Abu Aloun A, 'Developing civil liability for cyber breaches in Palestine: an analytical study in light of comparative law' (2025) 2 EJPLT.
DOI: https://doi.org/10.57230/EJPLT252AAA

EJPLT
ISSN 2704-8012



Developing civil liability for cyber breaches in Palestine: an analytical study in light of comparative law

Sviluppo della responsabilità civile per le violazioni informatiche in Palestina: uno studio analitico alla luce del diritto comparato

ANAS MOUSA ABU ALOUN
Associate Professor of Civil Law
Arab American University

Abstract

The paper analyses the influence of the Palestinian legal system on the breach of data and cyberattacks. The main problem is the dependence of Palestinian legislation on a statute that was passed during the British Mandate in 1944, which is known as British Civil Wrongs Ordinance. The age of this law makes it inadequate for current technological advancements. The research problem mainly revolved around how to adapt the rules of this obsolete ordinance to modern times. The researcher came to the conclusion that a person who wishes to claim compensation as a result of a cyberattack must establish three parts of liability, namely: a legal duty to protect the concerned personal data existed, that the data protector was negligent which resulted in the harm, and that there was actual harm due to the breach. To come up with a suitable law for Palestine, the researcher made a comparison between the Palestinian and the modern laws like the European General Data Protection Regulation (GDPR) and the UK Data (Use and Access) Act 2025. The researcher noted many differences between these laws and the Palestinian law, which include among others the lack of a clear right to compensation for non-material damage in the Palestinian law as well as the difficulty in assigning liability when several parties are involved and the absence of legal regulation on reasonable security measures that should be in place to prevent such breaches. The study made the argument for the amendment of laws by proposing changes that are in line with the recognized international standards, and offering training to those in the legal field to increase their knowledge of cybersecurity issues and their implications.

© The author(s) 2025, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Abstract
Lo studio affronta la questione di come la legislazione palestinese affronti le violazioni dei dati e gli attacchi informatici. La difficoltà risiede nella dipendenza della legislazione palestinese da una legge emanata durante il Mandato britannico nel 1944 (il British Civil Wrongs Ordinance). L'antichità di questa legge la rende incapace di affrontare gli attuali sviluppi tecnologici. Il principale problema di ricerca era come adattare le regole del British Civil Wrongs Ordinance del 1944, che rimane in vigore in Palestina.
Il ricercatore ha concluso che qualsiasi individuo che intenda presentare una richiesta di risarcimento derivante da attacchi informatici deve dimostrare tre elementi di responsabilità: l'esistenza di un obbligo legale di proteggere i dati personali, la negligenza da parte della persona responsabile della protezione dei dati che ha portato al verificarsi del danno, e il verificarsi del danno come risultato della violazione.
Al fine di sviluppare la legislazione palestinese, il ricercatore ha confrontato la legge palestinese con sistemi avanzati come il Regolamento Generale sulla Protezione dei Dati europeo (GDPR) e il Data (Use and Access) Act 2025 del Regno Unito. Il ricercatore ha riscontrato differenze significative tra queste leggi e la legge palestinese, tra cui l'assenza nella legge palestinese di un diritto chiaro al risarcimento per danni non materiali, la difficoltà nell'attribuire la responsabilità quando sono coinvolti più soggetti, e la mancanza di regolamentazione nella legge palestinese riguardo alle misure di sicurezza ragionevoli che dovrebbero essere adottate per prevenire tali violazioni.
Lo studio ha proposto emendamenti legislativi derivati da standard internazionali riconosciuti, nonché la formazione per coloro che operano nel settore legale al fine di ampliare le conoscenze sulle questioni di cybersecurity e sulle loro implicazioni.

Keywords: Cyber Liability; Civil Wrongs Ordinance; Palestine; Data Protection; Duty of Care; Causality; Comparative Law

Summary: 1. Introduction. – 2. Due Diligence in Cybersecurity under British Law. – 2.1. The Role of the UK GDPR and the Data Protection Act 2018 in the UK in Developing the Concept of Due Diligence. – 2.2. The Civil Wrongs Ordinance and the Draft Data Protection Law of 2025. – 2.3. Special Conditions for Considering an Act a Civil Wrong in the Context of Personal Data Protection. – 3. The Element of Damage in Cyber Liability Cases (From Tangible to Intangible Damages). – 3.1. Material (Tangible) Damage in Cyber Liability Cases. – 3.2. Moral Damage in Cyber Breaches. – 4. Legal Integration Between Articles 60 and 55 bis in Addressing Causality. – 4.1. Article 60 of the Palestinian Civil Wrongs Ordinance Provides a Solid Legal Framework for Linking Compensation to Causality. – 4.2. Enhancing Integration Between Article 60 and Articles 50 and 55 bis. – 5. Conclusion.

1. Introduction.

The rapid digitisation of Palestinian society – from mobile banking and e-government services to online education and health records – has brought

undeniable convenience.[1] Yet it has also made individuals and institutions vulnerable to cyber threats that are unprecedented in their scope and sophistication.[2] When personal information is stolen, money is drained from bank accounts, and intimate photos are shared, it is not a hypothetical problem; it is a living reality for ordinary citizens. The tragedy is that the legal tool most readily available to seek redress – the British Civil Wrongs Ordinance of 1944, as amended in 1947 – was drafted in an era when "data" meant paper files locked in cabinets. The question this study asks is therefore both simple and urgent: can a statute born in the Mandate period still deliver justice in the age of ransomware and state-sponsored hacking?

The answer, as the following pages demonstrate, is that it can – but only with considerable creativity, comparative borrowing, and, ultimately, legislative courage.

This research proceeds by placing the Ordinance in direct conversation with three far more modern frameworks: – the United Kingdom's post-Brexit regime (UK GDPR and Data Protection Act 2018, now being substantially reshaped by the Data (Use and Access) Act 2025 that entered into force on 19 June 2025); – the risk-based U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework; and – the ambitious yet still unfinished Palestinian Draft Data Protection Law of 2025.

