laws

MDPI

Article

Civil Liability Odds in Information Leaks: Controversial Legal Debates and Emerging Judicial Doctrines in Jordan

Ahmed M. Khawaldeh

Civil Law, Law School, Amman Arab University, Amman 11941, Jordan; a.khawaldeh@aau.edu.jo

Abstract

Cyberattacks and data breaches expose individuals and firms to liability in civil courts. Despite regulators' efforts to standardize cybersecurity laws, judges, justices and attorneys have offered a plethora of interpretations to the same laws, causing a great deal of confusion. The current investigation utilizes the Jordanian civil code to illustrate how complex liability becomes in data breaches cases. Through a comprehensive examination of liability rules 256–291 within the civil code, the Supreme Courts' liability precedents, and the new personal data protection law, this analysis finds that liability could be established under strict conditions. Liability claims in Jordanian courts must satisfy the standing doctrine, the presence of injury requiring compensation, and causality, and must demonstrate the clear links between data breaches and the harm/injury suffered. The novelty of the personal data protection law in Jordan is likely to impact how liability is interpreted and established in cybersecurity cases.

Keywords: cybersecurity; data breaches; liability; injury; torts; Jordan

1. Introduction

In 2024, Surfshark reported that 5.5 billion accounts were compromised in data breaches around the globe, marking an eightfold rise in the number of information leaks since the previous year (Surfshark 2024). IBM Security (2024) concluded that the average cost of a data breach was $4.88 million, recording a ten percent rise compared with the prior year. Ransomware attacks accounted for a quarter of all data breaches in 2024, with an average cost of $5.13 million (Firch 2025). On average, organizations spent about 9 months to accurately identify the type, source, cause and extent of a data breach (IBM Security 2024).

The existing cybersecurity practice has failed to keep pace with the increasingly evolving cybercrime around the world (Karasik and Morris n.d.; Morris 2025). In the United States, the number of class action lawsuits doubled between 2022 and 2023, rising from 615 to 1320 (Kardell 2025). The number of claims citing data breaches as the primary reason increased by more than 140% between 2022 and 2024 in the United States (Morris 2024). The total cost associated with data breach cases in the United States exceeded $600 million in 2024 (Nahra and Jessani 2024).

Legal research on liability and cybersecurity law is a developing subject (Nazish and Manzoor 2024). Many of the existing precedents and cases emerge from North America and Western Europe (Teichmann and Wittmann 2023). Little ink has been spilled on liability and data breaches in developing countries such as Jordan (Alshible and Issa 2025). To help address such gaps in the literature, the current study presents liability and data breaches within a rapidly developing cybersecurity legal system, the Jordanian Civil Law.

Check for updates

Academic Editor: Patricia Easteal

Received: 22 October 2025
Revised: 13 March 2026
Accepted: 18 March 2026
Published: 3 April 2026

Copyright: © 2026 by the author. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

The primary objective of this paper is to investigate liability in cybersecurity cases, with a focus on data breaches. The analysis attempts to answer the following related set of questions. What are the potential liability types arising in cybersecurity cases? Under which conditions is each type of liability invoked in legal battles involving data breaches? Additionally, the paper introduces readers to complex legal matters within the liability domain in cybersecurity, such as appropriate due diligence, responsible care or sheer negligence.

The findings of the present paper point to the presence of two broad liability categories in cybersecurity law: contractual and tortuous. More importantly, liability rules in Jordan appear to be more flexible compared with other systems, allowing plaintiffs further grounds for winning data breach-related legal battles. One of the methods in addressing liability challenges is the passage of holistic legislative frameworks, such as the Personal Data Protection Act in Jordan (Law No. 24 of 2023). The Act authorizes courts to assess damage suffered from injuries incurred because of data breaches. Defenses against liability claims in Jordan are afforded under rare circumstances, such as the occurrence of national disasters or compelling external or foreign force resulting in the injury in question.

Understanding liability risks helps decision makers in optimizing internal standard operating procedures so as to avoid fatal mistakes that give rise to liability. On another front, identifying legal remedies and defenses, as well as the conditions under which varying arguments held in courtrooms permit attorneys and judges to understand available and existing legal pathways in real-world cases. Comparatively, the current investigation permits legal scholars to understand the similarities and differences between legal systems with respect to liability issues in cybersecurity law (Onder 2019; Schwarcz et al. 2022). More importantly, legislators will be able to learn about the limits of present regulatory frameworks and the potential avenues to addressing how such controversies could be remedied.

2. Literature Review

2.1. What Is Cybersecurity

Cybersecurity represents the collective effort of protecting digital infrastructure, systems, data and assets (Stallings and Brown 2015; Pfleeger et al. 2015). Cybersecurity endeavors aim to avoid unauthorized access, damage or any type of attack to the digital or physical systems or their components (Tipton and Krause 2007). Thus, all processes, procedures, systems or controls that contribute to the protection of systems fall within the purview of cybersecurity (Whitman and Mattord 2009). Cybersecurity practices include, but are not limited to, strong authentication standards; placement of access controls; frequent software updates; firewalls; security, education, training and awareness (SETA) programs; information encryption; and backup (Andress 2014).

Cybersecurity attacks are plentiful and rising in frequency and intensity according to recent estimates from a variety of reputable organizations (Hadnagy 2014; White 2025). Ransomware attacks, where cyber criminals encrypt the data on a system and demand payment to decrypt the platform, present an ongoing nightmare for firms and organizations (Verizon n.d.). Phishing constitutes another common cybersecurity concern, where ordinary users receive fake or fraudulent emails disguised as formal or official messages with malicious links that collect information without their consent or authorization (The Open Worldwide Application Security Project 2023). Distributed denial of service (DDOS) attacks remain common around the world, which occur when a server receives high traffic to exhaust its limits, resulting in the service becoming unavailable to the users of the server (Bilge and Dumitraş 2012). Data breaches caused by insider threats or external unauthorized access compromise the sanctity of personal information (Bilge and Dumitraş 2012). There

are many forms of cyberattack beyond the common types mentioned previously that threaten the loss of personal data and its use for illicit purposes (White 2025).

2.2. Civil Liability Implementation Barriers in Cybersecurity Regulation

The private sector has vehemently opposed the imposition of strict liability conditions in the software development industry on the basis of fair or reasonable precautionary measures (Studer and De Werra 2017). Code developers have long argued that perfect cybersecurity infrastructures are impossible in the sector because every code could potentially be hacked, retrieved or altered (Studer and De Werra 2017). Thus, holding developers and firms accountable for cyber-attacks results in paralyzing innovators and entrepreneurs (Studer and De Werra 2017).

Many legal experts have proposed the adoption of civil liability requirements to encourage firms to develop less defective or penetrable products (Studer and De Werra 2017). Such an argument rests on the assumption that cyberattacks are facilitated by the presence of vulnerabilities, insufficient protections, and limited preventive measures on the part of manufacturers, code developers or owners of systems (Studer and De Werra 2017).

