QUBAHAN ACADEMIC JOURNAL
VOL. 6, NO. 2, May 2026
https://doi.org/10.48161/qaj.v6n2a2514

Toward a Risk-Calibrated Civil Liability Framework for Personal Data Breaches: A Comparative Study of Saudi, Jordanian, and EU Law

Emad Ahmad Abousud [1*] **and Mustafa Ibrahim Araibi** [1]

[1] Department of Business Administration, College of Business Administration, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh 13318, Saudi Arabia.

* **Corresponding author:** easaued@imamu.edu.sa

ABSTRACT: This study provides a theory-driven comparative analysis of civil liability for personal data breaches across three comparative legal frameworks: Saudi law, Jordanian law, and the European Union's data protection regime, with particular emphasis on the interaction between civil liability rules and personal data protection regulation, and the European Union General Data Protection Regulation (GDPR). It examines how these frameworks address key liability challenges arising from digital harms, including burden of proof, attribution of responsibility, non-material damages, and multi-party processing environments. Methodologically, the study adopts a functional comparative approach, complemented by a post-functional critical perspective that assesses the transferability of legal doctrines across jurisdictions. It develops a five-indicator analytical matrix to operationalize adequacy and effectiveness in civil liability systems, focusing on burden distribution, damage recognition, attribution mechanisms, preventive capacity, and judicial accessibility. Drawing on recent jurisprudence of the Court of Justice of the European Union (notably C-300/21 and C-340/21), the study identifies structural limitations in both Saudi and Jordanian regimes, particularly their continued reliance on traditional fault-based liability and limited doctrinal clarity regarding intangible harm and causation in complex digital environments. Building on these findings, the paper proposes a Risk-Calibrated Accountability Model (RCAM), which integrates a calibrated fault standard based on objective security benchmarks, a conditional presumption of liability, a structured approach to non-material damages, and layered joint attribution for distributed data processing. The model is theoretically grounded in accountability theory and moderate strict-liability principles, while remaining aligned with the institutional and doctrinal structures of Saudi and Jordanian law. The study concludes with targeted legislative and regulatory recommendations to enhance the effectiveness and coherence of civil liability for data breaches in both jurisdictions.

Keywords: Civil liability, Data breaches, General Data Protection Regulation (GDPR), Comparative data protection law, Risk-calibrated accountability model.

I. INTRODUCTION

The rapid expansion of digital technologies and data-driven economies has reshaped the nature of legal relationships, particularly those concerning personal data. As organizations rely on the large-scale collection, processing, and storage of personal information, data breaches have grown more frequent and their consequences more severe [1, 2]. High-profile incidents involving unauthorized access, data leaks, and

sophisticated cyberattacks have exposed significant gaps in existing legal frameworks to address the effects of such breaches, leading to the emergence of a new type of harm that is often intangible, diffuse, and has pervasive characteristics incompatible with the traditional concept of damages [3, 4]. Legal systems worldwide have responded to this shift to varying degrees. The European Union, through its General Data Protection Regulation (GDPR), has established the most sophisticated regulatory framework to date, explicitly recognizing the right to compensation for both material and moral damages, and through a growing body of case law from the Court of Justice of the European Union [5, 6] is gradually improving the conditions under which such compensation can be claimed. In parallel, the legal systems under study entered a distinct phase of legislative modernization. Saudi Arabia enacted the Personal Data Protection Law in 2021, which was amended in 2023 [7, 8], and subsequently issued its first-ever Civil Transactions Law (Royal Decree No. M/191 of 2023), which entered into force on December 16, 2023, and which codifies the general rules of contractual and tortious liability in 721 articles [9]. Jordan, for its part, enacted the Personal Data Protection Law No. 24 of 2023, which entered into force on March 17, 2024 [10], thus abandoning its previous reliance solely on the principles of general tortious liability.

This legal update between 2021 and 2024 represents a significant analytical moment. Both Saudi Arabia and Jordan possess dedicated legal instruments capable, at least in principle, of regulating civil liability for data breaches. However, these instruments were enacted without a full explanation of how they interact with one another or how general legal principles accommodate the specific challenges of digital harm. The result is a regulatory framework that remains, in important respects, incomplete. It is not fully adapted to the requirements and conditions of litigation in data breach cases, nor is it entirely free from the classical fault-based tradition.

In this context, this study conducts a comparative legal analysis of civil liability for data breaches under Saudi, Jordanian, and European law. Beyond its doctrinal dimension, the question of civil liability for personal data breaches carries substantial ethical weight. Liability rules are not normatively neutral instruments: they distribute the costs of digital innovation between data subjects who are typically the structurally weaker party in the informational relationship and data controllers, who derive economic value from large-scale processing. A liability framework that under-protects the former effectively externalizes the social costs of digital activity onto individuals, raising concerns about distributive justice that have been increasingly emphasized in recent interdisciplinary scholarship at the intersection of law, ethics, and information policy. This study takes that ethical dimension as one of the normative orientations of its proposed model (see Sections III and VII), without losing sight of the doctrinal coherence that any reform must preserve within the codified frameworks of Saudi Arabia and Jordan.

1. RESEARCH PROBLEM AND STUDY QUESTION

Although specific laws for the protection of personal data have been enacted in Saudi Arabia and Jordan to modernize personal data protection, and general rules of civil liability exist, the ability of these legal frameworks to provide effective and proportionate redress for victims of data breaches remains uncertain. The new laws address data protection and civil liability separately, without establishing a comprehensive and coherent system for data breach cases. This creates a structural imbalance between the stated protection of personal data as a legal interest and the practical availability of compensation mechanisms for those harmed by its violation.

This complexity is further exacerbated by three structural features of the digital environment: the technical opacity of cybersecurity systems, which weakens the victim's ability to prove fault [11]; the distributed nature of data processing, which complicates the assignment of responsibility among multiple actors [12]; and the intangible nature of a significant portion of the resulting harm, which challenges traditional concepts of compensation for damages [4]. Therefore, the question arises as to the adequacy of existing legal frameworks, Saudi, Jordanian, and European, in addressing these structural challenges, and what lessons can be learned from a comparative assessment. To address this issue systematically, this study will answer the following research questions:

- To what extent do the Saudi Civil Transactions Law of 2023 and the Jordanian Civil Code, in conjunction with relevant data protection laws, provide a sufficient legal basis for compensating victims of personal data breaches?
- How do the three legal systems, Saudi, Jordanian, and European, distribute the burden of proof in data breach claims, and what are the implications of this for related lawsuits?
- To what extent do these legal systems recognize non-material damages resulting from privacy breaches, and how do they determine compensation for such damages?
- How do these legal systems address issues of multilateral liability in distributed digital systems, and do they provide effective mechanisms for victims of breaches to obtain full compensation?
- What are the elements of the European model that can be utilized in Saudi and Jordanian law while maintaining general legal principles, and what are the specific reforms that would enhance the effectiveness of civil liability in both laws?

2. THE IMPORTANCE AND OBJECTIVES OF THE RESERCH

This study is important for three reasons. First, its subject matter addresses a pressing contemporary challenge: the protection of personal data in an era where violations are frequent and have serious consequences, directly impacting individuals' autonomy, financial security, and human dignity [3], [13]. Second, the existence of modern data protection laws, alongside the entry into force of the Saudi Civil Transactions Law (Royal Decree No. M/191 of 2023) on December 16, 2023 [9], presents a challenge in examining the capacity of these laws to regulate civil liability for data violations. Third, the comparative dimension of the study based on the well-established European framework under the General Data Protection Regulation [1, 14] fills a significant gap in Arab legal studies, which have not yet given sufficient systematic attention to the aspects of civil liability in data protection, compared to its criminal or regulatory dimensions.

Given this importance, and in response to the research questions stated above, this study pursues the following objectives:

- To examine the adequacy of traditional civil liability rules as codified in the Saudi Civil Transactions Law of 2023 and the Jordanian Civil Code in addressing damages resulting from personal data breaches.
- To analyze the contribution of the Saudi Personal Data Protection Law and the Jordanian Personal Data Protection Law No. 24 of 2023 to the civil liability system, identifying their strengths and areas requiring reconsideration.
- To compare these national rules with the European model under the GDPR, with particular attention to the evolving jurisprudence of the Court of Justice of the European Union.
- To identify the main theoretical and practical challenges that hinder the effective application of civil liability in the three fundamental areas: fault, non-material tort, and causation.
- Proposing an advanced model of civil liability that combines traditional legal principles with the requirements of the digital age, in a manner appropriate to the institutional contexts in Saudi Arabia and Jordan.

3. RESEARCH METHODOLOGY AND DESIGN

This study adopts a comparative-analytical methodology. This approach was selected because the research questions require both a systematic interpretation of legal texts and a critical comparison of how different legal systems address similar issues. The analytical dimension involves a careful and precise interpretation of primary legal sources, such as laws, regulations, and judicial rulings, while the comparative dimension enables the identification of similarities, differences, and applicable elements among the various legal systems [15, 16].

The selection of the three legal systems, Saudi Arabia, Jordan, and the European Union, stems from the fact that Saudi Arabia and Jordan share a civil legal tradition rooted in fault-based liability and have recently undergone parallel legislative modernization, making them particularly suitable for bilateral comparison. The European Union, through its GDPR and the accumulated case law of the Court of Justice of the European

Union [5, 6], offers the most mature regulatory framework in this field globally, making it a benchmark against which other legal systems can be evaluated.

The study consists of four parts. First, it establishes the conceptual framework for data violations, clarifying the legal nature of personal data and the categories of damages that warrant compensation (Section IV). Second, it identifies the general legal basis for civil liability and the challenges it faces in the digital context (Section V). Third, it conducts a detailed comparative analysis of Saudi and Jordanian law in light of the General Data Protection Regulation, supported by a comprehensive comparison table (Section VI). Fourth, it develops a proposal for a flexible liability model and draws specific implications that could lead to corrective legal amendments (Section VII).

The primary sources consulted include: the Saudi Civil Transactions Law (Royal Decree No. M/191 of 2023); the Saudi Personal Data Protection Law (2021, as amended in 2023); the Jordanian Civil Code; and the Jordanian Personal Data Protection Law No. 24 of 2023. Regulation (EU) 2016/679 (General Data Protection Regulation); relevant rulings of the Court of Justice of the European Union; and decisions of the Jordanian Court of Cassation. Other sources include peer-reviewed scholarly articles, legal studies, and institutional reports published between 2017 and 2026, selected for their direct relevance to the civil liability dimension of data protection.

The study acknowledges several difficulties and challenges. First, the scarcity of published case law applications, due to the relative newness of Saudi and Jordanian data protection laws, limits the empirical evaluation of their practical effectiveness. Second, the study focuses on civil liability and does not address criminal and administrative liability for data protection. Third, the comparative scope is limited to three systems to achieve analytical depth, while a broader regional comparison is reserved for future research.

II. RELATED WORKS AND PREVIOUS STUDIES

The literature on data protection and civil liability has expanded considerably in recent years. This section reviews the most relevant previous research, identifies the gap addressed by the present study, and clarifies its contribution to the field. Therefore, the previous studies have been organized into four thematic groups, followed by a statement of the research's contribution.

1. THEORETICAL ASPECTS OF DATA BREACH TORTS

Solove and Citron laid the theoretical groundwork for civil liability for data breaches in their seminal work on risk and anxiety as compensable torts [3]. Their argument that data breaches give rise to distinct torts that traditional tort categories cannot fully encompass influenced subsequent studies. Citron and Solove later developed this framework through a systematic classification of privacy torts [17], while Schwartz and Solove addressed the difficulties in defining the concepts posed by personal information itself [18]. Further work by Filler, Handler, and Fisher developed the concept of information custodians to establish a duty of care in data-processing relationships [11]. At the same time, Tschider examined organizational negligence in cases of data management failures [12]. While these fundamental contributions are indispensable, their focus is primarily theoretical and centered on U.S. legal norms.