The comparison is rather revealing. The law of Palestine uncovers three main weaknesses, namely: first, there is no reliable way for victims to get compensated for non-material damage (psychological distress and loss of privacy which have become the two major claims today); secondly, the situation is unclear when it comes to sharing responsibility of the case when there are many parties involved and all of them have contributed to the violation; thirdly, there are virtually no objective criteria for "reasonable security measures" at all. The absence of these benchmarks marginalizes the victims - either they are individuals or small enterprises - with remedies that seem to exist in theory but are practically impossible to obtain.

Yet the Ordinance is not a dead letter. Articles 50 (negligence), 55 bis (breach of statutory duty), and 60 (assessment of damage) retain remarkable elasticity. When read creatively – and in light of international precedents such as the £20 million British Airways penalty (2020) and the $575 million Equifax settlement (2019) – they can be pressed into service today. The Draft Data Protection Law 2025, once enacted, will supply the missing statutory duties; Article 55 bis can then transform their violation into an actionable civil wrong, bridging an eighty-year gap with surprising elegance.

Therefore, the main question that the research attempts to answer is: Can the rules of the British Civil Wrongs Ordinance frame liability for cyberattacks? What are the obstacles that prevent its application?

These questions will be answered using the analytical and comparative methods, thereby enabling the proposal of amendments to the British Civil

[1] Palestinian Central Bureau of Statistics, 'ICT Survey on Households and Individuals 2024' (Ramallah, PCBS 2025) (showing 87 % smartphone penetration and 72 % use of e-banking services). <https://www.pcbs.gov.ps/PCBS-Metadata-en-v5.2/index.php/catalog/733>

[2] See, eg, Human Rights Watch, '*A Threshold Crossed: Israeli Authorities and the Crimes of Apartheid and Persecution*' (HRW 2021) ch VII (on weaponised data leaks and doxing campaigns).

Wrongs Ordinance in force in Palestine to address cyber liability, and examining the extent to which the Palestinian Data Protection Draft Law provides comprehensive protection against cyberattacks.

2. Due Diligence in Cybersecurity under British Law.

The principle of the "duty of care" is considered the fundamental element in establishing civil liability arising from negligence, particularly in Anglo-Saxon legal systems, of which the British Civil Wrongs Ordinance in force in Palestine forms an integral part, as all its provisions are derived from this system. In light of the complex cyber-attacks, can this principle, as stipulated in the British Civil Wrongs Ordinance in force in Palestine, confront the complexities resulting from these attacks?

This part of the research aims to study this principle according to its modern concept, which has evolved in its original system in the United Kingdom, which has adopted a data protection system for 2018 and the Data (Use and Access) Act 2025. This is what we will address in:

- Section One: The Role of the UK GDPR and the Data Protection Act 2018 in the UK in Developing the Concept of Due Diligence; and
- Section Two: The Civil Wrongs Ordinance and the Draft Data Protection Law of 2025.

2.1. The Role of the UK GDPR and the Data Protection Act 2018 in the UK in Developing the Concept of Due Diligence.

The duty of care is the cornerstone of the tort of negligence. It obliges every person (whether natural or legal) to take reasonable measures to prevent foreseeable harm that may befall others who can reasonably be expected to be affected by their acts or omissions. The contemporary law of negligence has its roots in the leading case of Donoghue v Stevenson.[3] The “Neighbour Principle” formulated by Lord Atkin continues to be the ideological foundation of the duty of care principle., which remains to this day the philosophical and legal bedrock for determining when a duty of care arises. The classic formulation (almost poetic) formulation from Lord Atkin’s judgment: “You must take reasonable care to avoid acts or omissions which you can reasonably foresee would be likely to injure your neighbour. Who, then, in law is my neighbour? The answer is: persons who are so closely and directly affected by my act that I ought reasonably to have them in contemplation as being so affected when I am directing my mind to the acts or omissions which are called in question.” From the above, the duty of care is composed of three essential elements:

Reasonable care What the “reasonable and prudent person” would have done in the same circumstances – neither perfection nor indifference is required.

The neighbour = the reasonably foreseeable victim Any person (physically, functionally, or relationally proximate) whom it is reasonably foreseeable

[3] Donoghue v Stevenson [1932] AC 562 (HL).

would be directly harmed by your act or omission – even if you do not know their name.

Ought to be in your contemplation reasonably You do not have to have personal acquaintance with the particular person; it is enough that a hypotheti-cal person in your place could predict that a person similar to the plaintiff's might be harmed.

In the context of cybersecurity, this principle translates into an obligation for organizations to protect personal data and digital systems from various threats, including:

- Malware: Programs designed to steal data or damage systems, as in the Emotet attack (2020), which targeted banks and government institutions.[4]
- Phishing: Attempts to deceive users via fake emails or websites to obtain sensitive data, such as login credentials.
- Ransomware: Encrypting data and demanding a ransom for its release, as in the NotPetya attack (2017), which caused enormous global losses.[5]
- DDoS attacks: in essence, inundating a system with bogus requests to the point of collapse, similar to the 2016 Dyn attack that caused Twitter and Netflix to be unavailable for hours. The duty of care principle application in the cybersecurity context is reliant on a meticulous risk evaluation that takes into account data sensitivity, threat level, and security measures cost as the main factors.

Sensitive data, such as electronic health data subject to HIPAA or financial data, requires stricter security measures compared to public data like email addresses.[6] The threat level also varies according to the nature of the attacks; targeted attacks (Advanced Persistent Threats) require the use of advanced systems like Intrusion Detection Systems (IDS), while firewalls are sufficient to counter random attacks. [7] At the same time, security measures must be economically feasible, considering the principle of proportionality, as applying Security Information and Event Management (SIEM) systems may be costly for small companies but necessary for large institutions managing sensitive data.[8]

In this context, reasonable security measures that entities responsible for data protection must take to fulfil their duty of care obligations include: Encryption using standards like AES-256 to protect data in transit and at rest, reducing the risk of leakage [9] Multi-Factor Authentication (MFA), which combines passwords, temporary codes, or biometric identifiers to prevent

[4] 'Attack Chain Overview: Emotet in December 2020 and January 2021' (Unit42, Palo Alto Networks, 20 January 2021) <https://unit42.paloaltonetworks.com/attack-chain-overview-emotet-in-december-2020-and-january-2021/> accessed 4 September 2025.