2.3. Jordanian Context

The Jordanian legal system originated from various transformations from different civil traditions. First, Jordanian civil codes heavily borrow from the Islamic Ottoman codes that ruled the Middle East for several centuries (Ziadeh 1993). Second, new civil codes emerged after modern-day Jordan gained independence from Great Britain (Bhattarai and Yousef 2025). Over time, civil codes have evolved to accommodate emerging needs (Al-Shibli et al. 2023). Judges in Jordanian courts have little interpretive power and enforce civil codes more than setting new precedents (Al-Shibli et al. 2023; Bhattarai and Yousef 2025). Cases are more predictable when compared with common law systems, given the clarity of the civilian codes at hand.

The Jordanian legal system evolution matched the country's economic development over the past few decades (Toubat et al. 2020). Capitalism represents the main economic system underlying business in the country (Redding 2005). Islamic financial systems and instruments also exist to regulate many transactions within and outside of the kingdom. Duty of care is a revered Islamic concept, thus arising in legal approaches such as liability. The personal data protection law emerged because private firms failed to exercise due diligence in protecting consumers' identifiable information. Further, such information was exchanged with many marketing agencies, causing a real nuisance to ordinary citizens. Reports have indicated that, on average, a Jordanian citizen would receive multiple marketing calls and texts daily. To solve the issue, Parliament passed a series of cybersecurity protective measures.

Jordanian consumers have suffered from predatory marketplace practices, exhibited in the high volume of spam calls (Toubat et al. 2020). One of the driving forces behind the frequent telemarketing calls is the absence of firm cybersecurity regulations that protect individual information, privacy and security. Many companies have traded consumers' information for profit without consent in Jordan (Al-Kasassbeh et al. 2023). Therefore, popular pushback from ordinary citizens in Jordan has led the legislature to commence the foundation of a regulatory framework protecting citizens' privately identifiable information (PII).

3. Liability in the Jordanian Legal System

3.1. Contractual Liability

Contractual liability emerges when a party to an active contract fails to deliver the promised goods or services specified in an agreement. For instance, when an online career

services platform, such as LinkedIn, fails to protect premium subscribers' personal data, like passwords, thus breaching the guarantee of its security terms to provide an industry standard security to consumers' information because the company had in fact utilized outdated protection protocols (Perlroth 2012). A variety of reasons lead a party to commit contractual liability, including malicious behavior like fraud or inadvertent actions like fault or negligence (Perlroth 2012). In 2017, the Jordanian Parliament approved a new Consumer Protection Bill specifying the conditions under which contractual liability emerges in a transaction. Table 1 presents several articles in the law demonstrating the right to seek damages if sellers or vendors have failed to honor their commitments in a contract.

Table 1. Consumer Protection Law of 2017 and Contractual Liability.

Article Number	Article Text
Article 3 (a) (1)	The consumer enjoys the right to receive goods and services fulfilling their intended purposes without inflicting harm on his or her needs.
Article 3 (a) (2)	The consumer must receive full and accurate information explicitly about the goods and services purchased
Article 3 (a) (6)	Consumers have the right to seek litigation from any action that abridged his or her rights or cause any harm to his or her needs
Article (6) (a)	The product or service is defected if the necessary safe use conditions for regular or normal utilization are compromised
Article 6 (a) (2)	The product or service is defected if it lacks the necessary appropriate technical specifications applicable to the industry or setting
Article 6 (b) (2)	The product or service is defected if the information provided when the transaction occurs is misleading about the quality or characteristics of the product
Article 7 (a) (1 and 2)	The provider must monetarily compensate consumers in the following conditions: (1) return of defected products and (2) if the product or service has been dispensed already and was defected, then the provider compensates the consumer an appropriate amount commensurate with use and damage in question.
Article 8	It is prohibited to advertise inaccurate information about a product or service.

The Jordanian consumer protection law provides plaintiffs with a variety of pathways in seeking damages suffered from cyberattacks. The infliction of harm, intentional or inadvertent, constitutes the primary argument citizens may advance in Jordanian courts based on actual traceable and redressable injuries (Melfi Alqudah 2024). The second legal instrument plaintiffs possess under the consumer protection law is access to full, sufficient, accurate and reliable information provided clearly and in explicit terms prior to transactions (Alsharu et al. 2024). In cases of injuries, plaintiffs could resort to potential misleading information or incomplete disclosures as arguments justifying remedy claims. Third, plaintiffs may argue that producers or service providers have failed to exert all necessary reasonable effort to implement safety and security measures, causing harm.

3.2. Tort Liability (Harm and Duty of Care)

The Jordanian civil code is indifferent to contractual clauses, limiting liability. If courts find plaintiffs failing in the provision of full disclosures or properly securing consumers' data, liability is established regardless of a contracts' wording (Alsharu et al. 2024; Perlroth 2012). The primary object of interest in legal contests is the presence of harm. The Jordanian legal system treats contracts in the same manner regardless of their type (standard or customizable). All contracts are subject to the same criteria set forth in the varying liability codes. Thus, social treatment to standard form contracts does not exist in Jordan. The

concept of implied liability is subsumed under the full disclosure criterion of establishing liability. Jordanian courts assume that service providers must furnish all the necessary details on their products to consumers. Failure to satisfy such requirements in cases of harm constitutes sufficient grounds for the existence of a breach of an implied liability.

In the absence of contracts, users or firms may engage in harmful acts, sheer negligence, or a failure to exercise fundamentally appropriate protective measures, leading to the loss or leak of personal information (Fakhouri et al. 2023). Under Article 256 of the Jordanian Civil Code, "every harmful act compels its party with compensation" (Khawaldeh 2024). Harmful acts are defined in the Jordanian code as either (1) the breach of compliance with applicable laws causing harm or (2) an error causing harm to others resulting from a failure to exercise the duty of care (Khawaldeh 2024). The Jordanian legislature has allowed defendants to seek compensation resulting from any harmful act regardless of whether it is explicitly stated in a statute or not (Al-Sarayreh 2024). Thus, Jordanian courts have exercised a flexible definition doctrine when accepting claims under tort liability (Alshurman and Albnian 2024).

The single most important condition in tort liability is the presence of harm (Adar and Perry 2022). Jordanian courts have held that harm could be caused by transgressions or failures to exercise duty of care (Khawaldeh 2024). The exact characteristics of the situation have little bearing on the courts' determination to look for whether harm occurred or not, and, if it did, compensation would emerge as a remedy (Albnian and Algaber 2025). Harm manifests in two fashions. First, direct harm resulting from an immediate action causing damage such as spending others' financial assets recklessly. Second, harm could arise indirectly from an action. For instance, a doctor may prescribe a medication that causes other unforeseen illnesses in a patient.

