control (Cal. Civ. Code §§1798.100-.150) resemble a duty to inform and protect;

A private right of action for breaches of non-encrypted/non-redacted data ties inadequate security to liability, translating "reasonable security" into a justiciable standard (Solove & Hartzog, 2014; Tene & Polonetsky, 2013). Together these frameworks support a hybrid accountability model, where regulatory lapses can evidence breach in civil suits and where proactive governance mitigates negligence exposure (Pernot-Leplay, 2020; Labadie & Legner, 2022; Wong et al., 2023).

2.4 From compliance to culpability

Both GDPR and CCPA/CPRA press beyond box-ticking: accountability requires verifiable compliance; weak risk assessments or poor minimisation can approach culpable negligence (Comandè & Schneider, 2021; Kaminski & Malgieri, 2020). The CPRA's risk-based enhancements (minimisation, purpose limitation, assessments) further raise the expected standard of care (Krishnamurthy, 2020; Stallings, 2020). In short, negligence is increasingly viewed as a form of continuous governance, grounded in proportionality and risk mitigation (Bankins et al., 2023; Dorton et al., 2023).

2.5 Cultural norms and Islamic legal principles

In Saudi Arabia, Islamic jurisprudence provides normative anchors for negligence, emphasising amanah (trust) and la darar wa la dirar (no harm, no harm reciprocated). These principles underscore moral duty and public welfare (maslahah) across various legal domains (Herijanto, 2022). These principles can translate into fiduciary-like obligations for data custodians. Current scholarship, however, notes that PDPL has yet to juridify these ethical norms into enforceable standards, leaving gaps in doctrinal precision and sectoral guidance (Abobaker, 2024a; Kanojia, 2023; Voss, 2021; Stallings, 2020).

3 METHODS

This study employs a doctrinal and comparative legal research methodology, combining qualitative analysis of primary and secondary legal sources to examine how negligence is conceptualized and enforced within three major data protection regimes: the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA/CPRA), and the Saudi Arabian Personal Data Protection Law (PDPL).

3.1 Research design and method

The doctrinal approach focuses on analysing existing legal instruments, judicial interpretations, and regulatory mechanisms to understand the principles governing negligence in data protection law. The comparative component systematically contrasts the substantive and procedural elements of negligence—such as duty of care, foreseeability, accountability, and enforcement—across the three jurisdictions. The analysis draws on interpretive reasoning and analogical comparison to identify both convergences and divergences among these legal systems.

3.2 Jurisdictional selection

The jurisdictions were selected on the basis of their representativeness and analytical complementarity:

The GDPR serves as the global benchmark for data protection, known for its comprehensive regulatory architecture, strong enforcement mechanisms, and implicit negligence standards embedded in accountability and data security provisions.

The CCPA/CPRA represents a consumer-centric, market-oriented model of data protection within a common-law context, emphasising transparency, reasonable security measures, and private rights of action.

The PDPL exemplifies an emerging framework in a non-Western, Sharia-based legal system, where concepts of trust (amanah) and harm prevention (la darar wa la dirar) provide potential normative foundations for developing a culturally grounded doctrine of negligence.

3.3 Sources of data

The study relies on both primary and secondary sources:

Primary sources include statutory instruments (GDPR 2016/679; CCPA 2018/CPRA 2020; PDPL 2021 and its Implementing Regulations), case law (notably GDPR enforcement cases by the European Data Protection Board and the Court of Justice of the European Union), and official regulatory guidance (e.g., California Privacy Protection Agency, SDAIA/NDMO implementation guidelines).

- Secondary sources encompass scholarly articles, legal commentaries, policy papers, and comparative analyses published in reputable journals and institutional repositories. These sources provide interpretive depth and contextual understanding of negligence, accountability, and liability in digital governance.

3.4 Analytical procedure

The research proceeds through three analytical stages:

Doctrinal interpretation of how negligence-related obligations are expressed in legislative texts and interpreted by regulatory or judicial authorities.

Comparative evaluation to assess how different legal traditions (civil law, common law, and Sharia-based systems) conceptualise the duty of care, foreseeability, and liability in data protection.