[5] 'NotPetya (2017)' (CCDCOE) <https://cyberlaw.ccdcoe.org/wiki/NotPetya_(2017)> accessed 4 September 2025.

[6] J Kosseff, *Cybersecurity Law* (3rd edn, Wiley 2024) 145–147.

[7] R Ross, *Security and Privacy Controls for Information Systems and Organizations* (NIST Special Publication 800-53 Rev 5, NIST 2020).

[8] B Schneier, *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World* (WW Norton & Company 2018).

[9] A Solow-Niederman, 'Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches' (2018) 127 Yale Law Journal Forum 614.

unauthorised access[10] Security Information and Event Management (SIEM) systems that monitor systems in real-time to detect threats and log incidents to accelerate response; and finally, regular software updates by applying security patches to address vulnerabilities, as was the case with the Log4j vulnerability in 2021 that affected millions of systems.[11] .When you actually implement all of these things properly, they do actually strengthen your defenses against breaches of cyber security, while at the same time helping to ensure that you're discharging your duty of care that goes back to the classic case of Donoghue v Stevenson.[12]

The UK GDPR and similar legal and technical regulatory frameworks have a significant impact on cybersecurity. They impose clear and firm data protection standards rather than mere uncertain promises. These measures have practically compelled the parties involved in data handling to be serious and professional about security, such as using proper encryption, installing strict access controls, and even formulating incident-response plans, among others[13].

That way they cut down the chances of a breach and, more importantly, they can show they're not falling short on the duty of care they owe everyone.[14] If you link liability to actual technical defences like that, the whole thing forces everybody to stop reacting after the mess has happened and start protecting sensitive data properly before the hackers turn up. That's exactly the spirit of negligence law that was started by Donoghue v Stevenson nearly a century ago, and it works beautifully with how we try to run cybersecurity these days.

UK GDPR and Data Protection Act 2018 essentially give us a pretty solid legal backbone that ensures everyone handling personal data steps up their game in terms of their duty of care and throws down some pretty tough regulations in terms of cybersecurity and compliance. Article 32 of the UK GDPR states that:

" 1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a)the pseudonymisation and encryption of personal data;

(b)the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c)the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d)a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from

[10] DJ Solove, PM Schwartz, *Data Protection Law* (2nd edn, Wolters Kluwer 2020).
[11] A Wirth, 'Log Jam: Lessons Learned from the Log4Shell Vulnerability' (2022) 56 Biomedical Instrumentation & Technology 72.
[12] Donoghue (n 1).
[13] N Kshetri, 'The Log4j Vulnerability: Impacts and Lessons for Cybersecurity Governance' (2022) 2 Journal of Cybersecurity and Privacy 123; UK General Data Protection Regulation, art 32.
[14] ibid; P Carey, *Data Protection: A Practical Guide to UK and EU Law* (6th edn, OUP 2022).

accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by".

Furthermore, Article 33 of the UK GDPR sets a rather tight deadline: once a controller becomes aware of a personal data breach that is likely to pose a risk to individuals' rights and freedoms, it must notify the supervisory authority (in the UK, the ICO) within 72 hours. There is very little room for delay.

Article 82 takes this a step further by actually granting data subjects a right to compensation. This includes not only material damage (such as actual monetary losses due to fraud or identity theft) but also non-material damage (such as the distress and anxiety that often accompany a major data leak). This is reinforced by Section 168 of the DPA 2018. The following court rulings are examples of how these guidelines are enforced in practice, focusing specifically on instances where non-compliance with the duty of care has occurred:

ICO v British Airways (2020): The Information Commissioner's Office (ICO) punished British Airways with a fine of £20 million for not having Multi-Factor Authentication (MFA) and for having weak Security Information and Event Management (SIEM) systems. The attack, which was the result of an unpatched vulnerability, led to the breach of personal data of about 400,000 customers, including credit-card information and other highly confidential personal data.[15]

ICO v Marriott International (2020), The ICO imposed an enormous fine of £18.4 million on Marriott for their inefficient network segmentation and lack of monitoring. As a result, a breach that originally took place in Starwood's systems back in 2014 remained undetected until 2018, despite Marriott's acquisition in 2016. During this time, the personal data of about 339 million worldwide guests – names, addresses, passport numbers, etc. – had already been compromised.[16]

Various Claimants v WM Morrison Supermarkets plc [2020] UKSC 12The UK Supreme Court ultimately cleared Morrisons of vicarious liability for a malicious data breach carried out by a disgruntled employee who deliberately posted payroll data online. While the company escaped liability on those facts, the judgment (especially per Lord Reed) underscored how critical it is to keep tight access controls in place. The Court made clear that giving staff broader permissions than they actually need for their jobs can itself amount to organisational negligence – a point that has since become required reading for anyone designing "least-privilege" policies.[17]

TalkTalk Telecom Group (2016), In what was, at the time, the ICO's largest-ever fine under the old Data Protection Act 1998 regime, TalkTalk was penalised £400,000 for a catalogue of basic security failures. Outdated and

[15] *Various Claimants v Wm Morrison Supermarkets plc* [2020] UKSC 12 [2020] AC 989.
[16] *ICO v TalkTalk Telecom Group plc* [2016] (ICO Penalty Notice).
[17] National Cyber Security Centre (NCSC), 'Cyber Essentials: Requirements for IT Infrastructure' (2018).

unpatched web-server software, combined with inadequate encryption of sensitive customer data, left a glaring SQL-injection vulnerability wide open. A relatively unsophisticated attacker exploited it in October 2015, gaining access to the personal and financial details of 157,000 customers – including names, addresses, dates of birth, and, in thousands of cases, bank account numbers and sort codes. The case remains a textbook example of how neglect of routine patching and poor data-handling practices can trigger both regulatory sanctions and lasting reputational damage.[18]

Taken together, these cases drive home a point that no data controller can afford to ignore: serious compliance with the security obligations in the UK GDPR and the Data Protection Act 2018 is not optional.