2. THE EUROPEAN MODEL AND THE JUDGMENTS OF COURT OF JUSTICE OF THE EUROPEAN UNION

Several studies address the European framework for civil liability under Article 82 of the GDPR. The seminal commentaries by Kuner, Bygrave, and Docksey [1] and by Voigt and von dem Busch [14] provide a systematic analysis of the compensation regime under the Regulation. More focused jurisprudential studies have followed the rapid development of European Court of Justice jurisprudence: Lee analyzed the key issue decided in case C-300/21 [19]. At the same time, Walree addressed the relationship between the right to an effective remedy and the concept of tort under Article 82 [20]. Knetsch examined compensation for non-financial losses in GDPR infringement cases [4], and Zanfir-Fortuna offered a comprehensive commentary on the liability clause itself [21]. These works provide in-depth analyses of the European model, but naturally focus on the European legal trend and do not address Jordanian and Saudi law.

3. ACADEMIC STUDIES ON SAUDI PERSONAL DATA PROTECTION LAW

Several studies have examined Saudi personal data protection law. Al-Shamrani presented a systematic analysis of data protection challenges in the Kingdom [2], and in another study, Al-Hujaili presented the structural limitations of the personal data protection framework [22]. Sarabdeen and Muhammad Ishaq conducted a three-way comparison of health data protection in Malaysia, Saudi Arabia, and the European Union [7]. At the same time, Al-Nasser contributed two complementary theoretical studies: one focused on the standards of negligence under the personal data protection framework [8], and the other compared the principles of negligence in the European Union, California, and Saudi Arabia [23]. More recently, Brown and Al-Othman published a critical analysis of the use of personal data under Saudi insurance law, comparing the safeguards of the personal data protection framework with the standards of the GDPR through a comparative theoretical methodology [16]. Overall, these studies significantly enhance understanding of the Saudi personal data protection framework. However, none of them systematically incorporates the Saudi Civil Transactions Law of 2023 into their analysis of civil liability for data breaches, despite its fundamental importance as it contains the general rules of tort liability.

4. STUDIES IN CIVIL LIABILITY AND CYBERSECURITY IN JORDAN

Numerous studies have examined cybersecurity and civil liability in Jordan. Al-Tamimi analyzed civil liability for technical damages under Jordanian law and the prospects for its reform [24], while Jabbour addressed the protection of personal data in the Arab context [25]. Bani Migdad examined publishers' liability on social media platforms under Jordanian legislation [26], and Maaytah and Kobarie analyzed the impact of cybersecurity regulations on electronic civil transactions [27]. More recently, Al-Rawashdeh addressed the law applicable to civil liability for cyberattacks [28], and Khawaldeh, in 2026, presented an analysis of civil liability in cases of information leaks, reviewing emerging judicial principles [29]. These studies, in general, focus on legal principles in Jordanian law without comparison to Saudi law, and they do not specifically address Jordanian personal data protection law.

5. RESEARCH GAPS AND THE CONTRIBUTION OF THIS STUDY

The literature of this study, taken together, reveals three structural limitations that limit its contribution: First, no previous study has systematically integrated the three recently enacted legal systems the Saudi Civil Transactions Law of 2023, the Saudi Personal Data Protection Law, and the Jordanian Personal Data Protection Law No. 24 of 2023 into a unified comparative analysis of civil liability for data breaches. Existing Saudi studies address the Personal Data Protection Law in isolation from the Civil Transactions Law. In contrast, Jordanian studies generally date back to before the enactment of the 2023 Personal Data Protection Law. Second, although many studies offer binary comparisons (Saudi-European analyses or local Jordanian analyses), no published work systematically compares Saudi law, Jordanian law, and the European framework, taking into account the recent jurisprudence of the Court of Justice of the European Union [5, 6]. Third, the dimension related to proposing practical solutions still needs further study: few studies propose concrete models grounded in clear legal foundations that can be taken into account when developing related legal systems.

This study addresses three gaps, offering: (a) a comprehensive analysis of the Saudi Civil Transactions Law of 2023 and the Personal Data Protection Law, along with the Jordanian Personal Data Protection Law of 2023, focusing on specific articles rather than general principles; (b) a structured three-part comparison with the General Data Protection Regulation (GDPR) and its legal developments, summarized in a dedicated comparison table; and (c) a developed model of civil liability that translates comparative insights into targeted reform proposals. The methodological scaffolding through which these contributions are operationalized is set out in the next section.

III. RESEARCH METHODOLOGY AND ANALYTICAL FRAMEWORK

1. METHODOLOGICAL POSTURE: FUNCTIONAL COMPARATIVE LAW WITH A POST-FUNCTIONAL CRITICAL LAYER

This study adopts a two-layered comparative methodology. The first layer is the functional comparative method developed by Zweigert and Kötz and refined by Michaels, which proceeds from the premise that legal systems should be compared not by their formal categories but by the social problems they address and the functional solutions they generate. The function chosen as the comparative tertium comparation is in this study is the allocation of the legal consequences of personal data breaches between data subjects, controllers, processors, and the State. This functional anchor enables a meaningful comparison between systems whose doctrinal architectures differ substantially: the Civil Transaction Law of Saudi Arabia read with Personal Data Protection Law; the dualistic Jordanian framework combining the Civil Code with the Personal Data Protection Law No. 24 of 2023; and the supranational European framework of Regulation (EU) 2016/679.

The second layer is a post-functional critical correction. Pure functionalism has been criticized for its presumption of equivalence and for assuming that systems necessarily converge towards a common functional optimum. Following the post-functionalist critique advanced by Frankenberg and the contextual comparative law approach developed by Husa, this study treats functional similarity as a hypothesis to be tested rather than a premise to be assumed. In particular, the study interrogates the doctrinal and institutional transferability of European solutions to the Saudi and Jordanian contexts, attending to the embeddedness of legal rules in distinct constitutional, jurisprudential, and enforcement infrastructures. The post-functional layer is operationalized through an explicit transferability assessment in Section VII.

2. JUSTIFICATION FOR THE SELECTION OF JURISDICTIONS

The selection of Saudi Arabia, Jordan, and the European Union is not based on geographic or general similarity claims. It rests on three explicit selection criteria. First, recency of codification: each jurisdiction has enacted or substantially recodified its civil-liability framework relevant to data breaches between 2016 and 2024 (GDPR 2016/679; Saudi PDPL 2021 amended 2023 and Civil Transactions Law 2023; Jordanian PDPL No. 24 of 2023). This temporal alignment enables comparison of frameworks at comparable stages of doctrinal maturation. Second, structural diversity: the three systems represent three distinct doctrinal configurations a comprehensively codified national system rooted in Islamic legal tradition (Saudi Arabia), a dualistic system combining a continental-civilian Civil Code with a recent sector-specific statute (Jordan), and a supranational regulation operating across plural Member-State doctrines (EU). This diversity maximizes analytical leverage by ensuring that observed convergences are not artefacts of doctrinal proximity. Third, relevance to the research question: each jurisdiction has explicitly addressed civil liability for personal data breaches through a combination of general tort rules and sector-specific obligations, making them genuine objects of comparison rather than asymmetric cases.

The exclusion of other jurisdictions notably the United States, the United Kingdom, and other Gulf Cooperation Council States is principled rather than incidental. The United States operates a sectoral state-by-state liability regime that is structurally incommensurate with the codified frameworks studied here; the United Kingdom's post-Brexit divergence raises a distinct comparative question; and other GCC States have not yet enacted civil-liability provisions sufficiently developed to warrant inclusion. A broader regional or trans-Atlantic comparison is identified as a future research agenda.

3. JUSTIFICATION FOR THE SELECTION OF EUROPEAN CASE LAW

Three transparent criteria govern the selection of CJEU jurisprudence. First, all judgments selected interpret Article 82 GDPR (the right to compensation provision) and have been delivered by the Grand Chamber or in chamber-of-five formations, ensuring doctrinal authority. Second, the judgments selected address the three indicators of liability that frame the comparative analysis: the burden of proof (Case C-340/21), the threshold and scope of compensable non-material damage (Cases C-300/21, C-456/22, C-687/21), and the relationship between accountability obligations and exoneration (Case C-340/21). Third, the temporal

cut-off is set at judgments delivered up to and including 31 March 2026; subsequent rulings are referenced where relevant but are not included in the core analytical corpus, to maintain a stable evidentiary basis.

The selection deliberately privileges judgments that have generated doctrinal controversy or have been the subject of sustained academic commentary, ensuring that the comparative analysis engages with the contested rather than the settled portions of European case law. Earlier rulings concerning data-protection rights, prior to the GDPR's entry into force in 2018, are excluded, as they predate the liability architecture under analysis.

4. OPERATIONALISING ADEQUACY AND EFFECTIVENESS: A FIVE-INDICATOR ANALYTICAL MATRIX

The constructs of liability "adequacy" and "effectiveness" are notoriously contested in comparative tort scholarship. To avoid the criticism that they are deployed at high levels of generality without analytical traction, this study treats them as operational analytical constructs, each capable of structured assessment. Liability adequacy is taken to mean the extent to which a legal framework provides a coherent doctrinal basis for recognizing, attributing, and compensating harm arising from data breaches; it is concerned with the system's internal capacity to accommodate digital harm within its existing liability structure. Liability effectiveness, in turn, refers to the practical ability of that framework to enable claimants to obtain compensation in real-world litigation, and it therefore engages questions of procedural accessibility, evidentiary feasibility, and institutional enforcement. Both constructs are operationalized through a five-indicator matrix. Each indicator corresponds to a discrete analytical question, has identifiable doctrinal markers in each jurisdiction, and admits ordinal comparative ranking (low / partial / high). The indicators are derived inductively from the three principal structural challenges identified in the literature on digital tort liability evidentiary asymmetry, multi-actor processing, and intangible harm supplemented by two indicators that capture the preventive and remedial dimensions of civil liability.

- Indicator I. Burden distribution. Whether the legal framework places the burden of establishing fault, breach of duty, or non-compliance on the claimant, or whether it shifts (in whole or in part) to the controller or processor through statutory presumptions, accountability obligations, or evidentiary disclosure rules.
- Indicator II. Damage scope. Whether and to what extent the framework recognizes non-material damage including loss of control over personal data, anxiety, fear of misuse, and dignitary harm as compensable, and whether such recognition is subject to a severity threshold or de minimis filter.
- Indicator III. Attribution mechanism. Whether the framework provides a doctrinally articulated rule for allocating liability among controllers, joint controllers, processors, and third parties in multi-actor processing chains, including rules of joint and several liability and contribution.
- Indicator IV. Preventive function. Whether the framework links liability to demonstrable accountability obligations (security-by-design, DPIAs, breach notification, certification) rather than relying solely on reactive ex post fault assessment.
- Indicator V. Judicial accessibility. Whether the procedural and institutional environment, including evidentiary disclosure rules, supervisory authority cooperation with civil litigation, and the availability of representative or class actions, facilitates or impedes the practical exercise of the right to compensation.

Each jurisdiction is assessed against the five indicators in Sections V and VI, and the resulting matrix is presented in Table 2 (Section VI). The matrix discharges three analytical functions: it disciplines the comparison by ensuring that all three systems are evaluated on identical dimensions; it renders the assessment of "adequacy" transparent and replicable; and it provides the structural template against which the proposed Risk-Calibrated Accountability Model (Section VII) is designed.

5. REPLICABLE ANALYTICAL STEPS

The analysis proceeds in five replicable steps. Step 1 (doctrinal mapping) identifies the primary legal sources statutes, implementing regulations, and judicial decisions relevant to each indicator in each jurisdiction. Step 2 (indicator scoring) assigns each jurisdiction an ordinal rating (low / partial / high) on each indicator, supported by explicit textual citation to the underlying source. Step 3 (cross-jurisdictional

comparison) generates the comparative matrix and identifies points of convergence and divergence. Step 4 (transferability assessment) examines whether divergent solutions are transplantable across systems, taking into account doctrinal compatibility (for example, whether GDPR's reversal of burden coheres with the structure of fault under Article 120 of the Saudi Civil Transactions Law) and institutional capacity (for example, whether the Jordanian Personal Data Protection Council possesses the operational capacity to discharge supervisory functions). Step 5 (model construction) synthesizes the comparative findings into the Risk-Calibrated Accountability Model articulated in Section VII.