Normative synthesis that integrates the findings to propose how Saudi Arabia's PDPL can evolve by incorporating both international best practices and Islamic legal principles.

3.5 Limitations

The study acknowledges several limitations. First, Saudi jurisprudence and case law on data protection remain scarce, which constrains empirical verification of doctrinal propositions. Second, the analysis relies on statutory interpretation and secondary literature rather than extensive field data or stakeholder interviews. Finally, given that the PDPL is in a nascent stage of implementation, its interpretive guidance and enforcement practice are still developing; therefore, the findings should be read as a forward-looking theoretical and policy analysis rather than a fully empirical evaluation.

4 FINDINGS

4.1 Global regimes (GDPR and CCPA/CPRA): operationalising negligence

Standard of care & foreseeability. GDPR Article 32 and the CCPA's "reasonable security" provision serve as statutory proxies for negligence standards; DPIAs, breach notifications, and vendor oversight demonstrate proactive diligence.

Accountability to liability. GDPR's Art. 5(2), plus Arts. 82–83, and CCPA's private right of action shifts the system from compliance to enforceable culpability. Non-trivial governance failures (weak risk assessment, missing safeguards) increasingly satisfy breach and causation elements where harms are foreseeable (Acquah et al., 2024; Morrow & Fitzpatrick, 2020; Ke & Sudhir, 2022; Ou, 2025).

Practical upshot. Organisations must show continuous, risk-based governance; proactive controls (privacy-by-design, training, third-party risk management) operate both as compliance duties and defences in negligence claims.

4.2 Saudi Arabia's PDPL: doctrinal underdevelopment

Statutory silence and scope. PDPL adopts broad, GDPR-like definitions and an extraterritorial reach but omits explicit negligence language and lacks clear tiers for sensitive data, thereby weakening risk-based enforcement (Memish et al., 2021; Sarabdeen & Mohamed Ishak, 2025). Legal bases and consent. Heavy reliance on consent—without GDPR-style legitimate interest or contractual necessity—risks "consent fatigue" and blurs the evaluation of foreseeability and reasonableness (Voigt & Von dem Bussche, 2017; Kaminski & Malgieri, 2020)—particularly in cross-border transfers. Adequacy concepts exist, but the absence of SCCs/BCRs-like tools undermines the practical enforceability of security and breach notification across borders (Greenleaf, 2021). PDPL requires safeguards and notifications but lacks explicit timelines or severity thresholds—contrasting GDPR's 72-hour rule—leading to ambiguity that hampers deterrence. Data subject rights and remedies. Rights of access, correction, and erasure are provided, but there are no provisions for portability, objection to processing, or private right of action and compensation—marking a sharp contrast to GDPR Art. 82 and CCPA §1798.150. This diminishes bottom-up accountability (Alhazmi & Daghistani, 2024; Filler et al., 2022).

Controller/processor duties. PDPL establishes high-level responsibilities but lacks detailed processor-contract provisions, audit rights, and breach protocols, which limits enforceability (Abobaker, 2024b; Kanojia, 2023). Regulatory authority and sanctions. Oversight by SDAIA/NDMO lacks independence, procedural clarity, and jurisprudential output typical of EU DPAs or the California agency; penalty tiers and interpretive guidance are sparse, reducing predictability and deterrence (Amoo et al., 2024). Technology and sector gaps. PDPL does not include DPIA-like mechanisms for high-risk technology (AI, biometrics, ADM) and lacks sector-specific protocols for fintech/health/telecom; this creates liability grey zones as Saudi digitisation accelerates (Alqarni et al., 2023; Alzahrani, 2024; Yang et al., 2020). Cultural and legal integration. Islamic principles (amanah, la darar wa la dirar) are not yet codified into enforceable care standards (e.g., fiduciary duties, restorative remedies), missing an opportunity to develop a culturally coherent negligence doctrine and enhance public legitimacy.