If companies regard encryption, patching, access controls, and monitoring as mere box-ticking exercises (or even worse, completely ignore them), the outcome is almost always huge regulatory fines, personal injury claims worth millions of pounds and the company's reputation suffering in the long run. In the cases involving the firms Marriott, TalkTalk, and Morrisons, the litigation has largely shown how the bar has been set higher by the courts and the regulators to ensure that firms are improving their systems of security on an ongoing and proactive basis, rather than in a purely reactive manner after the event has occurred. In an environment in which threats are changing at an ever-accelerating pace, the message could not be clearer: invest in the security of the business, and do it properly, or pay the price down the line in terms of money and reputation.

The Cyber Essentials program that was developed and is now managed by the National Cyber Security Centre (NCSC) not only provides a solid foundation for legal obligations but also highlights them through five very simple but essential technical controls: boundary firewalls, secure user access controls, timely software patching, effective malware protection, and systematic vulnerability management. For small and medium-sized enterprises in particular, the scheme has come to serve as a highly practical, accessible benchmark – one that allows organisations to demonstrate, in a way regulators and courts readily recognise, that they are meeting the "appropriate technical and organisational measures" demanded by the UK GDPR.[19]

2.2. The Civil Wrongs Ordinance and the Draft Data Protection Law of 2025.

The amended British Civil Wrongs Ordinance No. (5) of 1947, effective in the West Bank, particularly its Article 50, forms the legal basis for civil liability for damages resulting from negligence. Negligence, in essence, is nothing more than causing harm through a lack or absence of due care.[20] According to Article 50 of the Civil Wrongs Ordinance, negligence consists of:

---

[18] S Al-Sayigh, *Civil Wrongs (Tortious Liability)* (1st edn, Al-Bahr and Al-Hay'ah Al-Khayriyah Press 1997) [Arabic].

[19] S Khan, C Roberts 'Operationalising Article 32 UK GDPR: The Role of Cyber Essentials as a Compliance Bridge for UK SMEs in a Post-Brexit Regulatory Landscape' (2024) 137 Computers & Security 103629. DOI: https://doi.org/10.1016/j.cose.2023.103629.

[20] B Cinar, *Supply Chain Cybersecurity: Legal and Technical Perspectives* (Cybersecurity Press 2023) 78.

"(a) doing an act which a person of ordinary prudence and foresight, in the circumstances in which the act was done, would not do, or omitting to do an act which such a person would not omit to do in the circumstances in which the omission took place;
(b) or omitting to use the skill or take the care which, in the circumstances, a person of ordinary prudence and foresight, possessing that skill, would use or take in that profession, trade, or art.
In respect of another person to whom the person who did the act or omitted to do it or to use the skill or take the care as aforesaid, owes a duty not to do that act, or to omit to do it, or to use the skill or take the care, as the case may be..."

This publication is a must for organizations to take actions that could prevent predictable damage, based on the "reasonable person standard", which denotes the behavior that society expects a reasonable entity in similar situations to display. In the context of cybersecurity, this standard is used to determine whether the security measures taken by organizations to prevent cyber-attacks are sufficient or not.[21]

The confirmation comes from the stipulations of Article 55 bis (a) of the revised British Civil Wrongs Ordinance of 1947, which declare: "...the infringement of a legal obligation is the non-fulfillment of any person's obligation imposed by any law, other than this Ordinance, if the actual aim of that law, after its true interpretation, is to give or protect another person, and the other person suffers the type or kind of loss that was meant to be prevented by that law through the non-fulfillment..."

The article referred to above implies that statutory duty breach happens if a person does not perform a task required by the law, as long as that law is meant for the protection or advantage of another party. This necessitates the proper understanding of the legislation's intent in order to figure out whether it really is intended to protect a certain group of people, and that the damage being suffered is of the kind that the legislation is trying to prevent. To illustrate, if a specific law requires safety equipment to be provided by the employer and the worker gets hurt due to the lack of it, this non-delivery will be considered a statutory duty breach and will lead to civil liability.

This provision establishes a clear pathway for imposing civil liability on individuals or organisations whose failure to comply with statutory obligations causes harm. At its core, it requires courts to examine two critical issues: whether the legislation was specifically intended to prevent the type of damage that occurred, and whether the harm suffered falls within the scope of protection the statute was designed to afford. In practice, successful claims hinge on demonstrating this close nexus between legislative purpose and actual injury, a principle that has long ensured the article serves as an effective tool for safeguarding the very groups Parliament sought to protect. This approach reinforces the principle of liability in the Civil Wrongs Ordinance, where breach is assessed based on objective standards linking duty, damage, and legislative purpose.

The Draft Data Protection Law of 2025 is intended to create an advanced statutory scheme to improve Cybersecurity and the protection of Personal

[21] A Abu Haniyeh, *Cybersecurity Strategy and Its Indicators* (National Protection Center for Cybersecurity 2023) [Arabic].

Data. Core obligations contained in the Draft Data Protection Law will protect the rights of individuals and require compliance through the following:

Authorising the National Data Protection Authority to set classification level security standards, such as the use of Encryption Technology, to provide periodic Risk Assessments.

Requiring Data Controllers to take reasonable and proportionate steps in developing security measures to mitigate and reduce the likelihood of any Security Breaches at acceptable levels. As examples, measures such as AES-256 Encryption, Multi-Factor Authentication and the implementation of Intrusion Detection Systems would be included within this requirement.