6. ROBUSTNESS CONSIDERATIONS, COUNTER-PERSPECTIVES, AND ETHICAL DIMENSIONS

The study incorporates three robustness considerations. First, alternative doctrinal interpretations of Saudi and Jordanian provisions particularly Article 120 of the Civil Transactions Law and Article 256 of the Jordanian Civil Code are explicitly canvassed where the doctrine admits more than one reading. Second, counter-perspectives drawn from law-and-economics scholarship (notably the deterrence-versus-compensation trade-off) and from critical privacy scholarship (notably the dignitary-versus-instrumental conception of data protection) are engaged in the construction of the proposed model. Third, the study acknowledges that legislative recency in Saudi Arabia and Jordan limits the empirical evaluability of judicial application; this limitation is treated as a finding in itself rather than as a reason to extrapolate beyond the available evidence.

The study also engages briefly with the ethical implications of digital civil liability. Liability rules are not normatively neutral: they distribute risk between data subjects (who are typically the structurally weaker party in informational power) and data controllers (who derive economic value from processing). A liability framework that under-protects data subjects effectively externalizes the costs of digital innovation onto individuals, raising distributive-justice concerns. The Risk-Calibrated Accountability Model proposed in Section VII is designed to internalize these ethical commitments while preserving doctrinal coherence with the codified frameworks of Saudi Arabia and Jordan.

IV. CONCEPTUAL FRAMEWORK FOR DATA BREACHES

1. DEFINING DATA BREACHES IN THE DIGITAL ENVIRONMENT

The concept of a data breach has gained increasing legal significance in legal systems and regulatory frameworks, as digital technologies continue to reshape the processing and storage of personal information. A data breach is generally defined as any unauthorized access to, disclosure of, or loss of personal data, whether accidental or intentional. This definition has been widely adopted in regulatory frameworks and academic studies, with an emphasis on both the security dimension and its impact on individual rights [1].

Legally, the danger of data breaches lies not merely in the unauthorized access itself, but in the resulting consequences, particularly when these incidents harm the individuals involved. Modern data protection regulations, most notably the GDPR, define data breaches as events that may compromise the confidentiality, integrity, or availability of personal data [14]. This three-part classification reflects a shift towards a risk-based understanding of data security, where legal judgment is closely linked to the potential impact on individuals [20]. Article 2 of the Jordanian Personal Data Protection Law No. 24 of 2023 adopts a largely similar approach, defining a data breach as any incident involving unauthorized access, processing, transfer, or any action that compromises the security and integrity of data [9]. Despite the clarity of definitions in relevant laws and regulations, the legal characterization of data breaches remains complex. Not all breaches result in harm that warrants legal action, and the establishment of liability varies considerably across different legal and judicial systems. This raises fundamental questions about the extent to which a mere data security breach can give rise to civil liability, particularly in cases where the damage is widespread, delayed, or difficult to assess [3].

2. THE LEGAL NATURE OF PERSONAL DATA AND PROTECTED INTERESTS

Understanding civil liability for data breaches requires a clear understanding of the legal nature of personal data and the interests it seeks to protect. Traditionally, civil liability systems have been designed to protect tangible interests such as property and physical safety. In contrast, personal data constitutes an intangible asset closely linked to an individual's autonomy, identity, and privacy [13]. The evolution of data protection law reflects a broader recognition that personal data is not merely something of financial value, but also a fundamental element of inherent human rights [30]. This is clearly evident in European legal frameworks, where data protection is treated as a fundamental right. Consequently, the harm caused by data breaches can extend beyond financial loss to include intangible damages such as psychological distress, loss of control over personal information, and reputational damage [31].

In contrast, the legal systems of Saudi Arabia and Jordan have gradually established personal data as a legally protected interest. Recent legislative developments, such as the Saudi Personal Data Protection Law [7, 16, 22, 32] and the Jordanian Personal Data Protection Law No. 24 of 2023 [10], indicate a growing awareness of data protection concerns. Furthermore, the Saudi Civil Transactions Law of 2023 [9] provided, for the first time, a legal basis for compensation for material and moral damages under Articles 120 to 143, which regulate tort liability. However, the integration of personal data within the broader framework of civil liability remains in its early stages in both legal systems, creating uncertainty about the types of damages that can be legally compensated and the standards that should be applied in assessing liability.

3. TYPES OF DAMAGE FROM DATA BREACHES

Identifying and classification of damage constitute one of the most complex aspects of civil liability in data breaches. Unlike traditional tort liability, where damage is often immediate and measurable, damage from data breaches can be indirect, cumulative, or even potential [19]. Legal research generally distinguishes between material and non-material damage. Material damage includes financial losses, such as identity theft, fraud, or costs associated with mitigating the effects of a breach. These types of damage are relatively easy to identify and assess, and they align with traditional concepts of damage compensation [33].

In contrast, non-material damage presents significant legal challenges. Data breaches can cause psychological harm, anxiety, or a sense of loss of privacy, even in the absence of direct financial loss [4]. Courts, particularly within the European Union, have increasingly recognized that such damages are compensable, reflecting a growing understanding of the impact of data misuse [34]. However, this recognition of the compensable nature of moral damages is not uniform across different legal systems, as many still impose restrictive standards for proving non-material damages. Moreover, the temporal dimension of the damage complicates assessing liability. The consequences of a data breach may not appear immediately, and in some cases, the full extent of the damage may remain unknown for a long time. This raises important questions about the adequacy of existing legal principles in accommodating the dynamic, uncertain nature of damages arising in cyberspace [35].

4. DATA BREACHES AND THE STRUCTURE OF CIVIL LIABILITY

The challenges in defining the concepts mentioned above have direct implications for the structure of civil liability. Traditional liability models are based on clearly defined elements: fault, tort, and causation. However, in the context of data breaches, proving each of these elements becomes more difficult [2]. Determining fault can be challenging due to the technical complexity of cybersecurity systems and the evolving nature of cyber threats. Organizations may implement reasonable security measures yet remain vulnerable to sophisticated attacks, raising the question of whether liability should be based on fault or on a more stringent standard [36]. Article 120 of the Saudi Civil Transactions Law states that “every fault that causes harm to another shall be compensated by the perpetrator,” thus adopting the classical fault-based approach [9]. However, the law does not explicitly address the standard of care required in cybersecurity contexts, leaving considerable room for judicial interpretation.

Similarly, as previously mentioned, the concept of harm must be broadened to include non-material damages, while establishing causation becomes more complex in multilateral environments involving data

controllers, processors, and third-party service providers [20]. These challenges suggest that current civil liability frameworks may require significant modification to remain effective in the digital age.

V. LEGAL BASIS OF CIVIL LIABILITY FOR DATA BREACHES

1. BURDEN OF PROOF AND EVIDENTIARY CHALLENGES IN DATA BREACH CASES

Determining and allocating the burden of proof is one of the most significant challenges in establishing civil liability for data breaches. Under traditional civil liability rules, the plaintiff bears the burden of proving fault, harm, and causation. However, in the context of data breaches, this allocation often places an excessive, and in some cases unrealistic, burden on data owners [11]. The technical complexity of cybersecurity systems, coupled with the information imbalance between data controllers and individuals, severely limits the plaintiff's access to relevant evidence. Key information regarding the cause of the breach, the adequacy of security measures, and internal compliance practices typically remains with the defendant. Consequently, data owners may face significant evidentiary obstacles, even when harm is evident [1]. Comparative legal developments indicate a gradual shift toward more balanced means of proof. Under the General Data Protection Regulation (GDPR), the burden of proof is partially alleviated by a mechanism requiring data controllers to prove their lack of liability for the harm. This approach effectively establishes a form of rebuttable presumption of liability, thereby enhancing access to justice for affected individuals [14, 19].

In contrast, the Saudi and Jordanian legal systems remain largely grounded in traditional rules of evidence, with limited mechanisms for shifting the burden of proof in civil cases [22, 28]. While Article 20 of Jordan's Personal Data Protection Law holds controllers liable for "gross negligence or misconduct" that caused harm to data subjects [10], it does not alter the burden of proof. Similarly, Saudi Arabia's Civil Transactions Law maintains the classic distribution under Article 120, requiring the plaintiff to prove fault [9]. This creates a disadvantage for plaintiffs and may undermine the deterrent function of civil liability. Therefore, there is a pressing need to reconsider the distribution of the burden of proof in data breach cases, particularly given the technical and informational complexities involved.

2. MULTI-PARTY LIABILITY AND THE PROBLEM OF ATTRIBUTION

Data breaches rarely result from the actions of a single party. Rather, they typically occur within complex digital environments involving multiple parties, including data controllers, processors, cloud service providers, and third-party vendors [1]. This multiplicity complicates the determination of liability and raises fundamental questions about the structure of civil liability. Traditional liability models are based on relatively direct relationships between the perpetrator and the victim. In contrast, modern data processing environments are characterized by a diffusion of liability, where multiple entities may contribute to or exacerbate a breach. For example, a vulnerability in a component of a third-party software program may be exploited to access data stored by the primary controller, making it difficult to identify the responsible party [12]. The European approach offers a more practical solution by recognizing joint and several liability among the actors involved in data processing. This allows claimants to obtain full compensation from any responsible party, which in turn may seek a contribution from other parties [34]. This approach reflects a political choice that prioritizes victim protection over the precise apportionment of liability [31].

In contrast, the Saudi and Jordanian legal frameworks adopt a more restrictive approach to multilateral liability in data breach cases. Article 127 of the Saudi Civil Transactions Law addresses multilateral liability in general terms, stating that if several persons are responsible for a harmful act, they are jointly and severally liable, and the court determines each party's share; if apportionment is not possible, liability is equal [9]. However, neither the Saudi nor the Jordanian Personal Data Protection Law contains explicit provisions specifically designed for multilateral data breaches [10, 22]. Consequently, courts may find it difficult to apply general principles to cases involving distributed technical liability, potentially leading to unsatisfactory outcomes. This highlights the need for clearer legal rules that reflect the realities of modern data environments and ensure effective compensation mechanisms.

3. RISK-BASED LIABILITY AND PREVENTIVE LIABILITY

A recent trend in contemporary legal thought is the gradual shift from fault-based liability to risk-based and preventive models [30]. This shift is particularly important in the context of data breaches, where harm often arises not from deliberate misconduct, but from systemic vulnerabilities and sophisticated technological risks. Risk-based liability emphasizes holding those best positioned to prevent harm responsible, regardless of whether fault can be proven in the traditional sense. In the context of data protection, this approach aligns with the principle of accountability, which obligates organizations to implement appropriate technical and organizational measures to ensure data security [36]. The GDPR embodies elements of this approach by imposing proactive obligations on data controllers and linking liability to compliance with these obligations [14, 37]. Rather than focusing solely on subsequent fault, the GDPR encourages proactive risk management, thus strengthening the preventive function of civil liability.

In Saudi Arabia and Jordan, the legal framework has begun to incorporate preventive elements, but it remains largely reactive. The Saudi Personal Data Protection Law imposes proactive obligations on data controllers, including reporting any data breach and taking appropriate security measures [7, 8, 27]. Similarly, Article 20 of the Jordanian Personal Data Protection Law requires data controllers to notify affected data subjects within 24 hours and the relevant unit within 72 hours of discovering any serious breach [10]. However, the integration of these preventive obligations with the civil liability system, particularly under Article 120 of the Saudi Civil Transactions Law and the general principles of tort liability in Jordanian law, remains incomplete [9]. This gap underscores the need for a more forward-looking approach that links legal liability with the ability to manage technical risks.