Article 291 of the Jordanian code states that "every person responsible for artifacts or tools requiring special care to avoid its potential harm such as mechanical machinery acts as its guardian" (Alabady 2023). Thus, harm caused by such machines is caused by the guardian except in cases or scenarios where appropriate care or protective measures would not prevent harm. For instance, information security officers are expected to protect digital systems and are responsible for harm caused in data breaches, except in cases such as natural disasters or acts of war (Almugamisi 2025). Article 261 of the Jordanian code provides several remedies to guardians in the case of the presence of harm. If the harm rose because of (1) foreign/alien reason, (2) heavenly blight, (3) compelling power, or (4) surprising accident, the guardian is exempt from the duty of care liability and would not be subject to compensation (Younes 2022).

Theoretically, the Jordanian civil code follows the negligence liability standard (Al-awamleh 2019). Negligence formulates a primary criterion for finding a party liable for a breach (Alshurman and Albnian 2024). Such a sweeping rule results in the cautious approach of firms to conducting business in the marketplace (Al-awamleh 2019; Alshurman and Albnian 2024). A manifestation of such an implication is the private sectors' rush to hire legal services to revamp standard operation procedures after the passage of the recent cybersecurity law (Othman et al. 2025). Similarly, consumers have more confidence in sharing information, knowing that breaches lead to real repercussions such as monetary compensation in liability cases (Alshurman and Albnian 2024).

Strict liability rules have no presence in the Jordanian civil code (Owaidi and Mahafzah 2011). Remedies and defenses exist to escape liability charges. Defendants must furnish adequate evidence showcasing harm resulting from negligence or intentional breaches (A. Z. Hayajneh 2012). Strict liability rules add further rigid layers to the marketplace, increasing transactional costs and legal fees (A. Z. Hayajneh 2012). Additionally, consumer

protection under strict liability rules have dwindled because individuals understand that liability is only established under strict criteria.

The novel Jordanian personal data protection law represents the administrative and regulatory approach for addressing liability in cybersecurity settings. Such an approach is consistent with the global trend of protecting consumer information under comprehensive legal vehicles, such as the European General Data Protection Regulation (GDPR). While negligence and harm remain the central components of liability law under the new tool, strict liability options are also afforded in the protection law. Thus, the Jordanian civil code utilizes an amalgamation of negligence, strict liability and comprehensive regulatory liability doctrines.

4. Liability and the Jordanian Personal Data Protection Law

In 2023, the Jordanian legislature passed the Personal Data Protection law (No. 24) providing another layer of safety to cybersecurity infrastructures. Article 8 (a) of the law requires entities to take all necessary measures to protect users' data. By the same token, Article 8 (b) mandates data controllers (firms or institutions) to exercise technical, organizational and physical protective procedures to ensure the safety of the data. The law also requires the explicit consent of users when obtaining, transferring or modifying their data. More importantly, Article 20 (b) holds data controllers liable for compensatory damages if gross negligence or misconduct occur in data breach incidents. Table 2 presents the exact language of the referenced articles above.

Strict liability rules have no presence in the Jordanian civil code. Remedies and defenses exist to escape liability charges. Defendants must furnish adequate evidence showcasing harm resulting from negligence or intentional breaches. Strict liability rules add further rigid layers to the marketplace, increasing transactional costs and legal fees. Additionally, consumer protection under strict liability rules have dwindled because individuals understand that liability is only established under strict criteria.

Table 2. Personal Data Protection Law No. (24) of 2023.

Article Number	Article Text
Article 8 (a)	The Controller shall adhere to the following obligations: Taking necessary measures to protect the Data under its custody and any Data received from any other person.
Article 8 (b)	The Controller shall adhere to the following obligations: Implementing security, technical, and organisational measures that ensure the protection of Data against any breaches, unauthorized disclosure, alteration, addition, destruction, or Processing, as directed by the Council in instructions issued for this purpose.
Article 20 (B)	In case of gross negligence or misconduct, the responsible Controller shall be liable to compensate the affected Data Subject.

The new Jordanian law protects two types of information: personal and sensitive data. Personal data covers direct or indirect information or combination of facts that identifies a person. Such information may include names, ages, sex, or any background facts about the person. The law specifically protects sensitive data understood as any type of information that could cause potential harm to individuals if exposed. Such information covers racial, financial, education, ethnic, political, social or religious backgrounds (Abduljaber et al. 2025; Onder 2023). The law also leaves the determination of information, such as genetic or biometric data, as sensitive to the discretion of the commission responsible for the enforcement of the law.

Article 4 of the law provides a list of rights to citizens with respect to personal data. First, direct consent is required from the individual to obtain, process or modify personal data. The law gives the individual the rights to access personal data, modify information, withdraw the authorization to use the data from organizations, specify data processing domains, and hide information, as long as such actions are compliant with other laws. Most importantly, the law requires organizations to inform citizens in case of data breaches. The regulation awards individuals the right to contest undesirable data processing activities and the right to know and modify the transfer of personal data. The law also requires organizations or individuals obtaining personal data to secure prior consent. Consent must be written in clear, easy to understand language and must specify the purposes of personal data requests or uses and the duration of possession.

The law also provides several exemptions regarding data obtainment and processing. Article 6 of the law exempts public agencies from consent when processing information. Further, healthcare providers are exempt from obtaining consent when providing preventive care requiring the request or processing of personal data. Organizations or agencies working with the Central Bank and conducting business requiring personal data processing are exempt from consent requirements as long as they comply with other laws governing the Central Bank and its third-party institutions. Consent is also waived in crime prevention activities or the provision of safety and security to the individual. Additionally, consent is not required in cases of research and historical surveys, as long as actions against people will not be taken. Likewise, statistical surveys or national security needs justify the waiver of consent. The most important part of Article 6 is that, once individuals make their personal data on the web public, consent is not required.

5. Liability Claims, Defenses, and Remedies in Jordanian Civil Law

5.1. Jordanian Supreme Court Precedents

One of the common claims plaintiffs could argue about is the potential harm caused by information exposures or leaks on the internet or to third parties (Al-Hunaiti 2018). Healthcare facilities may suffer from phishing attacks, resulting in patients' usernames, passwords, national identification numbers, health information and personal identifiable data being leaked to unauthorized users. Some patients could argue that such exposure will harm them in the future, and that such harm is caused by the providers' failure to secure its networks or systems. Harm could be in the form of insurance denial or social exclusion based on health history (Al-Nsour 2024). While evidence from Jordan has not surfaced with such arguments in civil courts, such cases have occurred elsewhere around the world. In 2025, the Illinois Supreme Court (i.e., Petta v. Christie Business Holding Company 2025) ruled that theoretical or conceptual future harm does not amount to compensation because actual harm has not occurred (Noonan 2025). Under the Jordanian Civil Code, article 256 clearly states that the presence of harm is necessary for damages to be assessed because of due diligence or duty of care failure (Khawaldeh 2024).