Establishing a 72-hour time frame to notify the National Data Protection Authority and/or affected individuals whenever a Cyber Incident is likely to result in a threat to the Rights and Freedoms of individuals.

Establishing a civil liability regime that creates a framework by which individuals may receive it for their Harm caused by insufficient Data Protection, including to recoup the Material Losses (by Fraud and/or Identity Theft) and Non-Material Losses (by Damaging an Individual's Reputation and Trust).

The Draft Data Protection Law will establish that there may be Administrative Fines, which would act as a deterrent to assist in the enforcement and ensure compliance with the Draft Data Protection Law.

In 2025, the Palestinian Authority has proposed a Data Protection Act which demonstrates their commitment to creating a safe digital environment through its emphasis on being clear and open, responsible and accountable, and to providing a proper level of security for both users and their data to build trust in digital services.

That said, one notable departure from more mature regimes (most obviously the UK GDPR) is the absence of an express right to compensation for non-material damage. Psychological distress, reputational harm, or the intangible loss of trust following a breach – losses that UK and EU courts now routinely recognise and award damages for – are not currently covered. This omission narrows the remedial landscape considerably and, in practice, places the Palestinian framework at a more restrained level of liability than its Western counterparts

The Palestinian Data Protection Law, as a new law, faces significant challenges in its practical application, including:

- Lack of technical expertise: In order to prove the breach of the duty of care, digital forensic reports are needed to ascertain the causes of the breach and the level of negligence. Palestine, however, faces a lack of resources in this area, [22] hindering accurate technical investigations.[23]
- Absence of judicial precedents: The Palestinian judicial system does not have clear judicial rulings that set standards of reasonableness and foreseeability of damage in the context of cybersecurity, which

[22] Kosseff (n 5) 145–147.

[23] International Organization for Standardization (ISO), 'ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements' (2013).

according to some, results in general judicial interpretations that might not be precise. [24]

- Absence of unified local security standards: Unlike international standards such as ISO/IEC 27001 or the British Cyber Essentials program me, there are no unified local security standards in Palestine, [25] making it difficult to determine what constitutes "reasonable" security measures.[26]
- Involvement of third parties: Cyber-attacks often involve external parties, such as hackers or malware, complicating the proof of foreseeable damage or liability. For example, the Home Depot case (2014) in the United States showed the difficulty of holding organisations liable when attacks are caused by sophisticated external parties.[27]
- Full Israeli control over internet infrastructure, including control over the import of technical equipment and restrictions on the development of local networks.[28]

In a hypothetical scenario, if a Palestinian bank neglected to implement Multi-Factor Authentication (MFA), leading to a leak of customer data, affected individuals could claim compensation under Article 24 of the Draft Data Protection Law, relying on Article 50 of the Civil Wrongs Ordinance to prove negligence. [29] However, proving negligence requires presenting precise technical evidence, such as digital forensics reports, highlighting the need to develop technical and judicial capabilities. [30] The National Data Protection Authority could also impose fines under Article 33, but the effectiveness of these penalties depends on the Authority's ability to conduct accurate and transparent technical and legal investigations. [31] The mentioned challenges, such as the lack of technical expertise and local standards, confirm the need for investments in technical infrastructure and training, [32] alongside the development of clear judicial precedents to enhance the effectiveness of the Draft Data Protection Law 2025 and ensure better protection of personal data in Palestine.[33]

2.3. Special Conditions for Considering an Act a Civil Wrong in the Context of Personal Data Protection.

Not Constituting a Conflicting Claim with the Repetition of the Act:

This part requires that the act not be of a type whose repetition leads to repeated or unjustified legal disputes. In the context of personal data protection, this condition can be applied to cases such as a company's database

[24] Cinar (n 20) 85.
[25] D J Solove, W Hartzog, *Breached! Why Data Security Law Fails and How to Improve It* (OUP 2022) 112–115.
[26] F Amoretti and others, 'Palestine: Whose Cyber Security Without Cyber Sovereignty?' in SN Romaniuk and M Manjikian (eds), *The Routledge Companion to Global Cyber-Security.*
[27] sup *Strategy* (Routledge 2021).
[28] Palestinian Draft Data Protection Law 2025, art 24.
[29] Kosseff (n 5) 149.
[30] Palestinian Draft Data Protection Law 2025, art 33; Cinar (n 20) 94.
[31] Kosseff (n 5) 149.
[32] Cinar (n 20) 94.
[33] *Vidal-Hall v Google Inc* [2015] EWCA Civ 311.

breach due to negligence in securing data. If the breach leads to the theft of customer data (such as credit card numbers or personal information) and causes substantial harm like financial fraud, this act is considered a civil wrong because it causes specific damage and is not merely a repetition of trivial disputes. For example, the case of Vidal-Hall v Google Inc [2015] EWCA Civ 311 in English law recognised that the misuse of personal data can constitute a privacy breach worthy of compensation.[34] If the act relates to the leakage of non-sensitive data (like a general email address) without tangible harm, it might be excluded as it could be interpreted as part of recurring digital interactions that do not form the basis for a legal claim, preventing it from becoming a conflicting claim.