4. REBUILDING THE RULES OF CIVIL LIABILITY IN THE DIGITAL ENVIRONMENT

The preceding analysis demonstrates that traditional legal foundations of tort and contractual liability may be insufficient when applied to data breach scenarios [11, 28]. The increasing impact of evidentiary challenges, multi-party involvement, and evolving risk structures necessitates a more nuanced and flexible model of civil liability. This model should incorporate several key elements: a more flexible approach to determining liability, a broader recognition of compensable harm (including non-material damages), a redistribution of the burden of proof, and mechanisms for addressing shared liability among multiple actors [20, 33]. It bears emphasizing that these modifications should not be seen as a departure from established legal principles, but rather as an evolution of them in response to new forms of harm.

From a comparative perspective, the European framework offers valuable insights into recalibrating civil liability to address digital risks more effectively [19, 20, 31]. However, any attempt to transfer these elements to the Saudi and Jordanian legal systems must take into account their respective doctrinal foundations and institutional contexts, including recent codifications. Ultimately, the challenge lies in establishing a coherent legal framework that ensures effective protection for individuals and a fair distribution of responsibility among data processors. This requires striking a delicate balance between legal certainty and normative flexibility, an issue addressed in greater detail in the following section through a comprehensive examination of national legal systems.

VI. CIVIL LIABILITY FOR DATA BREACHES UNDER SAUDI AND JORDANIAN LAW

1. CIVIL LIABILITY UNDER SAUDI LAW: BETWEEN GENERAL PRINCIPLES AND SPECIFIC REGULATION

The legal framework governing civil liability for data breaches in Saudi Arabia comprises two laws: the newly codified Saudi Civil Transactions Law of 2023, which serves as the general law on civil liability, and the Saudi Personal Data Protection Law, which is sector-specific [9, 22, 32]. Despite the significant progress the Kingdom has made through these two prominent pieces of legislation, their integration is still in its early stages.

At the level of general principles, civil liability under Saudi law is currently regulated by Articles 118 to 143 of the Civil Transactions Law, issued by Royal Decree No. M/191 dated 29/11/1444 AH, which entered into force on December 16, 2023 [9]. Article 120 establishes the principle of liability based on fault, stipulating that any fault that causes harm to another obligates the perpetrator to provide compensation. Article 125 defines exceptions, exempting liability in cases where the damage arises from force majeure, the fault of a third party, or the victim's own conduct. Article 136 establishes the principle of full compensation, which mandates restoring the injured party to the position they held had the damage not occurred [7]. These principles provide a more structured basis for addressing data breach claims compared to previous practice, which relied on judicial discretion in interpreting legal provisions. However, applying these modern principles to data breaches raises several theoretical and practical challenges. First, determining liability in cybersecurity contexts is highly complex. While organizations are required to implement appropriate security measures, the standard for what constitutes "adequate" protection remains undefined in the Civil Transactions Law. It is only partially addressed by the Personal Data Protection Law and its implementing regulations [2, 21, 23]. The absence of clear judicial or regulatory standards complicates the assessment of negligence and may lead to unacceptable outcomes.

Second, the recognition of non-material damages has seen significant development. Before 2023, Saudi courts were hesitant to award compensation for indirect or moral damages; however, the Civil Transactions Law now provides a legal basis for compensation for a wider range of damages, including lost profits and, in principle, moral damages [8]. Nevertheless, neither the Civil Transactions Law nor the Personal Data Protection Law provides an explicit legal framework to address privacy-related damages arising from data breaches. This creates uncertainty for both plaintiffs and courts when assessing claims based on loss of privacy or psychological distress. Third, the issue of causation presents a significant obstacle. As discussed in previous sections, data breaches often involve complex chains of events and multiple parties. Under Article 120 of the Civil Transactions Law, it can be difficult to establish a direct causal link between the defendant’s conduct and the harm suffered by the plaintiff, particularly in the absence of detailed technical evidence [12, 15].

The Saudi Personal Data Protection Law imposes important regulatory obligations, including requirements on data security, breach reporting, and the appointment of data protection officers [7, 16, 32]. However, it does not provide a comprehensive civil liability system comparable to more mature systems. In particular, the Saudi Personal Data Protection Law does not clearly define the conditions under which compensation is awarded, nor does it comprehensively address key issues such as the burden of proof or multilateral liability. As a result, the current Saudi framework can be described as transitional. While the Civil Transactions Law of 2023 and the Personal Data Protection Law reflect a significant recognition of data protection and civil liability concerns, their jurisprudential integration remains incomplete and requires further legislative and judicial development.

The doctrinal architecture described above operates against a still-formative judicial and supervisory landscape. Two practical considerations bear directly on the assessment of implementation. First, the Saudi Data and Artificial Intelligence Authority (SDAIA), which operates as the competent supervisory authority under the Personal Data Protection Law, has developed a documented enforcement practice through the issuance of regulatory guidance and compliance manuals, the publication of certification frameworks for data-protection officers, and the operation of a notification mechanism for personal data breaches under the Implementing Regulations. Although the body of administrative decisions is not yet systematically published, the documentary record generated by SDAIA particularly the breach notifications received under the Implementing Regulations is of decisive evidentiary value in civil-liability litigation, since it constitutes a contemporaneous record by which courts can assess whether the controller satisfied its security obligations.

Second, judicial implementation under the Civil Transactions Law is at an early stage. Saudi commercial and general courts have, since the entry into force of the 2023 codification, shown a discernible willingness to apply Articles 120 and 136 to non-physical and informational injury, including cases involving the unauthorized disclosure of confidential business data and breaches of professional confidentiality. The

interpretive trajectory suggests that the courts are treating the new codification as a comprehensive framework rather than as a minor adjustment to pre-existing Sharia-based tort principles. However, the absence of a binding system of judicial precedent in the Saudi system means that doctrinal consolidation depends on guidance from the Supreme Court and on horizontal coordination among first-instance courts a process that, in respect of personal data breaches specifically, is still nascent. Taken together, these observations indicate that the Saudi framework, although legislatively advanced, remains in a phase of doctrinal consolidation in which judicial interpretation will play a decisive role in shaping its practical effectiveness.

2. CIVIL LIABILITY UNDER JORDANIAN LAW: RELIANCE ON GENERAL TORT PRINCIPLES TO THE PDPL 2023

The Jordanian framework governance data breach liability is shaped by interaction between the long-established Jordanian Civil Code and the Personal Data Protection Law No. 24 of 2023 [10, 24]. Published in the Official Gazette on September 17, 2023, and entering into force on March 17, 2024, the Personal Data Protection Law represents a significant shift from a system dominated by the principle of general tort liability to a sector-specific legal framework. Under the general tort system in Jordanian law, civil liability is determined by tort, damage, and causation, as stipulated in Articles 256 et seq. of the Jordanian Civil Code. While these elements provide a sufficient theoretical basis for addressing cyber-related harms, their practical application reveals several limitations. As in the Saudi context, proving tort in data breach cases is a significant challenge due to the technical complexity of cybersecurity systems and the lack of clear standards of care [25, 27].

The Personal Data Protection Act 2023 provides a dedicated framework to address some of these limitations. Articles 5 to 15 and Article 20 explicitly set out specific obligations for data controllers, making them liable for "gross negligence or misconduct" and requiring them to compensate affected data subjects [10]. Article 20 imposes reporting obligations, requiring controllers to notify affected data subjects within 24 hours and the Personal Data Protection Unit within 72 hours of discovering a serious breach. Article 21 stipulates that the affected party retains the right to initiate civil proceedings for compensation, in addition to the administrative and criminal penalties provided for in the Act. However, the liability requirements under the Personal Data Protection Act, namely gross negligence or misconduct, are stricter than the standard of liability for a breach under civil law, which may limit their practical application.

The Personal Data Protection Law of 2023 provides a dedicated framework to address some of these limitations. Jordanian law has traditionally adopted a conservative approach to the recognition of non-material damages. While compensation for moral damages is not excluded particularly under Article 267 of the Civil Code courts tend to apply restrictive standards, which can limit plaintiffs' ability to recover compensation for privacy violations or psychological harm resulting from data breaches [24]. The Personal Data Protection Law does not explicitly address the amount or scope of compensable moral damages, leaving this to the general principles of tort liability.

The issue of proving causation also remains problematic. Data breaches often have delayed and indirect consequences, making it difficult to establish a clear and immediate link between the wrongful act and the resulting harm [28, 29]. This is compounded by the lack of procedural mechanisms that would facilitate access to evidence, such as rules on shifting the burden of proof or procedures for disclosing evidence. Although Jordan has enacted legislation to combat cybercrime, notably the Cybercrime Law No. 17 of 2023, this legislation is primarily criminal in nature. It does not provide a comprehensive framework for civil liability [26, 27]. In sum, the Jordanian legal framework is undergoing a significant transformation: the Personal Data Protection Law of 2023 provides a modern regulatory basis, but the civil liability dimension remains tied to general tort principles, which are not designed to address the complexities of digital harm. Furthermore, the Jordanian Data Protection Authority is not yet fully operational, which limits the practical application of the new system.

The Jordanian framework presents a more pronounced gap between statutory design and operational implementation. The Personal Data Protection Council established under Article 6 of the 2023 Law has been

formally constituted but, as of 2026, has not yet attained full operational capacity in staffing, technical expertise, and the routine issuance of implementing guidance. This institutional shortfall has two practical consequences for civil liability. The first is evidentiary: in the absence of regularly published breach reports, compliance findings, and supervisory decisions, civil claimants face significant evidentiary obstacles in establishing the controller's failure to discharge security obligations. The second is interpretive: the Council's silence on the operational meaning of "gross negligence or misconduct" under Article 20 leaves the threshold of liability to ad hoc judicial interpretation, perpetuating the indeterminacy that the 2023 Law was intended to resolve.

The Court of Cassation's jurisprudence offers limited but instructive guidance. In its established case law on professional confidentiality and the protection of trade secrets, the Court has interpreted Articles 256 and 261 of the Civil Code in light of a duty of care modulated by the nature of the relationship and the sensitivity of the information involved. This interpretive approach is doctrinally compatible with the calibrated fault standard advanced in Pillar I of the model proposed in Section VII. However, no published judgment of the Court of Cassation has yet applied these principles specifically to a personal data breach giving rise to digital harm, and the scope and quantification of non-material damage in this context remain unsettled. The Jordanian framework therefore faces a dual challenge: doctrinal limitations in its civil-liability rules and institutional constraints affecting their practical enforcement, with the latter compounding the former.

3. COMPARATIVE ASSESSMENT: STRUCTURAL GAPS AND CONVERGING CHALLENGES

A comparative study of Saudi and Jordanian law reveals similarities and differences in their approaches to civil liability for data breaches [15]. Both systems are based on liability for fault or compensable acts and now have sector-specific legislation for the protection of personal data. However, they differ in the depth of their codification of general civil law. While Saudi Arabia enacted a comprehensive Civil Transactions Law comprising 721 articles in 2023, which codifies tort liability [9], general civil liability in Jordan remains governed by its civil law based on Islamic Sharia, as well as the 2023 Personal Data Protection Law [10].

A key shared limitation is the difficulty of proving fault or compensable acts, and of establishing causation, in complex technical contexts. In both systems, the absence of specialized procedural rules tailored to data breaches places a significant burden on claimants and hinders the attainment of effective compensation [25]. Neither the Saudi Civil Transactions Law nor the Jordanian Personal Data Protection Law places the burden of proof on data subjects, a stark contrast to the GDPR's approach. Another common problem is the limited recognition of non-material damages. While awareness of the importance of protecting privacy and personal data has grown [26], this awareness has yet to translate into a consistent framework for compensation. As a result, individuals may suffer real harm without adequate legal recourse. To illustrate these structural differences, Table 1 provides a comparative overview of the three frameworks according to key dimensions of civil liability for data breaches.