4.3 Comparative negligence architecture across GDPR, CCPA/CPRA, and PDPL

To contextualise the discussion of negligence as a regulatory principle, Table 1 presents a comparative synthesis of the GDPR, CCPA/CPRA, and PDPL. The comparison highlights how Western legal systems have transformed negligence into a legally enforceable duty of compliance. In contrast, the PDPL remains largely administrative, offering valuable insights for normative and institutional reform within the Saudi context.

Table 1

Comparative negligence framework across GDPR, CCPA/CPRA, and PDPL

Dimension	GDPR (EU)	CCPA/CPRA (California)	PDPL (Saudi Arabia)
Standard of care/security duty	"Appropriate technical and organisational measures" (risk-based) under Art. 32; accountability under Art. 5(2). (Legislation.gov.uk)	Requires "reasonable security procedures and practices"; detailed in statute + regs; consumer-facing rights drive governance. (California DOJ)	Controllers must implement "organisational, administrative, and technical measures" (Art. 19 of PDPL). (SDAIA)
Breach notification	Notify supervisory authority within 72 hours (Art. 33); notify data subjects when high risk (Art. 34). (Legislation.gov.uk)	Breach notification governed by CA data-breach laws; CCPA ties security lapses to private action for certain data types. (California DOJ)	Implementing Regulations/official guidance: notify SDAIA within 72 hours; notify data subjects without undue delay (guidance/regs). (DLA Piper)
Private right of action	Yes—Art. 82 grants right to compensation for material & non-material damage. (EUR-Lex)	Yes—Cal. Civ. Code §1798.150 allows statutory damages ($100–$750 per consumer per incident) or actual damages after certain breaches. (Justia Law)	No general private right of action; enforcement is administrative. (SDAIA)
Administrative fines / penalties	Tiered fines up to €20M or 4% global turnover (Art. 83). (EUR-Lex)	Civil penalties by AG/CPPA; private statutory damages per §1798.150. (California DOJ)	Sanctions provided in PDPL/Implementing Regs; details primarily administrative (no statutory damages to individuals). (SDAIA)
Extraterritorial scope	Applies to offering goods/services to, or monitoring behavior of, people in the EU (Art. 3). (EUR-Lex)	Applies to businesses meeting CA nexus/thresholds handling CA residents' data. (California DOJ)	Applies to processing of personal data of individuals in KSA, including extraterritorial processing (Art. 2 PDPL). (SDAIA)
Supervisory authority / independence	Independent DPAs + EDPB coordination (Arts. 51–63). (EUR-Lex)	California Privacy Protection Agency (CPPA) + CA Attorney General. (California DOJ)	SDAIA/NDMO administer; independence and detailed powers outlined via

			law/regs & guidance. (SDAIA)
Sensitive data	Special protection for special categories (Art. 9). (Legislation.gov.uk)	"Sensitive personal information" defined; added duties/limits (CPRA). (California DOJ)	PDPL defines personal data broadly; sensitive category treatment addressed by regs/guidance (less granular than GDPR/CPRA). (SDAIA)
DPIA / risk assessment	DPIA required for high-risk processing (Art. 35). (Legislation.gov.uk)	Risk-assessment/PIA-style obligations via CPRA regs and sectoral guidance. (California DOJ)	Implementing Regulation and SDAIA guides set breach-response and governance expectations; no GDPR-style DPIA mandate articulated as such. (SDAIA)
Processor obligations & contracts	Detailed controller/processor duties & contracts (Arts. 28–30). (Legislation.gov.uk)	Service-provider/contractor restrictions and contractual requirements. (California DOJ)	Controller obligations specified; processor obligations emerging via Implementing Regulation templates/guidance. (SDAIA)
Cross-border transfers	Adequacy, SCCs, BCRs (Arts. 45–49). (Legislation.gov.uk)	No direct transfer regime; disclosures and contractual governance dominate. (California DOJ)	Adequacy-style approach; SDAIA has issued evolving transfer guidance/SCCs. (Clyde & Co)
Negligence hooks (foreseeability → accountability)	Accountability (Art. 5(2)) + security (Art. 32) + compensation (Art. 82) operationalize negligence-like standards. (GDPR)	"Reasonable security" + §1798.150 private action make failure to prevent foreseeable breaches legally actionable. (FindLaw Codes)	Duty to protect data and notify; no private claims—liability runs through regulator, with growing guidance (72-hour rule). (DLA Piper)