Improbability of the Act Being Committed by a Person of Ordinary Perception and Temperament:

This condition requires the act to be serious enough to motivate an ordinary person to file a complaint under the surrounding circumstances, based on the "reasonable person standard" derived from English common law, as in the case of Blyth v Birmingham Waterworks Co (1856) 11 Ex 781, which defined negligence as the omission to take the care a prudent person would take.[35]

Due to the potential impact on individuals whose highly sensitive personal information (such as medical records or banking information) has been improperly disclosed, as a result of a technology company not exercising due diligence and care, there is a clear basis for establishing this type of conduct as a civil wrong. This includes not only the creation of financial harm (direct losses) but also the psychological harm (anxiety and distress) that can ensue from the improper release of highly sensitive personal information. Furthermore, it is reasonable to expect that organisations that are entrusted with personal data will ensure an acceptable level of security in order to safeguard those data. This expectation is well established and ingrained in our society today.[36]

The UK Supreme Court's decision in Lloyd v Google LLC[37] is a definitive confirmation that compensation under Article 82 is not automatic. While the representative action failed, the Court did make clear what the evidentiary standard is for recovering damages, the UK Supreme Court confirmed that the mere violation of a person's rights under data protection legislation (and proven psychological harm) can provide a basis for compensation. Therefore, the judgment adds weight to the broader notion that non-material damages are no longer considered secondary (or peripheral) to this area of the law, but rather are now an integral aspect of the remedial framework.[38] By contrast, when the violation is genuinely trivial (say, sending a few unsolicited marketing emails with no real harm done), courts tend to treat it as something we simply have to live with in the digital age. After all, commercial spam has become part of the furniture of online life, and the threshold of tolerable inconvenience is set far higher than, for instance, the unauthorised disclosure of medical or

[34] *Blyth v Birmingham Waterworks Co* (1856) 11 Ex 781.
[35] *Lloyd v Google LLC* [2021] UKSC 50.
[36] J Pool and others, 'A systematic analysis of failures in protecting personal health data: A scoping review' (2024) 74 Int J Inf Manag 102719 <https://doi.org/10.1016/j.ijinfomgt.2023.10271>.
[37] Lloyd (n 36)
[38] N Nour, 'Damages: Restitutio in Integrum' in Fernández Antuña Antolín (ed), *Jus Mundi* (29 August 2025).

financial records. In such cases, the conduct rarely crosses the line into what would properly be regarded as an actionable civil wrong.

3. The Element of Damage in Cyber Liability Cases (From Tangible to Intangible Damages).

Article 1 of the British Civil Wrongs Ordinance of 1944 defines the term "damage" thus: "loss or injury to property, or deprivation of comfort, or injury to physical well-being or reputation, etc." Damage, as a notion, is one of the key aspects in civil liability cases related to cyber breaches, reflecting the very essence of compensatory claims in the context of intrusion, data leaks, or breach of privacy. The assessment of compensable damage in cases related to cyber liability is not always easy to establish, not only because it is necessary to determine whether the damage is financial, related to fraud or clean-up costs, or moral, reflecting the plaintiff's state of mind, but also to satisfy the quantification requirements, which differ significantly across the globe. The following chapter will attempt to provide a comparative overview regarding the assessment, proof, and compensability of damage in data protection cases, referring to two sets of laws, which, despite their significant differences, will be used to provide the reader with a better understanding of the issue, namely the mature, but now post-GDPR regime in the UK, and the emerging regime currently under development in Palestine. The discussion will be divided into two parts, the first referring to the assessment of material damage, where the routes for recovering financial loss are relatively well established under the laws of the UK and Palestine, while the second part will address the more complex issue of moral damages, where the Palestinian regime is lagging far behind the generous standards currently firmly established in the case law of the UK and the EU.

3.1. Material (Tangible) Damage in Cyber Liability Cases.

Material damage is defined as measurable financial loss resulting from cyber breaches, such as costs for system restoration, credit monitoring, ransom payments, or loss of profits. Proving it requires precise financial documentation, such as invoices or expert reports, to ensure compensation according to the principle of *restitutio in integrum*, i.e., restoring the affected party to their position before the damage occurred.[39] This section discusses material damage in British and Palestinian legal systems.

Firstly: Material Damage in British Law - Legal Framework.
In the United Kingdom, material damage in cyber liability cases is regulated by a legal framework combining the Data Protection Act 2018 (DPA 2018), the UK General Data Protection Regulation (UK GDPR), and common law principles. Under Article 82 of the UK GDPR, any individual who suffers material or non-material damage as a result of a data breach due to non-compliance with the

[39] UK GDPR (n 14) art 82.

Regulation is entitled to claim compensation from the controller or processor.[40]

Material damage in this context typically takes three main forms: the direct costs of restoring systems compromised or destroyed in a cyber-attack; the often-substantial expenses individuals incur for credit-monitoring services and identity-theft protection in the aftermath of a breach; and, most seriously, the financial losses flowing from actual identity theft or fraud enabled by the leaked data. [41]

This private right of action runs alongside, and is entirely independent of, the regulatory enforcement powers of the Information Commissioner's Office (ICO). In practice, it enables affected data subjects to bring civil claims on their own initiative and recover compensation even when the ICO chooses not to pursue (or has not yet completed) its own investigation. [42]

In Lloyd v Google LLC [2021] UKSC 50 the UK Supreme Court settled a point that had caused considerable uncertainty: compensation under Article 82 UK GDPR is never automatic. A claimant must prove actual damage – whether material or non-material – and the mere fact that a breach has occurred, however serious the infringement of the regulation may be, is not enough on its own.Material damage in this context most commonly takes the form of out-of-pocket expenses: the cost of forensic recovery or system rebuilding after an attack, losses directly attributable to fraud or identity theft, credit-monitoring subscriptions taken out in response to the breach notifications, and reasonable legal or administrative costs incurred in mitigating the consequences of the incident.