Table 1. Comparative Framework for Civil Liability for Data Breaches: General Data Protection Regulation (GDPR), Saudi Arabia, and Jordan.

Jordan (PDPL 2023 + Civil Code)	Saudi Arabia (PDPL + CTL 2023)	EU / GDPR	Dimension
It is based on the act that triggers the guarantee under civil law; and Article 20 of the Personal Data Protection Act requires "gross negligence or misconduct".	Fault-based under Article 120 of the Civil Transactions Law 2023; PDPL lacks a dedicated liability regime	Accountability-based; partial presumption of liability under Article 82 GDPR	Basis of Liability

Jordan (PDPL 2023 + Civil Code)	Saudi Arabia (PDPL + CTL 2023)	EU / GDPR	Dimension
Claimant bears the burden; no statutory reversal in favor of data subject	Claimant must prove fault, damage, and causation (Art. 120 CTL)	Partial reversal: controller must prove lack of responsibility (Art. 82(3))	Burden of Proof
Recognized under Art. 267 Civil Code but restrictively applied; PDPL silent on scope	Compensable in principle under CTL 2023 (scope broadened); no explicit framework for privacy-related harm	Expressly compensable (Art. 82); confirmed by CJEU in Case C-300/21 and subsequent case law	Non-Material Damage
General tort rules on joint wrongdoers; no PDPL-specific allocation mechanism	General joint liability under Art. 127 CTL; no PDPL-specific rules	Joint and several liability among controllers and processors (Art. 82(4))	Multi-Party Liability
24 hours to data subjects and 72 hours to the Unit (Art 20 PDPL 2023)	Mandatory under PDPL implementing regulations; specific timelines set by SDAIA	72 hours to supervisory authority; prompt notice to data subjects where high risk (Arts. 33–34)	Breach Notification
Personal Data Protection Council; not yet fully operational as of 2026	Saudi Data and AI Authority (SDAIA); fully operational	National DPAs within the EDPB framework; well-established enforcement practice	Supervisory Authority
Security obligations in PDPL; predominantly reactive liability under Civil Code	Security obligations in PDPL; no codified preventive liability in CTL	Risk-based obligations and accountability principle (Art. 24); DPIAs required (Art. 35)	Preventive Liability

Source: Authors' synthesis based on GDPR (Regulation (EU) 2016/679); Saudi Civil Transactions Law (Royal Decree No. M/191 of 2023) and Saudi PDPL; Jordanian Civil Code and PDPL No. 24 of 2023.

Read across these three columns; Table 1 reveals three deeper patterns that shape the analysis in the remainder of this study. The first concerns how each system allocates the burden of proof. The European model has moved towards a partial reversal under Article 82(3) GDPR, whereas the Saudi and Jordanian frameworks still place the full burden on the claimant. In a digital setting where the relevant evidence sits almost exclusively with the controller, this difference is more than procedural; it shapes whether compensation is realistically obtainable. The second pattern relates to non-material damage. All three systems recognize it in principle, but the doctrinal scaffolding differs sharply. European jurisprudence has developed an increasingly articulated framework, while Saudi and Jordanian courts operate under broader, more open-textured rules whose application to privacy-related harm remains uncertain. A third pattern emerges in the treatment of multi-party liability. The European approach prioritizes the data subject by allowing recovery from any controller or processor in the chain, with internal apportionment as a matter for the defendants. The Saudi and Jordanian systems rely on general tort principles that have not yet been calibrated to distributed processing environments. Taken together, these patterns suggest that the divergence between the three systems is structural rather than incremental, and that any reform proposal must engage with the architecture of liability itself, not merely with its individual components.

Table 1 illustrates three frameworks share a common foundation in tort liability based on fault or a provable act. Still, they differ significantly in the distribution of the burden of proof, in the recognition of non-material damages, and in the structuring of multilateral liability. Despite proactive legislative developments in both Saudi Arabia [7, 22] and Jordan [24, 28], a clear structural gap remains: the absence of a coherent and specialized civil liability system for data breaches that integrates general tort rules with sector-specific data protection standards. This gap is particularly pronounced when compared to the European model, which explicitly addresses many of the challenges mentioned above.

4. EMERGING CASE LAW AND LEGAL PRECEDENTS

No assessment of civil liability for data breaches is complete without considering the available case law, which constitutes the practical application of legal rules. However, the picture emerging across the three jurisdictions is strikingly uneven, reflecting not only differences in the maturity of the systems but also in the speed with which courts respond to interpreting emerging legal issues. In the European Union, the Court of Justice of the European Union has developed an important body of case law clarifying the scope of Article 82 of the GDPR. The landmark rulings in case C-300/21, UI v Österreichische Post AG [5], issued on 4 May 2023, established three cumulative conditions for compensation: a breach of the GDPR, material or moral damages, and a causal link between them. The Court explicitly rejected the imposition of a minimum seriousness threshold for non-material damages, thus broadening the scope of compensation while maintaining the requirement to prove actual harm. This ruling was widely considered a landmark in case law concerning Article 82 [4, 19].

Shortly thereafter, in case C-340/21, VB v National Revenue Agency [6], issued on 14 December 2023, the Court of Justice of the European Union addressed a cyberattack targeting the National Revenue Agency of Bulgaria that exposed the personal data of more than six million individuals. The Court established two fundamental principles directly relevant to data breach litigation: first, that the fear of potential future misuse of personal data, even in the absence of actual misuse, can constitute compensable intangible harm, provided that such fear is justified under the circumstances; and second, that the burden of proving the adequacy of technical and organizational measures lies with the data controller, not the data subject. The Court also clarified that the mere fact that the breach resulted from a third-party cyberattack does not relieve the data controller of liability under Article 82(3) of the GDPR. These two rulings, taken together, exemplify the evolving European approach: a broad concept of compensable harm, coupled with an effective redistribution of the burden of proof. Subsequent decisions of Court of Justice of the European Union, including cases C-456/22 Gemeinde Ummendorf and C-687/21 MediaMarktSaturn, have refined this approach, establishing the principle that data subjects must prove actual non-material harm, while benefiting from a more favorable evidentiary framework [20].

In contrast, the Jordanian legal landscape reflects the pre-data-protection-law era. The general principles governing civil liability remain enshrined in Article 256 of the Jordanian Civil Code, which stipulates that "any harm inflicted on another obligates the perpetrator, even if not legally competent, to compensate for the harm." The Jordanian Court of Cassation has consistently interpreted this provision to encompass both material and moral damages, considering physical pain, disfigurement, and reputational harm as moral damages warranting compensation [38]. However, no rulings of the Court of Cassation have yet specifically applied Law No. 24 of 2023 to data breaches. This lack of application stems from the law's recent enactment (it entered into force on March 17, 2024, with a one-year grace period ending on March 17, 2025) and the incomplete establishment of the Personal Data Protection Council, the primary enforcement body.

In Saudi Arabia, the application of civil liability in data breach cases is still in its early stages. The Civil Transactions Law of 2023 entered into force on December 16, 2023, while the Personal Data Protection Law became fully effective on September 14, 2023. To the best of the researchers' knowledge, no Saudi court rulings have yet addressed civil liability claims arising from personal data breaches under this new legal framework [8, 22]. Although rulings have been issued in cybercrime and privacy violation cases under the 2007 Cybercrime Law and related criminal laws, these rulings are primarily punitive and do not

substantively address the civil compensation framework currently provided for under the Civil Transactions Law.

The absence of domestic case law is itself a significant indicator, highlighting a considerable gap between the ambitious legislative frameworks recently adopted in both Saudi Arabia and Jordan and their practical application in the courts. As comparative European experience demonstrates, effective protection of data subjects' rights depends not only on the existence of legal provisions but also on courts' willingness to interpret them broadly and consistently. Developing this jurisprudence in the Arab context will likely require time, institutional capacity building, and perhaps legislative clarification to guide judicial reasoning in this new field [15, 21].

5. PROPOSED LEGAL REFORMS

An analysis of Saudi and Jordanian law underscores the urgent need to develop legal principles and improve legislation in the area of civil liability for data breaches [21, 29]. While the 2023 legislation in both countries provides an important foundation, it requires further amendment to ensure its effectiveness amid technological changes. From a general legal principle's perspective, courts may need to adopt more flexible interpretations of fault, tort, and causation, taking into account the specific characteristics of digital torts [4, 18]. This could include broader recognition of non-material torts and a more pragmatic approach to handling evidentiary challenges, particularly when applying Articles 120 and 136 of the Saudi Civil Transactions Law [9] and Article 20 of the Jordanian Personal Data Protection Law [10] to data breach contexts.

From a legislative standpoint, there is a need for clearer, more detailed rules governing civil liability in the context of data breaches [8], [28]. These rules should address key issues, including the distribution of the burden of proof, the handling of multilateral liability, and the scope of damages warranting compensation. Any reform must strike a balance between protecting individuals and ensuring that legal obligations remain proportionate and predictable for institutions. The comparative insights presented in this section provide a foundation for the analysis that follows. The next section will build upon these findings to propose a more coherent and flexible model of civil liability, drawing on both domestic legal principles and international best practices.

Table 2. Comparative matrix of the three jurisdictions across the five indicators of civil liability adequacy. Comparative scores are ordinal: Low / Partial / High.

Indicator	Saudi Arabia (PDPL + CTL 2023)	Jordan (PDPL 2023 + JCC)	EU (GDPR + CJEU)
I — Burden Distribution	Claimant bears the full burden under Art. 120 CTL; PDPL Implementing Regulations create administrative duties but no civil procedural reversal.	Claimant bears the full burden under Art. 256 JCC; Art. 20 PDPL 2023 requires "gross negligence or misconduct"—a heightened standard for the claimant.	Claimant must establish breach and harm; controller must then prove non-responsibility (Art. 82(3) GDPR; C-340/21).
Comparative score	Low	Low	High
II — Damage Scope	Material and moral damage compensable in principle (Art. 136 CTL); no codified framework for non-material harm specific to digital injury.	Material damage clearly compensable; moral damage recognized under Art. 267(2) JCC but restrictively applied to non-physical informational harm.	Material and non-material damage explicitly compensable (Art. 82(1)); CJEU C-300/21 and C-340/21 reject any de minimis threshold.

Comparative score	Partial	Partial	High
III — Attribution Mechanism	General joint liability under Art. 127 CTL (mubāshara/tasabbub); no PDPL-specific allocation rule for multi-party processing chains.	General tort principles on joint wrongdoers (Art. 265 JCC); no PDPL-specific allocation mechanism.	Joint and several liability among controllers and processors (Art. 82(4)); contribution among co-defendants under Art. 82(5).
Comparative score	Partial	Low	High
IV — Preventive Function	Security obligations in PDPL Implementing Regulations and SDAIA guidance; no explicit linkage to civil liability outcome.	Security obligations in PDPL 2023 and Civil Code; predominantly reactive ex post fault assessment.	Risk-based obligations (Art. 24); accountability principle (Art. 5(2)); DPIAs (Art. 35); explicit linkage to liability.
Comparative score	Partial	Low	High
V — Judicial Accessibility	Civil and commercial courts; SDAIA fully operational; no representative-action mechanism specific to data subjects.	Civil courts; Personal Data Protection Council not yet fully operational as of 2026; no representative-action mechanism.	Civil courts in each Member State; supervisory-authority cooperation; representative actions under Art. 80 GDPR.
Comparative score	Partial	Low	High
Aggregate assessment of "adequacy."	Partially adequate; structural recalibration via implementing regulations and judicial guidance is feasible without primary legislation.	Inadequate in present form; requires primary-law amendment (Art. 20 PDPL) and institutional capacity-building of the Council.	High overall adequacy; doctrinal solutions partially transferable (see Section VI.6).

Source: Authors' construction (2026), based on the analytical matrix introduced in Section III.4 and applied throughout Sections V and VI. Scores reflect doctrinal and institutional indicators identified in primary legal sources.