Note: This table summarises the principal legal dimensions of negligence-relevant provisions within three major data protection frameworks:
– GDPR (European Union): General Data Protection Regulation (EU) 2016/679 (Legislation.gov.uk, EUR-Lex)
– CCPA/CPRA (California): California Consumer Privacy Act and California Privacy Rights Act (California Department of Justice, California Civil Code §1798.150)
– PDPL (Saudi Arabia): Personal Data Protection Law (Royal Decree M/19 of 2021) and Implementing Regulations (Saudi Data and Artificial Intelligence Authority (SDAIA), Implementing Regulations PDF).
Supplementary interpretive sources include DLA Piper (2024), Clyde & Co (2024), and FindLaw (2024). All URLs were accessed in October 2025.

5 RECOMMENDATIONS

This paper advocates for several specific legislative and regulatory amendments to enhance Saudi Arabia's PDPL, based on doctrinal and comparative analysis. There is an immediate need to explicitly incorporate a negligence standard into the PDPL, either through legislative amendment or interpretive regulatory guidance, to clarify the duty of care required of data controllers and processors. This must include clearly expressed procedural and administrative measures, along with routine risk assessments and sector-specific rules of business based on best practices, as described under Articles 28 to 30 of

the GDPR. Second, the legislation must establish a private right of action as a remedy for data breaches, allowing individuals to pursue compensation for material and non-material damages, as outlined in GDPR under Article 82 and the statutory damage requirements under the CCPA. Third, the scope of application can be strengthened by establishing an independent supervisory or regulatory authority endowed with extensive fact-finding and sanctioning powers to ensure adequate supervision and accountability following incidents of negligence or data breaches. Fourth, to promote consistency in application, the PDPL can be improved by incorporating supervisory or regulatory advice, DPIA, and standard contractual clauses (SCCs), addressing the current lack of compliance tools. Saudi Arabia's data protection regime must incorporate culturally significant legal principles of trust (Amanah) and non-harm (la darar wa la dirar), to create a normative framework aligned with global standards while respecting local legal principles. These suggestions aim to transform the PDPL regime into a robust, enforceable instrument that guarantees "care" within a data-driven society.

6 CONCLUSION

The development of "negligence" in data protection legislation across Europe, the United States, and Saudi Arabia reveals evolving gaps in legal maturity and enforcement mechanisms. The GDPR and CCPA provide solid frameworks based on compliance standards, safety measures, and individual remedies; however, the PDPL in Saudi Arabia remains in its early stages in terms of normative and operational features. The lack of an explicitly defined "standard of care," the absence of breach reporting requirements, and the inability to establish a framework for individual compensation highlight doctrinal and practical gaps that hinder the prevention of data breaches within Saudi Arabia's digital governance. Moreover, the concept of negligence in the PDPL is notably absent, either as a regulatory principle or as an actionable provision, which diminishes its capacity to address complex emerging risks such as biometric surveillance and algorithmic threats. These deficiencies are further compounded by the lack of interpretive guidance from supervisory and regulatory bodies such as NDMO and SDAIA, as well as the absence of an autonomous entity with jurisdictional authority to enforce data rights. Significantly, Saudi Arabia upholds normative principles rooted in Islamic law, such as amanah (trust) and la darar wa la dirar (no harm), which can be invoked to establish a traditionally unified

and legally binding “standard of care” in data management. Embedding these cultural principles of “trust” and “non-harm” has the potential to strengthen the PDPL by promoting “accountability” in data handling, sector-specific protections, and individual rights of action. Such integration could support Saudi Arabia’s Vision 2030 in fostering a robust and ethically grounded digital ecosystem.

FUNDING

This research received no external funding.