When awarding compensation, courts are bound by the classic principle of restitutio in integrum: the claimant should, as far as money can do it, be placed in the same financial and psychological position they enjoyed before the wrongful act occurred – no more, no less.[43]

In the specific context of cyber-liability claims, this principle finds direct expression in Article 82 of the UK GDPR. That provision explicitly permits recovery of both material damage (the cost of system restoration, credit-monitoring subscriptions, fraud losses) and non-material damage (serious distress or reputational injury).[44]

Thus, if an individual suffers concrete financial loss because fraudsters exploited data released in a breach, the court will aim to make good that loss pound for pound; the aim is neither to punish the defendant nor to leave the victim short-changed, but simply to restore the status quo ante. [45]

This is evident in the case of Warren v DSG Retail Ltd,[46] where Saini J refused the claimant's claim for the cost of credit monitoring services on the basis that no invoices, receipts, or other tangible evidence of outlay had been placed before the court. It is clear that the court will not pay compensation, even in

[4040] Information Commissioner's Office (ICO), 'Guide to the GDPR: Right to Compensation' (2025).
[41] *Lloyd* (n 39).
[42] F Cuena Boy, 'Restitutio in integrum (DCH)' (Max Planck Institute for Legal History and Legal Theory Research Paper Series No 2024-10, 2024).
[43] UK GDPR (n 14) art 82.
[44] DPA 2018 (n 43) s 168.
[45] *Warren v DSG Retail Ltd* [2021] EWHC 2168 (QB).
[46] ibid.

data breach claims, on a speculative basis.: there must be hard proof of loss actually suffered. Absent such evidence, the claimant cannot be restored to the position they occupied before the breach, and the claim therefore fails. The case has quickly become authoritative on the point that accurate, contemporaneous documentation of loss remains indispensable if Article 82 GDPR damages are to be recovered in practice.[47]

Secondly: Material Damage in American Law - Legal Framework. In the United States, material damage from cyber breaches covers direct financial losses (system repair, forensic costs) and indirect losses (lost profits, missed business opportunities). Tort law governs compensatory damages, while statutes like the California Consumer Privacy Act (CCPA) and the CLOUD Act allows statutory damages of $100–$750 per consumer per incident (or actual losses if higher) and, for intentional violations, civil penalties up to $7,500 per breach.[48]

In In re Equifax, Inc Customer Data Security Breach Litigation,[49] the court held Equifax liable for the 2017 data breach that exposed the personal information of approximately 147 million people. The ruling was based on the legal duty of care stipulated in the Gramm-Leach-Bliley Act (15 U.S.C. § 6801(b); 16 C.F.R. § 314.3), which obliges financial institutions to protect customer data, and on Section 5 of the Federal Trade Commission Act (15 U.S.C. § 45(a)), which prohibits unfair practices that cause substantial harm to consumers

In the case of In re Equifax, Inc. Customer Data Security Breach Litigation,[50] the court dealt with the data breach that occurred in 2017, which revealed the personal data of about 147 million people. The court held Equifax liable for not following the federal statutory obligations regarding the protection of consumer financial information and the prohibition of unfair trade practices.[51] The $425 million settlement remains a landmark in U.S. data-breach litigation.[52]

The court further anchored Equifax's liability in the classic tort principle of foreseeability. Evidence showed that the company had received clear, public warnings about a critical vulnerability in the Apache Struts software as early as March 2017, yet failed to apply the available patch in a timely manner. In the court's view, a breach of this magnitude was not merely possible but entirely foreseeable; the failure to act on known, high-risk vulnerabilities therefore constituted a clear breach of the reasonable standard of care expected of a major credit-reporting agency. The court also relied on the precedent Collins v Athens Orthopedic Clinic 307 Ga 555 (2019). to affirm that the mere exposure of personal data to hacking constitutes a legal injury because it opens the door to risks of identity theft, and the occurrence of subsequent financial fraud is evidence of direct causality, which established Equifax's liability for the resulting damages.[53]

---

[47] California Consumer Privacy Act 2018, Cal Civ Code § 1798.150.
[48] Gramm-Leach-Bliley Act 1999, 15 USC § 6801(b); 16 CFR § 314.3; Federal Trade Commission Act 1914, 15 USC § 45(a).
[49] In re Equifax, Inc Customer Data Security Breach Litigation (MDL No 2800, ND Ga 2022).
[50] ibid.
[51] Gramm-Leach-Bliley Act 15 USC § 6801(b); 16 CFR § 314.3; Federal Trade Commission Act 15 USC § 45(a).
[52] *Collins v Athens Orthopedic Clinic PA*, 307 Ga 555 (2019).
[53] *In re Anthem, Inc. Data Breach Litigation*, No. 15-md-02617-LHK (ND Cal, 2018).

American law, through its recent decisions in the field of data breaches, provides a good principle based on the recognition of the civil liability of companies resulting from the infringement of the legal duty to keep personal data in their custody secure. The case of Anthem may be considered the most evident example of the willingness of American judges to consider a data breach as, by itself, a prima-facie case of unreasonable security practices. The district court did not dismiss the case at the pleadings phase, holding that the mere fact of the successful data breach of 79 million individuals was sufficient to sustain a reasonable inference of unreasonable practices in data security, as implied by tort law and the company's own privacy policy. However, most importantly, the liability was not limited to actual out-of-pocket loss. The final settlement approved in 2020 covered actual financial loss, but it also covered substantial awards for time expended on mitigation, credit monitoring, and, in a marked departure from the traditional scope of tortious liability under the common law, a figure for the inherent loss of privacy in the form of the increased likelihood of identity theft in the future. The message of the Anthem litigation has become a landmark statement of the proposition that the liability for data breach can, and increasingly does, extend beyond economic loss to embrace the concepts of moral injury and potential risk, thereby providing the consumer with a much broader framework of potential redress than many civil law systems would currently support. [54]

Most importantly, however, liability was not restricted to actual out-of-pocket damages. The settlement that was finally approved in 2020 will provide for compensation for actual financial losses, but will also include significant awards for time expended in mitigation, for credit monitoring services, and, in a dramatic shift away from traditional notions of the boundaries of tort liability, for an element recognizing the increased risk of future identity theft and the inherent damage to privacy. In other words, the court and the parties were effectively recognizing that the damage to the value of personal information and the non-economic damage resulting from a data breach are, in and of themselves, compensable forms of damage. The Anthem case has thus become a landmark authority for the proposition that data breach liability does, and increasingly will, go beyond actual economic damage to encompass moral damage and future risk, thus providing a potentially much broader framework." Most importantly, [55] however, liability was not restricted to actual out-of-pocket damages. The settlement that was finally approved in 2020 will provide for compensation for actual financial losses, but will also include significant awards for time expended in mitigation, for credit monitoring services, and, in a dramatic shift away from traditional notions of the boundaries of tort liability, for an element recognizing the increased risk of future identity theft and the inherent damage to privacy. In other words, the court and the parties were effectively recognizing that the damage to the value of personal information and the non-economic damage resulting from a data breach are, in and of themselves, compensable forms of damage. [56] The Anthem case has thus