Plaintiffs may recover some of the damages addressing potential risks associated with information leaks or data breaches (Mohammed 2022). While actual harm may not have materialized directly because of data breaches, subsidiary harm manifested in the containment of risks qualifies as grounds for compensatory damages (Shandilya et al. 2024). For instance, if some patients spend time and money monitoring and erasing the leaked information, such expenses may be taken as applicable damage. Notwithstanding the emerging nature of data breach litigation in Jordanian courts, the civil code affords defendants remedies if some type of harm, like cost and time, is suffered because of information leaks under the personal data protection law, as well as tort liability rules (A. Hayajneh 2011). Courts in the United States within California and Alabama have awarded

compensation to consumers who spent money and time fending off risks associated with data breaches and information leaks (Nahra et al. 2025).

Negligence constitutes another common argument plaintiffs may use to seek damages in data breach cases. One of the difficulties plaintiffs face is in furnishing convincing evidence establishing negligence. The use of expert witnesses is a common practice in cybersecurity cases, assisting courts determine the facts and the technical environment involved in the case. In many data breach cases, judges have awarded damages to plaintiffs for varied harm experienced from data breaches caused by negligence (Kornas 2021). In a case from the United States, a court ruled that leaking consumers information to the dark web, including financial records like credit card information, constituted present harm (Kardell 2025). Additionally, the court ruled that the failure of organizations to take the necessary precautions protecting sensitive data leading to high-risk exposures and actual harm provides grounds for negligence, and therefore remedies for damage. Under the Jordanian Civil Code, negligence qualifies as a basis for establishing tort liability under rule 256, as well as the personal data protection law (Al-Amawi 2023).

Privacy invasions or web tracking are increasingly used by plaintiffs as grounds for compensatory damages in data breach claims (Romanosky et al. 2014). Courts, however, are unlikely to find liability, simply because privacy or tracking have been compromised in a specific instance (Romanosky et al. 2014). Like many countries, including the United States, Jordanian law requires the cause and effect (standing) principle leading to observed harm (Melfi Alqudah 2024). Many judges in the US have been unwilling to entertain privacy invasion arguments, exposing people to theoretical future misuse (Abril and del Riego 2021). In Jordanian courts, contractual or tort liability demands the presence of harm, and the temporal connectedness of such harm to negligence or misuse (Al-Amawi 2023). Thus, plaintiffs would need to furnish explicit particularized evidence demonstrating actual damages linked to web tracking to satisfy the standing (injury) requirement under the civilian code (Morrisey et al. 2025).

5.2. Liability Remedies in Jordanian Law

Article 266 of the Jordanian Civil law provides the overarching rule to courts in determining remedies in cases of liability. The law states "the guarantee (compensation) is assessed in all conditions commensurate to the harm experienced by the defendant or reasonable to the potential gains missed under the condition that the harm rose as a natural action because of the harmful act" (Khawaldeh 2024). Compensation under such a rule could be symbolic or material. Defendants are asked to comply with contractual obligations in question thereby providing the plaintiff with the original agreement execution. Material compensation occurs in cases where harm led to states or conditions that cannot be restored to their original or authentic states. Monetary value could be assessed as a mitigation measure to the individual who experienced the harm. Oftentimes, judges rule in favor of a single payment in such cases, however, judges could also mandate defendants to furnish payments over a certain period of time or in extreme cases for life.

5.3. Applicable Liability Precedents in the Jordanian Supreme Court

Notwithstanding the recent emergence of liability in cybersecurity or data breach laws in the Jordanian Court of Cassation that have provided several precedents setting the stage for liability claims involving data breaches. In 2021, the court ruled in favor of a police officer claiming disability damages because of an injury incurred during a gunnery routine training that failed to provide necessary protective equipment (Mansour 2021). The officer practiced without wearing proper ear covers causing partial damage to his hearing. The court reversed an appellate court decision, finding no liability based

on negligence. The Supreme Court held that "necessary protection must be taken by responsible individuals operating physical or mechanical equipment." Such a rule provides clear guidance that operators of networks and systems must take all precautionary measures protecting sensitive data from potential exposure that leads to injury (Mansour 2021).

In a separate decision in 2021, Jordanian justices held the military responsible for damages resulting from landmine accidents. In decision 4631, the court reversed an appellate decision absolving the military from liability in a landmine accidents case. The Supreme Court of Jordan suggested that the military is the guardian against landmines, and it is thus required to take proactive steps in safeguarding human life and property. Failure to take responsibility violated Article 291, requiring special care of mechanical equipment or anything worthy of particular care, like landmines. Thus, the Arab Legion (Jordanian Army) was responsible for damages and held liable in the concerned case. Based on such precedents, firms and organizations are expected to be proactive in protecting sensitive and personal data from unlawful or unauthorized exposures causing harm to individuals (Mansour 2021). More specifically, data handling falls under Article 291, which requires any institution to exercise special care over all actions involving personal or sensitive data.

The Jordanian Supreme Court has activated the heavenly plague doctrine enshrined in Article 261 of the civilian code in liability cases. In decision 4286 of 2021, the Court denied damages requested by the plaintiff as a result of inclement weather in 2013. The defendant argued that the basement damaged by flooding resulted from the heavy rain in northern Jordan. After careful review of expert witness reports, the Supreme Court ruled that foreign causes outside of the control of caregivers over the property do not warrant contractual nor tort liability (Mansour 2021). The residence damage was a direct impact of the weather, which is beyond the purview of the landlord, therefore no liability is applicable. Based on such ruling, data breaches caused by natural disasters or heavenly plague or blight do not incur liability costs on defendants.

6. Discussion

Amidst the absence of legal tests or doctrines determining the limits of organizational reasonable duty of care in preventing cyberattacks, the adoption of static and dynamic security regimes enhances defendants claims in case of litigation. Static regimes refer to the collection of objective measures an organization takes to protect its systems. Examples of objective procedures include regular vulnerability assessments, risk analyses or engagement in bounty protection endeavors. Static steps follow the best practices recommended to solidify systems against cyberattacks. In addition to objective efforts in securing systems, organizations also need to apply subjective dynamic measures appropriate to their systems or industries. Proactive endeavors to test the specific technology or platforms used against cyberattacks demonstrate commitment to the protection of personal data (Tschider 2022). Courts may also use the static and dynamic model in guiding their determination of whether the organization exercised due diligence or not.

One of the broad contemporary debates in cybersecurity liability legal research and practice is the enforcement of strict liability or negligence-based rules. The Jordanian civil code has traditionally applied strict liability in cases of harm with narrow exemptions. Courts are expected to continue implementing the strict liability standard in cybersecurity claims in the near future. The strict liability approach shifts responsibility to organizations and firms rather than individuals. Negligence liability rules offer the private sector more protection against data breaches claims and include rules such as "the intent standard" (Gardner 2024). The implementation of strict liability is likely to generate more private sector investments in cybersecurity to avoid potential liability, adding more protection to citizens' personal and sensitive data (Bhatti 2024; Novelli et al. 2024).