Beyond the descriptive comparison offered in Table 1. Table 2 applies the five-indicator matrix to deliver a more disciplined assessment. Two readings stand out. The first is that the European framework scores highly across all five indicators, reflecting an architecture that treats accountability not as a separate compliance regime but as the structural pillar on which compensation rests. The second, more important for the comparative argument, is the close convergence between the Saudi and Jordanian systems. Both retain a fault-based liability core, both lack tailored mechanisms for multi-party processing, and both display only a partial recognition of non-material harm in the digital context. Where the two systems diverge is in institutional capacity. SDAIA's operational maturity gives the Saudi framework a stronger platform for doctrinal consolidation than its Jordanian counterpart, where the Personal Data Protection Council remains in a formative phase. The matrix thus performs two functions at once. It exposes the structural, not incremental, distance between the European model and the two Arab frameworks; and it shows that the deficits within those Arab frameworks are similar enough to justify a shared reform horizon, even if the

implementation pathways must differ. This dual finding furnishes the analytical foundation for the Risk-Calibrated Accountability Model developed in Section VII.

6. TRANSFERABILITY OF EUROPEAN JURISPRUDENCE: A POST-FUNCTIONAL ASSESSMENT

The post-functional methodological posture requires that European doctrinal solutions be assessed for their transferability to the Saudi and Jordanian frameworks. Three considerations structure that assessment. The first is doctrinal compatibility. The reversal of burden under Article 82(3) GDPR, which is anchored in the accountability principle of Article 5(2), is doctrinally compatible with Saudi and Jordanian fault-based codifications only where the satisfaction of statutory preconditions mediates its operation. A direct transposition of the European reversal operating on the bare occurrence of a breach would be doctrinally incongruent with Article 120 of the Saudi Civil Transactions Law and with Articles 256 and 261 of the Jordanian Civil Code, which presuppose proof of a wrongful act by the defendant. By contrast, a conditional reversal triggered by proof of a notified breach causally linked to harm, the formulation adopted in Pillar II of the model proposed in Section VII is doctrinally accommodable within both codifications.

The second is institutional compatibility. The European reversal operates against the background of a mature accountability infrastructure that includes mandatory data-protection impact assessments, certified data-protection officers, codes of conduct, and a network of supervisory authorities coordinated through the European Data Protection Board. The Saudi framework, while not yet replicating the European architecture in full, has developed an operationally significant supervisory infrastructure through SDAIA. The Jordanian framework, as discussed in Section VI.2, has not yet attained equivalent institutional capacity. The transferability of European doctrinal solutions accordingly varies across the two jurisdictions.

The third is the autonomous interpretive concept of "non-material damage" as developed by the CJEU in Cases C-300/21 and C-340/21. The Court's rejection of any de minimis threshold is doctrinally transferable to Saudi law, given the architecture of Article 136 of the Civil Transactions Law (full restoration without a severity floor), and to Jordanian law, given Article 267(2) of the Civil Code (recognition of moral damage without an explicit threshold). The Court's specific characterization of "loss of control over personal data" as a compensable harm in its own right is doctrinally compatible with both systems. Still, it requires articulation of the four objective criteria, sensitivity, scale, foreseeability, and duration, proposed in Pillar III as the structured framework for quantification. The transferability assessment, therefore, concludes that the European jurisprudence offers substantive interpretive resources but cannot be transplanted wholesale; rather, its structural insights must be reconstructed within the doctrinal idiom of each receiving system.

VII. TOWARDS A MODERN LEGAL FRAMEWORK FOR CIVIL LIABILITY FOR DATA BREACHES

1. A PRELIMINARY OBJECTION: THE OVER-DETERRENCE CONCERN

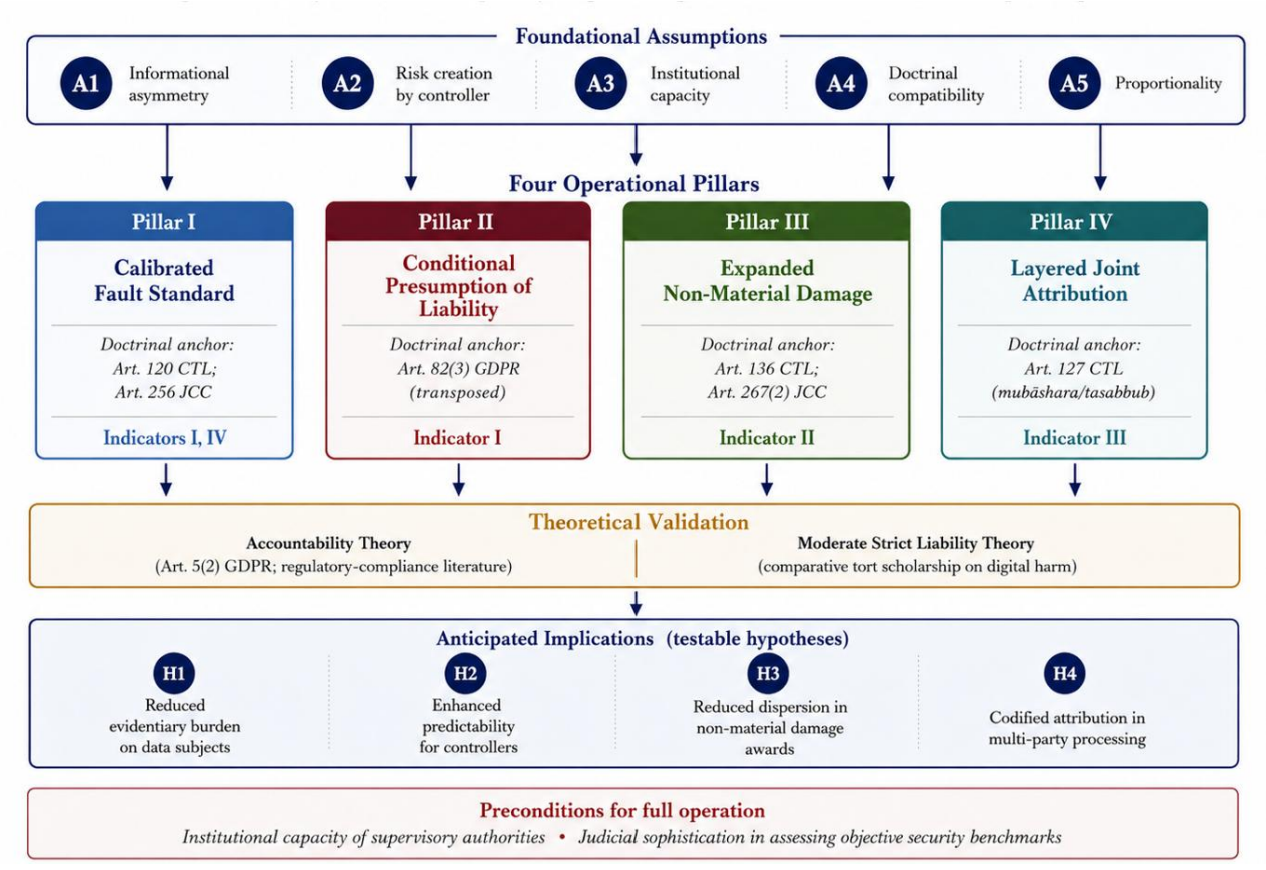
Before turning to the model itself, it is worth pausing to consider a counterargument advanced in the comparative tort literature against the kind of recalibration proposed below. The objection is that introducing burden-shifting mechanisms and broadening the recognition of non-material damage may lead to over-deterrence, disproportionately increase compliance costs for small and medium-sized enterprises, and ultimately discourage the very digital innovation that data protection law was designed to accommodate. The concern carries particular weight in jurisdictions where digital regulatory frameworks are still bedding in. Saudi Arabia has only recently established a coherent supervisory architecture under SDAIA, and Jordan's Personal Data Protection Council is still moving towards full operational capacity. Imposing a high-cost compliance regime on controllers in those institutional environments could, the argument goes, produce reform on paper without enforcement in practice.

This study takes the objection seriously, but does not regard it as a reason to retreat from doctrinal recalibration. The objection rests on an implicit assumption that any departure from claimant-borne burden-shifting necessarily entails strict liability. The Risk-Calibrated Accountability Model developed in the next section is designed precisely to avoid that outcome: liability remains anchored to fault, the reversal of burden

is conditional rather than absolute, and a calibrated proportionality defense is built into the fault standard itself. The model also incorporates the institutional preconditions that the objection rightly identifies, distinguishing the implementation profile suitable for a system with mature supervisory capacity from one in which capacity is still developing. Read in this way, RCAM does not expand liability indiscriminately. It refines the structure of liability so that legal responsibility tracks the realities of digital risk while preserving the doctrinal grammar of fault. This response to the over-deterrence objection forms part of the model's design and is revisited in Section VII in the context of the theoretical validation.

2. FOUNDATIONS AND ASSUMPTIONS OF THE RISK-CALIBRATED ACCOUNTABILITY MODEL (RCAM)

Building on the comparative findings of the preceding sections, this study formalizes a Risk-Calibrated Accountability Model (RCAM) for civil liability arising from personal data breaches. The model is articulated explicitly through three components required of any rigorous legal-theoretical proposal: (a) a set of foundational assumptions, (b) four substantive pillars expressed as operational rules, and (c) anticipated implications and conditions of validity. RCAM is presented as a doctrinal proposal, not as a transplant; it is calibrated to operate within the codified frameworks of Saudi Arabia and Jordan and is validated against existing comparative tort theory (Section VII).



Source: Author's construction (2026). Based on the comparative analysis in section v.

FIGURE 1. The Risk-Calibrated Accountability Model (RCAM): conceptual structure with foundational assumptions, four operational pillars, theoretical validation, and anticipated implications.

RCAM rests on five foundational assumptions, each of which is testable in principle and traceable to identifiable doctrinal anchors. Assumption A1 (informational asymmetry): In personal data processing relationships, the data controller possesses materially superior access to evidence relevant to the cause and adequacy of security measures than the data subject. Assumption A2 (risk creation): the data controller engages in an activity (large-scale automated processing) that creates a non-trivial risk of harm to data subjects, and economically benefits from that activity. Assumption A3 (institutional capacity): liability rules operate against the background of supervisory authorities (the Saudi Data and Artificial Intelligence Authority, the Jordanian Personal Data Protection Council, and EU Data Protection Authorities) whose accountability obligations generate documentary records relevant to civil litigation. Assumption A4 (doctrinal compatibility): a partial reversal of the burden of proof and an objective standard of conduct can be accommodated within fault-based codifications without requiring a wholesale shift to strict liability, by anchoring the reversal to the breach of statutory accountability obligations. Assumption A5 (proportionality): the resulting liability framework must be calibrated to avoid imposing disproportionate burdens on small and medium enterprises and on legitimate processing activities, and must therefore admit objective compliance defenses. These assumptions jointly justify the four pillars articulated below. Where any assumption fails in a particular jurisdiction or context (for example, where supervisory institutional capacity is insufficient, as is presently the case in Jordan), RCAM identifies the failure as a precondition that legislative or regulatory reform must address before the model can operate effectively. The pillars are therefore not free-floating reform proposals but conditional rules whose effectiveness is bound to the satisfaction of the underlying assumptions.

3. PILLAR I — CALIBRATED FAULT STANDARD ANCHORED IN OBJECTIVE SECURITY BENCHMARKS

Pillar I addresses Indicator I (burden distribution) and Indicator IV (preventive function) of the analytical matrix. The pillar reformulates the fault element of civil liability for data breaches by anchoring it not in subjective negligence assessed ex post, but in compliance with objective, ex ante security benchmarks. The operational rule is the following: a data controller is presumed to have acted without fault if, and only if, it can demonstrate compliance with recognized technical and organizational standards proportionate to the risk profile of the processing activity, including but not limited to ISO/IEC 27001, NIST cybersecurity standards, and any sector-specific guidance issued by the competent supervisory authority.