REFERENCES

1. Abobaker, M. Y. (2024a). Analysis of Saudi Arabia's Legislative Reforms to Strengthen Compliance with The Convention on the Rights of the Child and SDGS: Enhancing Online Protection for Future Generations. Journal of Lifestyle and SDGs Review, 4(3), e02374-e02374.
2. Abobaker, M. Y. (2024b). Analysis of Saudi Arabia's Legislative Reforms to Strengthen Compliance with The Convention on the Rights of the Child and SDGS: Enhancing Online Protection for Future Generations. Journal of Lifestyle and SDGs Review. https://doi.org/10.47172/2965-730x.sdgsreview.v4.n03.pe02374
3. Acquah, E., Ganapati, S., & Choi, Y.-J. (2024). Examining the effects of California Consumer Privacy Act (CCPA) on Organizational Data Breach Notification. Proceedings of the 25th Annual International Conference on Digital Government Research. https://doi.org/10.1145/3657054.3657082
4. Alhazmi, A., & Daghistani, A. (2024). Privacy practices of popular websites in Saudi Arabia. Journal of Umm Al-Qura University for Engineering and Architecture. https://doi.org/10.1007/s43995-024-00085-x
5. Alhejaili, M. O. M. (2024). SECURING THE KINGDOM'S E-COMMERCE FRONTIER: EVALUATION OF SAUDI ARABIA'S CYBERSECURITY LEGAL FRAMEWORKS. Journal of Governance and Regulation/Volume. virtusinterpress. org.
6. Alkhamsi, N. N., & Alqahtani, S. S. (2024). Compliance Framework for Personal Data Protection Law Standards. International Journal of Advanced Computer Science & Applications, 15(7).
7. Alqarni, A., Timko, D., & Rahman, M. (2023). Saudi Arabian Perspective of Security, Privacy, and Attitude of Using Facial Recognition Technology. 2023 20th Annual International Conference on Privacy, Security and Trust (PST), 1-12. https://doi.org/10.1109/PST58708.2023.10320185

8. Alshehadeh, A. R., Elrefae, G. A., Khudari, M., & Injadat, E. (2022). *Impacts of financial technology on profitability: Empirical evidence from Jordanian commercial banks.* In S. G. Yaseen (Ed.), *Digital economy, business analytics, and big data analytics applications* (Studies in Computational Intelligence, Vol. 1010, pp. 487–496). Springer. https://doi.org/10.1007/978-3-031-05258-3_38

9. Alzahrani, R. B. (2024). An overview of AI data protection in the context of Saudi Arabia. International Journal for Scientific Research, 3(3), 199-218.

10. Balkin, J. (2016). Information Fiduciaries and the First Amendment. https://consensus.app/papers/information-fiduciaries-and-the-first-amendment-balkin/d6f3c69d99bf5f72882273346bfc9b38/

11. Balkin, J. M. (2020). The fiduciary model of privacy. Harv. L. Rev. F., 134, 11.

12. Bankins, S., Ocampo, A., Marrone, M., Restubog, S., & Woo, S. (2023). A multilevel review of artificial intelligence in organizations: Implications for organizational behavior research and practice. Journal of Organizational Behavior. https://doi.org/10.1002/job.2735

13. Bunyamin, B. (2021). The Effectiveness of Legal Protection for the Victims of Violence Due to the Criminal of Mishandling. Al-Ishlah: Jurnal Ilmiah Hukum. https://doi.org/10.33096/AIJIH.V24I2.279

14. Chandler, J. (2007). Negligence Liability for Breaches of Data Security. https://consensus.app/papers/negligence-liability-for-breaches-of-data-security-chandler/3d8d5eef1fbb5da69c4920854f209392/

15. Claudia, Z., & Gunadi, A. (2023). Vicarious Liability in Personal Data Protection. Rechtsidee. https://doi.org/10.21070/jihr.v12i2.995

16. Comandè, G., & Schneider, G. (2021). Can the GDPR make data flow for research easier? Yes it can, by differentiating! A careful reading of the GDPR shows how EU data protection law leaves open some significant flexibilities for data protection-sound research activities. Computer Law & Security Review, 41, 105539.