Unlike common law courts, Jordanian judges are less likely to entertain the reasonableness standard in cases involving liability leading to actual injury. The civil code clearly states that machines are under the purview of operators and that the harm produced is the strict responsibility of the operator unless the cause is heavy or induced by foreign powers. Therefore, reasonable tests are unlikely to stand as defenses against liability claims featuring injury. Such a system leads to preventive cybersecurity practices. Firms are more likely to invest in robust technology and update the networks used to house and process data. Thus, a number of legal experts in Jordan celebrated the new data protection legislation as a major milestone in curbing illegal data transfers and undesirable marketing behavior within the Jordanian Kingdom (Atlas Team 2024).

Courts may measure injury in a variety of ways without solely relying on diagnoses. Judges may infer harm from the different testimonies provided in a case. Further, plaintiffs may furnish courts with a plethora of circumstantial evidence in support of harm. Expert opinions also provide a supportive method of assessing the duration, strength, and intensity of an injury. Jordanian courts prefer observational measurement through assessing the limits plaintiffs have at the time of the case.

Privacy harms have emerged as hindrances to legislatures and courts in establishing consistent regulation and application of cybersecurity law (Solove 2021). Courts demand the establishment of harm to grant compensation to plaintiffs (Citron and Solove 2022). Establishing harm is the key issue in such lawsuits (Cofone and Robertson 2017). In the US, plaintiffs must furnish convincing evidence demonstrating tangible harm to gain standing and credibility (Cofone and Robertson 2017). Similarly, compensatory damages in Jordan are only ruled when real harm exists (Alshurman and Albnian 2024). Judges tend to dismiss many cases because the establishment of harm is weak or unconvincing, leading to loss of confidence in the law (Citron and Solove 2022; Solove 2021). Jordanian courts, however, tend to place more significance on negligence than other systems as due diligence and the duty of care are parts of the harm rules in the civilian codes (Alshurman and Albnian 2024). Therefore, in many cases, judges have held public agencies responsible for paying damages to plaintiffs because of duty of care failures leading to harm. Thus, it appears to be easier to establish harm in Jordanian courts compared with American courts. Nevertheless, because of the nascent nature of the cybersecurity law, it is still early to determine whether such a trend holds or not.

6.1. Recommendations

The novelty of personal data protection regulation in Jordan leads to potentially fierce legal battles in courts concerning liability in data breaches. Attorneys, judges, and regulators need to consider several key aspects in cases claiming liability prior to making crucial decisions regarding the matter concerned. First, clear criteria for negligence needs to be defined if applicable in a liability case. Did the company fail to address or patch security vulnerabilities leading to cyberattacks? Does the defendant have strong access controls? Did the company practice acceptable encryption standards? Beyond obvious negligence criteria, parties to liability cases need to consider whether the company or service provider followed industry standards to secure its networks and systems. Here, regulators are urged to work with various sectors to publish clear standards on how to best comply with personal data security to minimize risk.

Regulators are urged to furnish detailed documents guiding service providers on how to best comply with the Personal Data Protection Law. For instance, many articles of the law require companies to comply with necessary procedures shielding personal data from all types of compromise. However, many small to medium-sized companies in Jordan lack the resources or expertise to properly understand or practice such rules. Thus,

the government is urged to develop detailed guidance on how companies could exercise systems or network testing, prepare incident reports and administer security training programs. Most importantly, regulators could develop voluntary programs for service providers to learn the aforementioned practices in collaboration with experts in the private sector. Such an endeavor creates a culture of data security in the marketplace protecting against data breaches.

Citizens' awareness of the developing laws and guidance on personal data protection is a key endeavor Jordanian policymakers need to consider. Given the novelty of personal data protection laws, citizens are still grappling with the basic understanding of their rights. Most importantly, the government is recommended to develop awareness workshops not only to explain the new law, but also to demonstrate potential legal remedies through liability rules in courts. Historically, Jordanian citizens have fallen victims to irresponsible advertisement companies that have exchanged personal data on a massive level, leading to a real solicitation problem in the marketplace. Prior to the passage of the law, Jordanians used to receive a barrage of undesirable texts or calls marketing a variety of services. Companies traded personal data without strict guidance. The new law has resulted in an immediate decrease in unsolicited marketing schemes. Notwithstanding the immediate impact of the legislation, citizens still do not know about their potential rights to seek damages based on liability claims for violations of the new law. Policymakers recommend partners with financial, educational and health institutions to start awareness campaigns informing citizens about the law and their litigation rights (Abduljaber 2017, 2018).

6.2. Implications

A probable implication arising from liability claims from data breaches is the development of consulting firms specializing in legal and technical services helping clients avoid fatal negligence in securing sensitive information. Market trends in North America and Western Europe note the proliferation of cybersecurity firms offering vulnerability assessments featuring legal evaluations of organizational procedures and systems (McCann 2024). Oftentimes, the assessments generate detailed reports, resulting in systems and infrastructure updates signaling the exercise of due diligence in protecting clients' information (Abduljaber and Onder 2024; Onder 2021, 2022). A potential growth of similar organizations is expected to occur in Jordan in the near future (Cherian 2024). The data protection law is fairly recent, and cases have started to appear in lower court trials. Thus, the number of attorneys, firms and organizations offering cybersecurity services is expected to rise in the next decade within the country.

Another important implication concerning liability and data protection in Jordan is the government's proactive role in furnishing further guidance on the implementation of the new data protection law (Saqqaf et al. 2024). Advocacy groups and large businesses around the country have already formally requested clear processes and standards on how to comply with certain elements of the law, such as the items measuring how firms should "transform" or "process" data. Relatedly, the government is expected to equip the data protection commission responsible by enforcing the law with sufficient resources to assist in boosting cybersecurity. Similarly, the judicial branch of the government is expected to offer training to judges on cybersecurity, data breaches, and how liability manifests in such cases (Yahia and Heldt 2023). All such developments are parts of the new legislation on personal data protection in Jordan.

The most important implication of the new personal data protection law and the codification of liability in the legislation is the decrease in marketing calls citizens receive daily. One of the chief motivators giving rise to data protection regulation in the country is the high number of marketing calls people receive every day. On some occasions, citizens

received more than 10 calls advertising similar services, like the purchase of American Visas (Jordan Times 2022). The new law prohibits marketing agencies from selling personal information without the consent of users. Thus, the marketing sector will be negatively impacted by the new rules. Relatedly, liability claims are expected to rise because of potential violations of marketers to the data protection law. Judges and justices in Jordanian courts are, therefore, expected to rule in such claims offering clearer interpretations and future guidance of liability in information leaks cases.

7. Conclusions

The present analysis investigates liability in data breach incidents using the Jordanian civil code as an illustrative legal framework. The number of data breaches have exponentially increased in the past few years, resulting in a dramatic rise of legal battles seeking to establish liability to afford remedies for affected plaintiffs. Broadly speaking, companies and institutions could be held liable for failing to comply with contracts signed with consumers or for committing harm that intensively or inadvertently causes injury to individuals because of information exposure. The Jordanian code, however, offers defendants a few legal defenses against liability, such as harm caused by natural disasters, heavenly blight or plague, or something beyond the control of organizations or their personnel responsible for the protection of individuals' sensitive or personal data.