Pillar I is doctrinally compatible with Article 120 of the Saudi Civil Transactions Law, which establishes fault as the basis of liability without specifying how it is assessed. The pillar retains fault as the doctrinal basis but renders its assessment criterion-bound and predictable, addressing the criticism that subjective fault assessment in cybersecurity contexts produces indeterminate outcomes. The same reasoning applies, mutatis mutandis, to the general tort framework set out in Articles 256–267 of the Jordanian Civil Code. The pillar also coheres with the accountability principle in Article 5(2) GDPR and with the European doctrinal trajectory traced in C-340/21, where the Court held that the burden of demonstrating the adequacy of technical and organizational measures lies with the controller.

The pillar admits a calibrated proportionality defense: compliance with industry benchmarks of equivalent rigor to those listed above, including national and regional standards where these exist, satisfies the burden, and the controller is not required to demonstrate compliance with the most onerous available standard. This calibration addresses Assumption A5 and ensures that Pillar I does not impose a uniform high-cost compliance regime on all controllers, irrespective of their risk profile.

4. PILLAR II CONDITIONAL PRESUMPTION OF LIABILITY AND BURDEN-SHIFTING

Pillar II directly addresses the structural deficit identified across all three jurisdictions regarding Indicator I. The pillar introduces a conditional presumption of liability that is triggered upon the joint satisfaction of two preconditions: (a) the claimant establishes the occurrence of a personal data breach within the meaning of the applicable statute (Article 2 Jordanian PDPL; the corresponding provisions of the Saudi PDPL implementing regulations), and (b) the claimant establishes the occurrence of legally cognizable harm causally linked to the breach. Once both preconditions are satisfied, the burden shifts to the controller to

rebut the presumption by demonstrating that it took the security measures required under Pillar I, or by establishing one of the recognized exoneration grounds (force majeure, third-party act, or claimant's own fault, as codified in Article 125 of the Saudi Civil Transactions Law).

The conditional structure of the presumption is essential to its doctrinal compatibility with the Saudi and Jordanian frameworks. Unlike strict liability, the presumption is rebuttable; unlike traditional fault-based liability, the burden of establishing the absence of fault lies with the party in possession of the relevant evidence. This calibration mirrors the architecture of Article 82(3) GDPR, but is triggered by domestic statutory preconditions rather than by reference to GDPR provisions. The pillar accordingly transposes the structural insight of the European model without importing its specific normative content, a distinction central to the post-functional methodological posture adopted in Section III.

Pillar II requires legislative implementation. In the Saudi context, this implementation is appropriately affected through amendment of the implementing regulations of the Personal Data Protection Law, supplementing rather than displacing the general fault rule of Article 120 CTL. In the Jordanian context, implementation requires amendment of Article 20 of the Personal Data Protection Law to reduce the standard of liability from gross negligence or misconduct to ordinary fault assessed under the calibrated standard of Pillar I, accompanied by the conditional presumption of Pillar II.

5. PILLAR III EXPANDED BUT CRITERION-BOUNDED RECOGNITION OF NON-MATERIAL DAMAGE

Pillar III addresses Indicator II (damage scope). The pillar requires the recognition of non-material damage including loss of control over personal data, justified fear of misuse, anxiety, and dignitary harm as a compensable head of damage in personal data breach cases, subject to four objective criteria designed to ensure predictability and consistency: (a) the sensitivity of the data category affected (with sensitive data within the meaning of Article 9 GDPR and the equivalent provisions of the Saudi and Jordanian statutes triggering a heightened presumption of compensable harm), (b) the scale of the breach measured by the number of affected data subjects, (c) the foreseeability of misuse given the nature of the breach, and (d) the duration of exposure between breach and remediation.

Pillar III rejects the de minimis or severity-threshold approach. This rejection is doctrinally grounded: in Saudi law, Article 136 of the Civil Transactions Law mandates restoration of the injured party to the position they would have held had the harm not occurred, and contains no severity floor; in Jordanian law, Article 267(2) of the Civil Code recognizes moral damage without imposing such a threshold; and in European law, the Court of Justice has explicitly rejected the imposition of a severity threshold in C-300/21 and reaffirmed this position in subsequent rulings. The four objective criteria function not as a threshold for admissibility but as a structured framework for quantification, addressing the legitimate concern that unbounded recognition of non-material damage can lead to indeterminate compensation awards.

The pillar coheres with the broader trajectory of Saudi and Jordanian doctrine on moral damage. Saudi judicial practice since the entry into force of the Civil Transactions Law has shown a growing acceptance of moral damage claims; Jordanian Court of Cassation jurisprudence has long recognized moral damage but has applied it restrictively in cases involving non-physical harm. Pillar III provides a structured doctrinal framework that channels rather than expands judicial discretion.

6. PILLAR IV LAYERED JOINT ATTRIBUTION FOR MULTI-PARTY PROCESSING

Pillar IV addresses Indicator III (attribution mechanism). The pillar introduces a layered attribution rule designed to operationalize multi-party liability in technically complex processing chains. The rule has three layers, each with distinct doctrinal implications.

Layer 1 (external joint and several liability): vis-à-vis the data subject, all entities involved in the processing chain that materially contributed to the breach, including data controllers, joint controllers, processors, and third-party service providers, are jointly and severally liable for the full amount of compensable damages. This layer prioritizes the data subject's practical access to a remedy. It is anchored in Article 127 of the Saudi Civil Transactions Law (general joint liability for harmful acts) and in the corresponding general tort principles of Jordanian law. The European parallel is Article 82(4) GDPR. Layer

2 (internal contribution and apportionment): among the jointly liable entities, contribution is determined according to each party's causal contribution and degree of fault. Where causal contributions cannot be precisely apportioned, Article 127 CTL's default rule of equal apportionment applies. This layer preserves fairness among potentially liable parties without compromising the data subject's ability to obtain full compensation from any single defendant. Layer 3 (contractual reallocation): processing agreements, data processing addenda, and similar contractual instruments may reallocate the internal apportionment of Layer 2. Still, they cannot derogate from the external joint and several liability of Layer 1. This layer preserves contractual freedom in the commercial relationships among processing entities while protecting the public-interest dimension of data subject protection.

The three-layer structure is grounded in the classical Islamic legal doctrine of attribution, which distinguishes between direct causation (mubāshara) and indirect causation (tasabbub), and underpins Article 127 CTL. Pillar IV accordingly draws on doctrinal resources internal to the Saudi framework while achieving functional equivalence with the European model.

7. THEORETICAL VALIDATION: RCAM AGAINST ACCOUNTABILITY THEORY AND MODERATE STRICT LIABILITY THEORY

RCAM is validated against two existing strands of comparative tort theory. The first is accountability theory, developed in the regulatory-compliance literature and codified in Article 5(2) GDPR, which posits that liability rules should be structured around the demonstrable discharge of organizational obligations rather than around ex post fault assessment. RCAM aligns with accountability theory through Pillar I (the calibrated fault standard) and Pillar II (the conditional presumption tied to statutory preconditions). The model satisfies the central commitments of accountability theory while preserving the doctrinal centrality of fault, thereby avoiding the criticism leveled at pure accountability frameworks that they sever liability from individual moral responsibility.

The second is the moderate strict-liability theory, which holds that liability for harm arising from inherently risky activities should rest on the entity that creates and controls the risk, subject to defined grounds for exoneration. RCAM aligns with a moderate strict-liability theory through the conditional presumption of Pillar II, but resists the full strict-liability corollary by requiring proof of breach and harm as preconditions and by admitting the calibrated compliance defense of Pillar I. RCAM thus occupies a doctrinally defensible middle position between fault-based and strict-liability paradigms. This position has been advocated in recent comparative tort scholarship as the appropriate response to digital harm.

The model's anticipated implications can be specified. First, RCAM is expected to reduce the evidentiary burden on data subjects without imposing strict liability, thereby improving Indicator V (judicial accessibility) without compromising doctrinal coherence. Second, by anchoring fault assessment in objective benchmarks, RCAM is expected to enhance predictability for controllers and reduce litigation indeterminacy. Third, by providing a structured framework for quantifying non-material damage, RCAM is expected to reduce dispersion in judicial awards. Fourth, by codifying multi-party attribution, RCAM is expected to address the structural deficit identified in Indicator III without requiring fundamental restructuring of the underlying civil codes. These implications are framed as testable hypotheses for future empirical evaluation, as the Saudi and Jordanian frameworks generate sufficient case law.

Two limitations of RCAM should be acknowledged. First, the model's effectiveness is conditional on the institutional capacity of the supervisory authorities. Where institutional capacity is deficient, as in the present Jordanian context, given the partial operationality of the Personal Data Protection Council, Pillar II's presumption operates with reduced effectiveness because the documentary record on which it relies is thinner. Second, the model presupposes a degree of regulatory and judicial sophistication in assessing objective security benchmarks that may not be uniformly available in early-stage case law. These limitations are not fatal to the model; they identify the institutional preconditions for its full operation.

8. IMPLICATIONS FOR LEGAL DEVELOPMENT IN SAUDI ARABIA AND JORDAN

The implementation of RCAM in Saudi Arabia and Jordan has distinct profiles that reflect the different doctrinal and institutional starting points of the two jurisdictions, even though the underlying analytical deficits are structurally analogous.

In Saudi Arabia, RCAM operates principally by interpreting Articles 120, 125, 127, and 136 of the Civil Transactions Law in their application to data breach cases, supplemented by amendments to the implementing regulations of the Personal Data Protection Law. The calibrated fault standard for Pillar I can be instantiated by issuing supervisory guidance in accordance with accepted technical and organizational standards. The conditional presumption of Pillar II requires regulatory rather than legislative reform: an amendment to the implementing regulations specifying that, upon proof of a notified breach causing harm, the burden of establishing compliance with security obligations shifts to the controller. The non-material damage framework of Pillar III is coherent with Article 136 CTL and requires only judicial articulation through guidance from the Supreme Court. Pillar IV is already substantially covered by Article 127 of the CTL and requires only supervisory clarification regarding its application to data processing chains.

In Jordan, the implementation profile is more demanding because the institutional preconditions are less fully realized. Pillar I require the Personal Data Protection Council to issue technical guidance on security obligations, a function currently hindered by the Council's partial operational capacity. Pillar II requires legislative amendment of Article 20 PDPL to recalibrate the standard of liability from gross negligence or misconduct, which is structurally too high, to ordinary fault assessed under the calibrated standard. Pillar III can be implemented through judicial articulation under Article 267(2) of the Civil Code without legislative reform. Pillar IV requires either legislative articulation in the PDPL or a sustained line of Court of Cassation jurisprudence applying joint liability principles to multi-party processing chains.

In both jurisdictions, the implementation of RCAM is therefore a graduated reform agenda rather than a single legislative event. The model identifies the doctrinal anchors and the institutional preconditions for each pillar, providing a structured pathway for incremental reform that respects the codified architecture of each system. By drawing on comparative insights, on doctrinal resources internal to each system, and on the post-functional caution against legal transplantation, RCAM offers a calibrated response to the digital transformation of civil liability that is both theoretically grounded and practically actionable.

VIII. CONCLUSION

The doctrinal trajectory traced in the preceding sections discloses a recurrent structural feature of contemporary civil liability for personal data breaches: across the three jurisdictions examined, the architecture of fault-based liability, however refined by recent codification, remains imperfectly calibrated to the evidentiary, attributional, and compensatory peculiarities of digital harm. The Saudi Civil Transactions Law of 2023 and the Jordanian Personal Data Protection Law of 2023, although they represent significant legislative achievements, reproduce within their respective doctrinal idioms the same five structural deficits identified by the analytical matrix in Section III.4: an unrelieved burden of proof on the data subject, an under-articulated framework for non-material damage, an under-developed mechanism for multi-party attribution, a thin preventive-accountability linkage, and limited judicial accessibility through procedural infrastructure. The European model, by contrast, has developed an accountability-based architecture that addresses each of these deficits but does so through doctrinal devices that are not directly transplantable to non-EU codifications.