17. Dąbrowska, J., Almpanopoulou, A., Brem, A., Chesbrough, H., Cucino, V., Di Minin, A., Giones, F., Hakala, H., Marullo, C., & Mention, A. L. (2022). Digital transformation, for better or worse: a critical multi-level research agenda. R&D Management, 52(5), 930-954.

18. Dorton, S., Ministero, L., Alaybek, B., & Bryant, D. (2023). Foresight for ethical AI. Frontiers in Artificial Intelligence, 6. https://doi.org/10.3389/frai.2023.1143907

19. Filler, D. M., Haendler, D. M., & Fischer, J. L. (2022). Negligence at the Breach: Information Fiduciaries and the Duty to Care for Data. Conn. L. Rev., 54, 105.

20. Giliker, P. (2010). Vicarious liability in tort: A comparative perspective (Vol. 69). Cambridge University Press.

21. Greenleaf, G. (2021). Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance.

22. Hamdani, R. E., Mustapha, M., Amariles, D. R., Troussel, A., Meeùs, S., & Krasnashchok, K. (2021). A combined rule-based and machine learning approach for automated GDPR compliance checking. Proceedings of the Eighteenth International Conference on Artificial Intelligence and Law. https://doi.org/10.1145/3462757.3466081

23. Hamon, R., Junklewitz, H., Sanchez, I., Malgieri, G., & De Hert, P. (2022). Bridging the Gap Between AI and Explainability in the GDPR: Towards Trustworthiness-by-Design in Automated Decision-Making. IEEE Computational Intelligence Magazine, 17, 72-85. https://doi.org/10.1109/MCI.2021.3129960

24. Herijanto, H. (2022). Al amanah in al qur'an vs trust: a comparative study. International Journal of Ethics and Systems. https://doi.org/10.1108/ijoes-03-2021-0064

25. Hylton, K. N. (2014). Information and Causation in Tort Law: Generalizing the Learned Hand Test for Causation Cases. Journal of Tort Law, 7(1-2), 35-64.

26. Ikram, N. A. H. S. (2024). Data breaches exit strategy: A comparative analysis of data privacy laws. Malaysian Journal of Syariah and Law, 12(1), 135-147.

27. Ishwara Bhat, P. (2020). Idea and methods of legal research.

28. Islam, M. T. (2018). Abu Bakar Munir, Siti Hajar Mohd Yasin and Ershadul Karim, Data Protection Law in Asia (Vol. 8). Oxford University Press.

29. Islam, M. T. (2022). An Assessment of Privacy Regime in Bangladesh: A Legal Analysis. UUM Journal of Legal Studies, 13(2), 77-108.

30. Juma'h, A., & Alnsour, Y. (2020). The effect of data breaches on company performance. International Journal of Accounting and Information Management, 28, 275-301. https://doi.org/10.1108/ijaim-01-2019-0006

31. Jun, J., & Kim, J.-Y. (2024). Strict liability versus negligence in the case of data breach. International Review of Law and Economics. https://doi.org/10.1016/j.irle.2024.106218

32. Kaminski, M., & Malgieri, G. (2020). Multi-layered explanations from algorithmic impact assessments in the GDPR. Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency. https://doi.org/10.1145/3351095.3372875

33. Kanojia, S. (2023). Ensuring privacy of personal data: a panoramic view of legal developments in personal data protection law in Saudi Arabia. J. Int'l L. Islamic L., 19, 270.

34. Ke, T., & Sudhir, K. (2022). Privacy Rights and Data Security: GDPR and Personal Data Markets. Manag. Sci., 69, 4389-4412. https://doi.org/10.1287/mnsc.2022.4614

35. Ke, T. T., & Sudhir, K. (2023). Privacy rights and data security: GDPR and personal data markets. Management Science, 69(8), 4389-4412.