Data breaches are expected to rise in the future. Technological development in cybersecurity lags the evolving knowledge and practice, causing information leaks. Thus, courts, companies, and affected individuals are likely to hear more liability cases in the coming years. While Jordan has made commendable progress toward the regulation of personal data use, lower courts and the appellate court have yet to grapple with liability cases involving actual harm caused by data breaches in the country. Much of the liability precedents set by the Supreme Court originate from causes of physical harm such as landmines, heavy rain, or gunnery training grounds injuries. While the court established clear guidelines on establishing liability in cases where due diligence is limited or responsibility is evaded, judges and justices are likely to debate the facts of the new cases arising from data breaches. Such a scenario is likely given the absence of courts' interpretations of the new personal data protection law.

Liability rules in the Jordanian code allow individuals to litigate in courts based on harm causing an injury. Individuals, therefore, could sue the company that leaked the information, other individuals who used the information resulting in harm, and any third parties throughout the data processing chain that caused the incident leading to the injury. The Jordanian code does not afford defendants immunities or reservations in cases involving injury resulting from due diligence or caretaking failures. Rule 261 of the code specifies the few exemptions, which include natural disasters or foreign causes like wars or countrywide blackouts. Liability is a serious concern in the Jordanian marketplace, leading organizations and firms to update their systems, network security, vulnerability testing, access controls, authentication procedures, and cloud protection.

Uncertainty concerning the enforcement of the personal data protection law is prevalent among individuals and firms in Jordan. The government is expected to publish guided documents informing people and institutions on how to comply with the legislation. For instance, the law specifically awards individuals the right to seek damages, yet it does not inform them how to proceed with the claims. Further, institutions are expected to implement Article 4 protections on personal data, but they are not informed about any potential defenses. Liability rules in Jordan are flexible, which could result in an influx of new cases claiming remedies because of personal data protection law violations. All such observations add a modicum of confusion to stakeholders in the judiciary and the market-

place, requiring more guidance to be furnished by the commission that the government commanded to enforce the law.

Unlike other countries that have not passed comprehensive data protection laws, Jordan has regulated data breach responsibility under the new bill of the personal data protection law. The articles of the legislation allow individuals to seek monetary compensation as damage relief for injuries causing harm that are associated with information leaks. The Jordanian Supreme Court, in more than a single case on liability, has reversed appellate decisions to establish liability because of a defendant's failure to take precautionary measures to prevent the harm that caused the injury in question. The court did not shy away from placing responsibility and making a case for liability, with the country's public safety and armed forces divisions sending a chilling message that anyone would be held liable if they caused harm through internal failure. Thus, failing to properly protect networks, systems and digital infrastructure causing data breaches would stand as a proper legal argument for plaintiffs in Jordanian courts as a claim for liability. Firms cannot hide behind the reasonable and appropriate standard of establishing due diligence in liability contestations in Jordan. The Supreme Court of the country has demanded proactive endeavors for caretakers of special systems to avoid harm, thus requiring organizations dealing with data to take on a more aggressive role in preventing leaks.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The author declares no conflict of interest.

References

Abduljaber, Malek. 2017. *The Dimensionality of Political Ideology in the Arab World Comparing the Structure of Political Attitudes on Political Parties' and Mass Publics' Levels in Algeria, Egypt, Jordan, and Morocco*. Detroit: Wayne State University.

Abduljaber, Malek. 2018. The determinants of political cleavages in Jordan, Tunisia, and Yemen: An analysis of political attitudes structure in the Arab World. *Digest of Middle East Studies* 27: 97–120. [CrossRef]

Abduljaber, Malek, Mehmet Onder, and Retaj Aljadaan. 2025. Perceptions of democracy within the Middle East and North Africa. *Journal of International Studies* 18: 60–80. [CrossRef]

Abduljaber, Malek F., and Murat Onder. 2024. When we can't see the wood for the trees: The lurking effect of sustainability on corruption. *Cogent Social Sciences* 10: 2318859. [CrossRef]

Abril, Patricia Sánchez, and Alissa del Riego. 2021. Judging Offensiveness: A Rubric for Privacy Torts. *North Carolina Law Review* 100: 1557.

Adar, Yehuda, and Ronen Perry. 2022. Negligence without harm. *Georgetown Law Journal* 111: 187. [CrossRef]

Alabady, Hasan S. 2023. Towards a legal framework for civil liability of smart robots in Jordanian legislation. *International Journal of Cyber Criminology* 17: 23–39.

Al-Amawi, Mohammed. 2023. The legal basis for guaranteeing the wrongful act on funds in the Jordanian Civil Law. *Russian Law Journal* 11: 1269–78.

Al-awamleh, Atef Salem. 2019. The provisions of supervisor responsibility in the Jordanian civil code. *Journal of Law, Policy and Globalization* 86: 100.

Albnian, Ahmad Awwad, and Sara Nabeal Algaber. 2025. Basis of Tort Liability Arising from Artificial Intelligence Technologies in Jordanian Legislation. In *From Machine Learning to Artificial Intelligence: The Modern Machine Intelligence Approach for Financial and Economic Inclusion*. Cham: Springer, pp. 1433–42.

Al-Hunaiti, Mamoun. 2018. The Liability of the Witness for His Wrongful Action under the Jordanian Civil Law. *Journal of Politics and Law* 11: 111. [CrossRef]

Al-Kasassbeh, Fahad Yousef, Ali Mohammad Abu Ghazleh, Ma'moon juma'h M. Kareem, and Dr manal Omar breizat. 2023. International and National Efforts to Protect Cyber Security: Jordan Case Study. *International Journal of Cyber Criminology* 17: 350–63.

Almugamisi, Haifa. 2025. Multiple Perspectives of Data Breaches in Higher Education Institutions (HEI): A Case of Universities in Saudi Arabia. Doctoral dissertation, UCL (University College London), London, UK.

Al-Nsour, Hazem Ali. 2024. The Impact of the Medical and Health Liability Law under Jordanian Legislation. *Pakistan Journal of Criminology* 16. [CrossRef]

Al-Sarayreh, Riyad Mahmoud. 2024. Jordanian Cybercrime Law No. (17) of 2023 between Regulating Social Media Sites and Restricting Freedom of Opinion. *Scholars International Journal of Law, Crime and Justice* 7: 339–51. [CrossRef]

Alsharu, Ahmad Ibrahim, Tasnim Fakri Aldowery, and Nidaa Kadhim Mohammed Jawad. 2024. Jordanian Legal Provisions for Electronic Commerce: Consumer Protection Perspectives-A Comparative Study. *Beijing Law Review* 15: 444. [CrossRef]

Alshible, Mohammad, and Hamzeh Abu Issa. 2025. Criminal protection to the digital right to be forgotten in Jordan. *International Journal of Electronic Security and Digital Forensics* 17: 295–306. [CrossRef]

Al-Shibli, Farouq Saber, Mohamad Alkhalaileh, and Nathan J. Brown. 2023. Judicial Review and the Jordanian Constitutional Court: False Start or Slow Start? *Arab Law Quarterly* 39: 611–28. [CrossRef]

Alshurman, Sohib, and Ahmad Albnian. 2024. Compensation for Missed Opportunity within the Scope of Contractual Liability in Jordanian Legislation: A Comparative Study. *Pakistan Journal of Criminology* 16: 719–32. [CrossRef]

Andress, Jason. 2014. *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*. Rockland: Syngress.