The principal theoretical contribution of this study lies in three propositions that together constitute its claim to scholarly novelty. The first proposition is that the constructs of liability adequacy and effectiveness, which are pervasive in the comparative privacy-tort literature, are analytically tractable only when operationalized through a finite set of doctrinally measurable indicators. Section III.4 of this study has advanced one such operationalization, the five-indicator analytical matrix, and has demonstrated its capacity to discipline the comparative analysis by ensuring that all three systems are evaluated on identical

dimensions. The matrix is offered as a methodological contribution that is portable to other comparative inquiries in digital civil liability.

The second proposition is that the comparative method appropriate to the inquiry is the functional comparative method in its post-functional form: functional similarity must be treated as a hypothesis to be tested rather than as a premise from which convergence may be inferred. The systematic transferability assessment in Section VI.6 has illustrated the operational consequences of this methodological commitment: European doctrinal solutions may furnish substantive interpretive resources to Saudi and Jordanian courts and legislators, but they cannot be transplanted wholesale; their structural insights must be reconstructed within the doctrinal idiom of each receiving system. The post-functional layer accordingly performs a critical function not in disqualifying European jurisprudence as a comparative reference point, but in disciplining its use.

The third and most substantive proposition is the RCAM advanced in Section VII. RCAM occupies a doctrinally defensible middle position between fault-based liability and strict liability: it preserves fault as the doctrinal basis of liability while anchoring its assessment in objective security benchmarks (Pillar I); it conditions a partial reversal of the burden of proof on statutory preconditions rather than on the bare occurrence of a breach (Pillar II); it expands the recognition of non-material damage but bounds the expansion through four objective quantification criteria (Pillar III); and it codifies multi-party attribution through a three-layer rule anchored in the classical Islamic legal doctrine of mubāshara and tasabbub (Pillar IV). RCAM is validated against accountability theory and moderate strict liability theory, yielding four anticipated implications framed as testable hypotheses (H1–H4) and two explicitly acknowledged institutional preconditions. The model is calibrated, in distinct implementation profiles, to the codified architectures of Saudi Arabia and Jordan.

Three normative conclusions follow from this theoretical apparatus. For the Saudi legislator and supervisory authority, the most pressing reform is regulatory rather than legislative: the implementing regulations of the Personal Data Protection Law should be amended to articulate the conditional presumption of Pillar II, and the Supreme Court should be invited to issue interpretive guidance on the application of Article 136 to non-material harm in data breach cases. For the Jordanian legislator, the priority is twofold: amending Article 20 of the Personal Data Protection Law to recalibrate the standard of liability from gross negligence to ordinary fault assessed under the calibrated standard, and implementing capacity-building measures to render the Personal Data Protection Council fully operational. For both jurisdictions, the implementation of RCAM is a graduated reform agenda, not a single legislative event.

The study acknowledges its limitations. The legislative recency of both Saudi and Jordanian frameworks limits the empirical evaluability of judicial application; this limitation, identified as a finding rather than as a methodological defect (Section III.6), frames the empirical agenda for future research. The four anticipated implications of RCAM are offered as testable hypotheses for evaluation as the case-law record develops. Future research is also invited to extend the comparative scope to other Gulf Cooperation Council jurisdictions, to undertake empirical assessment of SDAIA enforcement outcomes, and to interrogate the interaction between civil liability and emerging regulatory regimes for artificial intelligence and algorithmic decision-making, which lie beyond the scope of the present inquiry but represent the natural doctrinal frontier of the framework advanced here.

In sum, this study has sought to move the comparative legal analysis of civil liability for personal data breaches beyond descriptive juxtaposition toward a methodologically disciplined, theoretically grounded contribution. The Risk-Calibrated Accountability Model is offered not as a definitive solution but as a calibrated theoretical proposal that respects the doctrinal architectures of the receiving systems, draws on comparative insights without presuming convergence, and provides a structured pathway for incremental reform in two jurisdictions whose codified frameworks are simultaneously recent in enactment and rich in doctrinal resources.

Funding Statement

This research received no external funding.

Author Contributions

Both authors contributed equally to this work. E. A. A. and M. I. A. participated in the conceptualization, methodology, legal analysis, theoretical framework development, drafting, critical revision, and approval of the final version of the manuscript.

Conflicts of Interest

The authors declare that they have no known competing financial interests or personal relationships that could have influenced the work reported in this paper.

Data Availability Statement

No datasets were generated or analyzed during the current study. All legal materials, statutes, case law, and scholarly sources relied upon in this article are publicly available and cited in the references.

REFERENCES

1. Manrique, J. I. T., & Mukhtar, R. (**2025**). Regulating Intelligent Systems in Digital Governance and Legal Transformation. *Qubahan Techno Journal*, *4*(3), 24-40.
2. Alshamrani, A. (**2022**). Data protection and privacy law in Saudi Arabia: Emerging challenges and regulatory responses. *Arab Law Quarterly*, *36*(2), 145–168.
3. Solove, D. J., & Citron, D. K. (**2018**). Risk and anxiety: A theory of data breach harms. *Texas Law Review*, *96*(4), 737–786.
4. Abraham, M. M., Dev, S. I., & Manrique, J. I. T. (**2024**). Asymmetric surveillance governance: A thematic analysis of privacy, national security, and AI regulation in India. *Qubahan Political Journal*, *3*(1), 1-11.
5. Court of Justice of the European Union (**2023**). *Judgment of 4 May 2023, UI v Österreichische Post AG, Case C-300/21, ECLI:EU:C:2023:370*. CJEU.
6. Court of Justice of the European Union (**2023**). *Judgment of 14 December 2023, VB v Natsionalna agentsia za prihodite, Case C-340/21, ECLI:EU:C:2023:986*. CJEU.
7. Sarabdeen, J., & Mohamed Ishak, M. M. (**2025**). A comparative analysis: health data protection laws in Malaysia, Saudi Arabia, and the EU GDPR. *International Journal of Law and Management*, *67*(1), 99–119.
8. Alnasser, H. (**2025**). Negligence and data breaches under Saudi Arabian Personal Data Protection Law (PDPL): A doctrinal analysis. *Journal of Advances in Humanities Research*, *4*(3).
9. Kingdom of Saudi Arabia (**2023**). *Civil Transactions Law, Royal Decree No. M/191 of 29/11/1444H (18 June 2023), entered into force on 16 December 2023*—official Gazette of the Kingdom of Saudi Arabia.
10. Hashemite Kingdom of Jordan (**2023**). *Personal Data Protection Law No. 24 of 2023, Official Gazette No. 5881, p. 4338 (17 September 2023), entered into force on 17 March 2024*—official Gazette of the Hashemite Kingdom of Jordan.
11. Filler, D. M., Haendler, D. M., & Fischer, J. L. (**2022**). Negligence at the breach: Information fiduciaries and the duty to care for data. *Connecticut Law Review*, *54*(1), 105–162.
12. Tschider, C. (**2024**). Data governance failures and the problem of organizational negligence. *Minnesota Journal of Law, Science & Technology*, *25*(2), 231–274.
13. De Hert, P., & Papakonstantinou, V. (**2016**). The new General Data Protection Regulation: Still a sound system for the protection of individuals?. *Computer Law & Security Review*, *32*(2), 179–194.
14. Voigt, P., & von dem Bussche, A. (**2017**). *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer.
15. Zhao, X., Li, J., & Nguyen, H. (**2023**). Data protection and negligence liability: Comparative evidence from the EU and Asia-Pacific. *Computer Law & Security Review*, *50*, 105850.
16. *Brown, J. E., & Alothman, M. S. (2025). Balancing privacy and risk: A critical analysis of personal data use as governed by Saudi insurance law. Laws, 14(4), 47.*
17. *Citron, D. K., & Solove, D. J. (2022). Privacy harms. Boston University Law Review, 102(3), 793–863.*

18. *Schwartz, P. M., & Solove, D. J. (2014). The PII problem: Privacy and* a new concept of personally identifiable information. *New York University Law Review*, *86*(6), 1814–1894.
19. Li, S. (**2023**). Compensation for non-material damage under Article 82 GDPR: A review of Case C-300/21. *Maastricht Journal of European and Comparative Law*, *30*(6), 612–628.
20. Walree, T. F. (**2023**). The relationship between Article 47 CFR and the concept of damages under Article 82 GDPR. *International Data Privacy Law*, *13*(3), 169–185.
21. Zanfir-Fortuna, G. (**2023**). Article 82 GDPR: Right to compensation and liability. In C. Kuner et al. (Eds.), *The EU General Data Protection Regulation (GDPR): A Commentary* (pp. 1160–1179). Oxford University Press.
22. Alhejaili, A. (**2024**). Data protection and privacy in Saudi Arabia: Challenges under the PDPL. *Arab Law Quarterly*, *38*(2), 145–170.
23. 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: Direito Ambiental e Desenvolvimento Sustentável*, *22*(3).
24. Al-Tamimi, Y. (**2021**). Civil liability for technological harm under Jordanian law: Challenges and prospects. *Jordanian Journal of Law and Jurisprudence*, *13*(1), 55–78.
25. Jabbour, M. S., & Jabbour, M. (**2018**). *Personal data and Arab laws: Security concerns and individual rights*. Arab Center for Legal and Judicial Research.
26. Bani Migdad, M. A. M. (**2023**). Publishing via social media sites and the civil liability of the publisher in the Jordanian legislation. *International Journal of Membrane Science and Technology*, *10*(1), 1–12.
27. Maaytah, S., & Kobarie, H. (**2024**). The extent of the impact of cybersecurity rules on electronic civil transactions in Jordanian law. *International Journal of Religion*, *5*(6), 1892–1904.
28. Al-Rawashdeh, A. M. (**2025**). Law applicable to civil liability for cyberattack from the perspective of Jordanian legislation. *International Journal of Legal and Comparative Jurisprudence Studies*, *6*(Special Issue).
29. Khawaldeh, A. M. (**2026**). Civil liability odds in information leaks: Controversial legal debates and emerging judicial doctrines in Jordan: laws, *15*(2), article 26.
30. Lynskey, O. (**2016**). Tortious liability and data protection under the GDPR. In O. Lynskey, *The Foundations of EU Data Protection Law*. Oxford University Press.
31. Koops, B. J. (**2014**). The trouble with European data protection law. *International Data Privacy Law*, *4*(4), 250–261.
32. Kingdom of Saudi Arabia (**2021**). *Personal Data Protection Law, Royal Decree No. M/19 of 09/02/1443H (as amended by Royal Decree No. M/148 of 05/09/1444H, 27 March 2023)*. Saudi Data and Artificial Intelligence Authority (SDAIA).
33. Wright, D., & De Hert, P. (**2016**). *Privacy impact assessment*. Springer.
34. European Data Protection Board (**2021**). Guidelines 01/2021 on data breach notification examples. EDPB.
35. Citron, D. K. (**2019**). *Hate crimes in cyberspace*. Harvard University Press.
36. Allakuliev, M. D. (**2024**). Legal regulation of liability for cyber attacks and data breaches. *International Journal of Law*, *10*(5), 111–113.
37. Schlackl, F., Link, N., & Hoehle, H. (**2022**). Antecedents and consequences of data breaches: A systematic review. *Information & Management*, *59*(7), 103638.
38. Jordanian Court of Cassation (Civil Capacity) (**2019**). *Cassation Decision No. 1598/2019, 6 October 2019, and subsequent decisions to the same effect*. Qararak Legal Publications.
39. Zweigert, K., & Kötz, H. (**1998**). An Introduction to Comparative Law (3rd ed.). Oxford University Press.
40. Michaels, R. (**2019**). The functional method of comparative law. In M. Reimann & R. Zimmermann (Eds.), *The Oxford Handbook of Comparative Law (2nd ed.)* (pp. 345–389). Oxford University Press.