36. Kesan, J., & Hayes, C. (2018). Liability for Data Injuries. University of Illinois Law Review, 2019, 295-363. https://consensus.app/papers/liability-for-data-injuries-kesan-hayes/f3443085d15b502fa026a6e31aae5c25/

37. Khan, S., Kabanov, I., Hua, Y., & Madnick, S. (2022). A Systematic Analysis of the Capital One Data Breach: Critical Lessons Learned. ACM Transactions on Privacy and Security, 26, 1-29. https://doi.org/10.1145/3546068

38. Krishnamurthy, V. (2020). A tale of two privacy laws: The GDPR and the international right to privacy.

39. Labadie, C., & Legner, C. (2022). Building data management capabilities to address data protection regulations: Learnings from EU-GDPR. Journal of Information Technology, 38, 16-44. https://doi.org/10.1177/02683962221141456

40. Lim, S., & Oh, J. (2025). Navigating Privacy: A Global Comparative Analysis of Data Protection Laws. IET Information Security, 2025(1), 5536763.

41. Masur, P. K. (2020). How online privacy literacy supports self-data protection and self-determination in the age of information. Media and Communication, 8(2), 258-269.

42. Memish, Z. A., Altuwaijri, M. M., Almoeen, A. H., & Enani, S. M. (2021). The Saudi Data & Artificial Intelligence Authority (SDAIA) vision: leading the kingdom's journey toward global leadership. Journal of epidemiology and global health, 11(2), 140-142.

43. Mirshekari, A., Ghasemi, R., & Fattahi, A. (2020). Digital accounts after death: a case study in Iran law. UUM Journal of Legal Studies, 11(2), 153-182.

44. Morrow, P., & Fitzpatrick, T. (2020). U.S. and International Legal Perspectives Affecting Cybersecurity Corporate Governance. International Relations and Diplomacy. https://doi.org/10.17265/2328-2134/2020.06.001

45. Nusairat, W. M. (2024). Legal Protection of Personal Data Privacy in the Kingdom of Saudi Arabia. Manchester Journal of Transnational Islamic Law & Practice, 20(1).

46. Ou, L. (2025). Regulatory Responses to Data Breaches: Evaluating the Effectiveness of GDPR and CCPA in Consumer Protection. International Journal of Social Sciences and Public Administration. https://doi.org/10.62051/ijsspa.v6n1.22

47. Pemuli, R., & Barkatullah, A. H. (2024). Liability Of Business Actors For Breaches In Electronic Banking Systems. JURNAL HUKUM SEHASEN. https://doi.org/10.37676/jhs.v10i2.6839

48. Pernot-Leplay, E. (2020). EU Influence on Data Privacy Laws: Is the U.S. Approach Converging with the EU Model? , 18, 25-48. https://consensus.app/papers/eu-influence-on-data-privacy-laws-is-the-us-approach-pernot-leplay/6e036795f7885084933af53832d6ca61/

49. Pimenta Rodrigues, G. A., Marques Serrano, A. L., Lopes Espiñeira Lemos, A. N., Canedo, E. D., Mendonça, F. L. L. d., de Oliveira Albuquerque, R., Sandoval Orozco, A. L., & García Villalba, L. J. (2024). Understanding data breach from a global perspective: Incident visualization and data protection law review. Data, 9(2), 27.

50. Posner, R. A. (2004). Frontiers of legal theory. Harvard University Press.

51. Quinn, P., & Malgieri, G. (2021). The difficulty of defining sensitive data—the concept of sensitive data in the EU data protection framework. German Law Journal, 22(8), 1583-1612.

52. Regulation, P. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council. Regulation (eu), 679, 2016.

53. Rogers, W. V. H. (2010). Winfield and Jolowicz on tort (Vol. 515). Sweet & Maxwell London.

54. Sarabdeen, J., & Mohamed Ishak, M. M. (2025). A comparative analysis: health data protection laws in Malaysia, Saudi Arabia and EU General Data Protection Regulation (GDPR). International Journal of Law and Management, 67(1), 99-119.