Atlas Team. 2024. Understanding Data Protection and Privacy Laws in Jordan. Atlas. Available online: https://www.atlashxm.com/resources/understanding-data-protection-and-privacy-laws-in-jordan (accessed on 20 June 2024).

Bhattarai, Keshav, and Mahmoud Yousef. 2025. Colonial past and current ruling systems. In *The Middle East: Past, Present, and Future*. Cham: Springer, pp. 83–103.

Bhatti, Rafae. 2024. SEC Cybersecurity Rules: Navigating Cyber Risk and Liabilities. *TortSource* 26. Available online: https://www.americanbar.org/groups/tort_trial_insurance_practice/resources/tortsource/2024-spring/sec-cybersecurity-rules-navigating-cyber-risk-liabilities/ (accessed on 13 March 2026).

Bilge, Leyla, and Tudor Dumitraş. 2012. Before we knew it: An empirical study of zero-day attacks in the real world. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*. New York: Association for Computing Machinery, pp. 833–44.

Cherian, Sanjiv. 2024. Cybersecurity Companies in Jordan. Microminder Cyber Security. Available online: https://www.micromindercs.com/blog/cybersecurity-companies-in-jordan (accessed on 23 December 2024).

Citron, Daniel Keats, and Daniel J. Solove. 2022. Privacy harms. *Boston University Law Review* 102: 793. [CrossRef]

Cofone, Ignacio N., and Adriana Z. Robertson. 2017. Privacy harms. *Hastings LJ* 69: 1039.

Fakhouri, Hussam N., Sadi Alawadi, Feras M. Awaysheh, Faten Hamad, Sawsan Alzubi, and Mohammad Naser AlAdwan. 2023. An Overview of using of Artificial Intelligence in Enhancing Security and Privacy in Mobile Social Networks. In *2023 Eighth International Conference on Fog and Mobile Edge Computing (FMEC)*. New York: IEEE, pp. 42–51.

Firch, Jason. 2025. The Average Cost of Ransomware Attacks. PurpleSec. Available online: https://purplesec.us/learn/average-cost-of-ransomware-attacks/ (accessed on 24 May 2025).

Gardner, Angel R. 2024. Who Should be Liable? Examining the Corporate Liability Regime for Cybersecurity Risks. *Student Journal of Information Privacy Law* 2: 4.

Hadnagy, Christopher. 2014. *Social Engineering: The Science of Human Hacking*. Hoboken: Wiley.

Hayajneh, Abdelnaser. 2011. Vanishing Borders: Can Human Rights be a subject of Private Law? Exploring Human Rights under Jordanian Civil Law. *European Journal of Social Sciences* 23: 277–87.

Hayajneh, Abdelnaser Zeyad. 2012. Legal surgery: The need to review jordanian civil law. *British Journal of Humanities and Social Sciences* 6: 45–53.

IBM Security. 2024. Cost of a Data Breach Report 2024. Available online: https://www.ibm.com/reports/data-breach?utm_source=chatgpt.com (accessed on 5 November 2025).

Jordan Times. 2022. Jordanians Complain of Scam Calls Promising US Visa, Green Card. *The Jordan Times*, December 31. Available online: https://jordantimes.com/news/local/jordanians-complain-scam-calls-promising-us-visa-green-card (accessed on 31 December 2022).

Karasik, Alex, and Duane Morris. n.d. A Dive into Data Breach Class Action Risk. GRC Outlook. Available online: https://grcoutlook.com/a-dive-into-data-breach-class-action-risk/ (accessed on 21 May 2025).

Kardell, Robert L. 2025. An Update on Standing in Data Breach Class Actions. BairdHolm. Available online: https://www.bairdholm.com/blog/an-update-on-standing-in-data-breach-class-actions/ (accessed on 21 February 2025).

Khawaldeh, Ahmed M. 2024. Generative AI Hallucinations and Legal Liability in Jordanian Civil Courts: Promoting the Responsible Use of Conversational Chat Bots. *International Journal for the Semiotics of Law-Revue Internationale de Sémiotique Juridique* 38: 381–401. [CrossRef]

Kornas, Lukasz. 2021. Malicious v. Negligent Loss of Data: The Second Circuit's Questionable Test to Determine Data Breach Standing. *UIC Review of Intellectual Property Law* 21: 3.

Mansour, Ahmad. 2021. Civil Liability for Objects and Machines in Jordanian Law. Jordan Lawyer. Available online: https://jordan-lawyer.com/2021/12/29/civil-liability-for-objects-and-machines/ (accessed on 19 December 2021).

McCann, Kristian. 2024. Top 10 Largest Cybersecurity Companies. *Cyber Magazine*, November 13. Available online: https://cybermagazine.com/articles/top-10-largest-cybersecurity-companies (accessed on 13 November 2024).

Melfi Alqudah, M. Mohammad. 2024. Civil Legal Framework for Moral Damage in Jordanian Law. *Pakistan Journal of Criminology* 16: 317–31. [CrossRef]

Mohammed, Zareef. 2022. Data breach recovery areas: An exploration of organization's recovery strategies for surviving data breaches. *Organizational Cybersecurity Journal: Practice, Process and People* 2: 41–59. [CrossRef]

Morris, Duane. 2024. Data Breach Class Action Review—2024. Lexology. Available online: https://www.lexology.com/library/detail.aspx?g=86d1feb5-be78-473a-b434-bcee3d27cba4 (accessed on 23 August 2024).

Morris, Duane. 2025. Duane Morris LLP Publishes Its Data Breach Class Action Review—2025. DuaneMorris. Available online: https://www.duanemorris.com/pressreleases/duane_morris_llp_publishes_its_data_breach_class_action_review_2025_0225.html (accessed on 11 February 2025).

Morrisey, Matthew M., Andy Taylor, and Charles E. Westerhaus. 2025. Courts Reject Theoretical Privacy Violations Due to Lack of Standing. *FaegreDrinker*, April 21. Available online: https://www.faegredrinker.com/en/insights/publications/2025/4/courts-reject-theoretical-privacy-violations-due-to-lack-of-standing (accessed on 21 April 2025).

Nahra, Kirk J., and Ali A. Jessani. 2024. Year in Review: Top 2023 Data Breach Litigation Trends. *WilmerHale*, March 15. Available online: https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20240315-year-in-review-top-2023-data-breach-litigation-trends (accessed on 15 March 2024).