55. Schlackl, F., Link, N., & Hoehle, H. (2022). Antecedents and consequences of data breaches: A systematic review. Inf. Manag., 59, 103638. https://doi.org/10.1016/j.im.2022.103638

56. Setyawan, F. R., Fajrin, Y. A., Prasetyo, S. N., Nuryasinta, R. K., Alam, S., Kurniawan, K., & Kurniawan, W. (2024). Preventive Legal Protection Against Leaks Consumer Data by Company Negligence Financial Technology. KnE Social Sciences. https://doi.org/10.18502/kss.v8i21.14745

57. Sinaga, H. (2023). Legal and Ethical Implications in Data Theft Cases in the Digital Era. East Asian Journal of Multidisciplinary Research. https://doi.org/10.55927/eajmr.v2i11.6791

58. Solove, D. J., & Hartzog, W. (2014). The FTC and the new common law of privacy. Colum. L. Rev., 114, 583.

59. Stallings, W. (2020). Handling of Personal Information and Deidentified, Aggregated, and Pseudonymized Information Under the California Consumer Privacy Act. IEEE Security & Privacy, 18, 61-64. https://doi.org/10.1109/MSEC.2019.2953324

60. Teichmann, F. M. J., & Wittmann, C. (2023). When is a law firm liable for a data breach? An exploration into the legal liability of ransomware and cybersecurity. Journal of Financial Crime, 30(6), 1491-1498.

61. Tene, O., & Polonetsky, J. (2013). A theory of creepy: technology, privacy and shifting social norms. Yale JL & Tech., 16, 59.

62. Terry, N. P. (2012). Protecting patient privacy in the age of big data. UMKC L. Rev., 81, 385.

63. Thomas, L., Gondal, I., Oseni, T., & Firmin, S. S. (2022). A framework for data privacy and security accountability in data breach communications. Computers & Security, 116, 102657.

64. Tschider, C. (2024). Unto the (Data) Breach. University of Richmond Law Review, Forthcoming.

65. Vaka, P. R. (2020). Data Breaches or Regulatory and Compliance. International Journal Of Multidisciplinary Research In Science, Engineering and Technology. https://doi.org/10.15680/ijmrset.2020.0312020

66. Voigt, P., & Von dem Bussche, A. (2017). The eu general data protection regulation (gdpr). A practical guide, 1st ed., Cham: Springer International Publishing, 10(3152676), 10-5555.

67. Voss, G. (2021). The CCPA and the GDPR Are Not the Same: Why You Should Understand Both. AARN: Law of Technology. https://consensus.app/papers/the-ccpa-and-the-gdpr-are-not-the-same-why-you-should-voss/8637bd3228d6595a9b45f0891d8c3ea0/

68. Weitzman, R. (2023). Forensic Statistics: Taking the Mishandling and Misuse of Statistics to Court. Journal of Forensic Sciences & Criminal Investigation. https://doi.org/10.19080/jfsci.2023.17.555955

69. Williams, S. (2020). CCPA tipping the scales: Balancing individual privacy with corporate innovation for a comprehensive federal data protection law. Ind. L. Rev., 53, 217.

70. Wong, R., Chong, A., & Aspegren, R. (2023). Privacy Legislation as Business Risks: How GDPR and CCPA are Represented in Technology Companies' Investment Risk Disclosures. Proceedings of the ACM on Human-Computer Interaction, 7, 1-26. https://doi.org/10.1145/3579515

71. Yang, P., Xiong, N., & Ren, J. (2020). Data security and privacy protection for cloud storage: A survey. Ieee Access, 8, 131723-131740.

72. Young, K., & Billings, K. (2020). Legal Consciousness and Cultural Capital. Law & Society Review. https://doi.org/10.1111/lasr.12455

73. Zhao, H., Jiang, N., Cai, Z., Lim, E. T., & Tan, C.-W. (2023). Toward a taxonomy of corporate data protection malpractices and their causal mechanisms: A regulatory view. Journal of Information Technology, 38(3), 319-333.

Authors' Contribution

Both authors contributed equally to the development of this article.

Data availability

All datasets relevant to this study's findings are fully available within the article.

How to cite this article (APA):

Alnasser, H. A. (2025). THE CONCEPT OF NEGLIGENCE IN DATA BREACH: A COMPARATIVE DOCTRINAL ANALYSIS OF THE EU, CALIFORNIA, AND SAUDI ARABIA. *Veredas Do Direito*, 22(3), e223404. https://doi.org/10.18623/rvd.v22.n3.3404