Nahra, Kirk J., Molly Jennings, Rachel Grenne, and Ali A. Jessani. 2025. 2024 Year in Review: Data Breach Litigation. *WilmerHale*, April 9. Available online: https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20250409-2024-year-in-review-data-breach-litigation (accessed on 9 April 2025).

Nazish, and M. Manzoor. 2024. The Evolving Legal Landscape of Cybersecurity Law. *Law Research Journal* 2: 36–43.

Noonan, James. 2025. Illinois Supreme Court Holds There Is No Standing to Sue for a Data Breach Where Victim Did Not Suffer a Concrete Injury. Noonan & Lieberman. Available online: https://www.noonanandlieberman.com/updates/illinois-supreme-court-holds-there-is-no-standing-to-sue-for-a-data-breach-where-victim-did-not-suffer-a-concrete-injury/ (accessed on 21 May 2025).

Novelli, Claudio, Federico Casolari, Philipp Hacker, Giorgio Spedicato, and Luciano Floridi. 2024. Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity. *Computer Law & Security Review* 55: 106066. [CrossRef]

Onder, Mehmet. 2019. Regime type, issue type and economic sanctions: The role of domestic players. *Economies* 8: 2. [CrossRef]

Onder, Mehmet. 2021. Economic sanctions outcomes: An information-driven explanation. *Journal of International Studies* 14: 38–57. [CrossRef]

Onder, Mehmet. 2022. Consequences of economic sanctions on minority groups in the sanctioned states. *Digest of Middle East Studies* 31: 201–27. [CrossRef]

Onder, Mehmet. 2023. Overview of secondary sanctions: Turkey under the ghost of western economic sanctions. In *The Routledge Handbook of the Political Economy of Sanctions*. London: Routledge, pp. 260–73.

Othman, Srbaz Nidham, Aqeel Mahmood Jawad, Raed Hameed, Raad Tomaa Kawad, and Dmytro Khlaponin. 2025. The impact of cybersecurity law in the middle east. *Encuentros: Revista de Ciencias Humanas, Teoría Social y Pensamiento Crítico* 23: 392–420.

Owaidi, Ahmad A., and Qais A. Mahafzah. 2011. The Surety's Right in Canceling the Suretyship under Jordan Civil Code. *European Journal of Social Sciences* 20: 499–512.

Perlroth, Nicole. 2012. Lax Security at LinkedIn Is Laid Bare. *The New York Times*, June 10. Available online: https://www.nytimes.com/2012/06/11/technology/linkedin-breach-exposes-light-security-even-at-data-companies.html (accessed on 13 March 2026).

Petta v. Christie Business Holding Company. 2025. Illinois Supreme Court 130337. Available online: https://law.justia.com/cases/illinois/supreme-court/2025/130337.html (accessed on 21 May 2025).

Pfleeger, Charles P., Shari Pfleeger, and Jonathan Margulies. 2015. *Security in Computing*, 5th ed. Westford: Prentice Hall.

Redding, Gordon. 2005. The thick description and comparison of societal systems of capitalism. *Journal of International Business Studies* 36: 123–55. [CrossRef]

Romanosky, Sasha, David Hoffman, and Alessandro Acquisti. 2014. Empirical analysis of data breach litigation. *Journal of Empirical Legal Studies* 11: 74–104. [CrossRef]

Saqqaf, Khaled, Dana Abduljaleel, and Hakam Al Shawwa. 2024. Data Protection in Jordan: An Overview of the Current and Future Framework. Al Tamimi & Co. Available online: https://www.tamimi.com/law-update-articles/data-protection-in-jordan-an-overview-of-the-current-and-future-framework/ (accessed on 21 May 2025).

Schwarcz, Daniel, Josephine Wolff, and Daniel W. Woods. 2022. How privilege undermines cybersecurity. *Harv. JL & Tech.* 36: 421.

Shandilya, Shishir Kumar, Agni Datta, Yash Kartik, and Atulya Nagar. 2024. Achieving Digital Resilience with Cybersecurity. In *Digital Resilience: Navigating Disruption and Safeguarding Data Privacy*. Cham: Springer, pp. 43–123.

Solove, Daniel J. 2021. The myth of the privacy paradox. *The George Washington Law Review* 89: 1–51. [CrossRef]
Stallings, William, and Lawrie Brown. 2015. *Computer Security: Principles and Practice*. London: Pearson.
Studer, Evelyne, and Jacques De Werra. 2017. Regulating Cybersecurity—What Civil Liability in Case of Cyber-Attacks? *Expert Focus* 8: 511–17.
Surfshark. 2024. Global Data Breach Statistics: A 2024 Recap. Available online: https://surfshark.com/research/study/data-breach-recap-2024?srsltid=AfmBOoqKWg27BGfNUsbJPsWSdc_4jOuTv81zKeeC_2L6PFv1Amh7Ad29 (accessed on 21 May 2025).
Teichmann, Fabian Maximilian Johannes, and Chiara Wittmann. 2023. When is a law firm liable for a data breach? An exploration into the legal liability of ransomware and cybersecurity. *Journal of Financial Crime* 30: 1491–98. [CrossRef]
The Open Worldwide Application Security Project. 2023. OWASP API Security Project. Available online: https://owasp.org/www-project-api-security/ (accessed on 21 May 2025).
Tipton, Harold F., and Micki Krause. 2007. *Information Security Management Handbook*. Boca Raton: CRC Press.
Toubat, Hazem Suleiman, Rohizan Halim, and Nabeel Magableh. 2020. The Impact of Technological Development on Legal Rules: A Case Study of Jordan. *Journal of Critical Reviews* 7: 1574–79.
Tschider, Charlotte A. 2022. Locking Down" Reasonable" Cybersecurity Duty. *Yale Law & Policy Review* 41: 75.
Verizon. n.d. 2025 Data Breach Investigations Report. Verizon Business. Available online: https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf (accessed on 21 May 2025).
White, Monica. 2025. Broadcom Named One of America's Best Cybersecurity Companies 2025. *Symantec*, May 21. Available online: https://symantec-enterprise-blogs.security.com (accessed on 21 May 2025).
Whitman, Michael E., and Herbert J. Mattord. 2009. *Principles of Information Security*. Boston: Thomson Course Technology, p. 656.
Yahia, Afnan Abu, and Valeska Heldt. 2023. Jordan's New Cybercrime Law Passes Despite Freedom Concerns. The Tahrir Institute for Middle East Policy. Available online: https://timep.org/2023/10/19/jordans-new-cybercrime-law-passes-despite-freedom-concerns/ (accessed on 19 October 2023).
Younes, Alaa Majed Ahmad Bani. 2022. Responsibility of Objects in Jordanian Civil Law. *Journal of Positive School Psychology* 6: 7991–98.
Ziadeh, Farhat J. 1993. Property rights in the Middle East: From traditional law to modern codes. *Arab Law Quarterly* 8: 3–12. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.