[54] ibid.
[55] Federal Rules of Civil Procedure, r 23.
[56] *TransUnion LLC v Ramirez*, 141 S Ct 2190 (2021); *Tsao v Captiva Software Inc*, 2020 US Dist LEXIS 172113 (SD Fla).

become a landmark authority for the proposition that data breach liability does, and increasingly will, go beyond actual economic damage to encompass moral damage and future risk, thus providing a potentially much broader framework of remedies for the consumer than many civil law traditions might support.[57]

Thirdly: Material Damage in Palestinian Law. In Palestine, material damage is defined under the Civil Wrongs Ordinance (1944) as "the term 'damage' means loss or injury to property, or deprivation of comfort, or injury to physical well-being or reputation, etc." (Article 2). In the context of cyber liability, this includes costs for system restoration, ransom payments, or compensating customers for financial losses. Article 3 obligates the causer to compensate, stating: "The following matters, as set out in this Ordinance, are civil wrongs, and subject to the provisions of this Ordinance, any person who has suffered harm or damage, due to a civil wrong committed in Palestine, is entitled to obtain the redress which this Ordinance grants him from the person who committed that wrong, or who is responsible for it... Provided that no act shall be deemed a civil wrong if its repetition would not lead to the formation of a conflicting claim, and would not cause a person of ordinary perception and temperament to complain under the circumstances surrounding the case."

The aforementioned article sets the framework for tortious liability by granting a person who has suffered harm or damage within Palestine the right to seek "redress" (compensation or legal remedy) from the perpetrator or person responsible for the civil wrong. The claimant must still prove both damage and a causal link, requirements that remain firmly rooted in the English common-law tradition, most famously articulated in Donoghue v Stevenson [1932] AC 562, the case that gave us the modern concept of duty of care. [58]

In relation to the particular sector of personal data protection, Article 3 is easily employed within the two broad themes of illegal conduct, namely the negligent handling of private data (failing to protect databases, lack of controls on access, inter alia), as well as intentional breaches (unauthorised publication/discovery of private information). If harm, whether of a tangible (loss from financial fraud, clean-up expenses) or non-material (clinically significant distress, defamation, inter alia) nature, is thereby caused, it is clearly a civil wrong. The article thus expands the traditional tortious regime into the new arena of cyberspace, while ensuring that the essence of causation is retained, with a corresponding modification of 'breach' to suit the peculiarity of the handling of private data.

The goal is to achieve justice by compensating the affected party, considering the modern technological context.

Referring to the rulings of Palestinian courts, we find that they have not directly addressed cyber liability cases, but principles can be extrapolated from the following rulings:

The Palestinian Court of Cassation, Decision No 11/2024 (14 May 2024) held that: Material damage in tortious liability requires proving actual or anticipated financial loss (such as burial expenses or loss of support) with clear evidence proving its occurrence and its causal link to the harmful act. Speculative or

[57] Tsao v Captiva MVP Restaurant Partners LLC 986 F3d 1332 (11th Cir 2021).
[58] *Ramirez* (n 57).

unsubstantiated claims are rejected, and the damage must be personal to the claimant, according to Article 55/1/7 of the Civil Wrongs Ordinance of 1944.

In the same context, Palestinian Court of Cassation, Decision No 453/2022 (10 December 2023)., held that material damage, as defined by Article 1 of the Civil Wrongs Ordinance No. 36 of 1944, is the actual loss or expense estimable in monetary terms. For a compensation ruling, the plaintiff must detail it in the statement of claim or its attachments, negating gross uncertainty according to Article 60(b). The statement must contain the act of damage, the dates of the act of damage, and the nature of the material damages for the case to be considered acceptable, with the emphasis being that a defect in the details of the statement does not necessarily disqualify the case, as upheld by the Court of Cassation Ruling No. 847 of 2020.

The judgment also clearly distinguishes between the grounds of objection to the case, whether substantive or procedural, as in the case of a denial of the case being vexatious. The judgment clearly states that an inadmissibility plea under Article 90 of the Code of Civil and Commercial Procedure may only be grounded on purely procedural grounds. It follows then that where the plaintiff has furnished the court with the requisite particulars of the act of damage, it becomes unlawful for the court to strike the case off for uncertainty. The court must then proceed to examine the case to determine the extent of the loss. Anything less than this would be a violation of the principle of procedural economy and the plaintiff's constitutional right to have the case heard by the trial court.

In my view, the UK takes a fair stance on proving damage and standing in cyber liability cases under Article 82 of the UK GDPR, which requires proof of actual damage, whether material or non-material. This is substantiated by the ruling in Lloyd v Google LLC [2021] UKSC 50, which reiterated that a simple data breach is insufficient for a claim of compensation, which requires proven financial loss or psychological suffering, signifying a dedication to judicial specificity. However, it is significant that the UK stance is far more sympathetic to claims of psychological suffering than the United States. Where American courts (outside a scattering of progressive states) remain loath to commit to a full compensation remit unless there is actual physical harm or, at the very least, some form of pecuniary loss, the UK has clearly gone the other way.[59]

This is clearly demonstrated in the case of Warren v DSG Retail Ltd [2021] EWHC 2168 (QB). In that case, although the claim failed, it is significant that it failed not on the basis that a lack of financial loss following a data breach, amounting merely to anxiety/distress, is automatically non-compensable. Instead, Mr. Justice Saini simply stated that he rejected the case on a narrow technical point that the plaintiff could not plead a degree of distress sufficient to cross the threshold for compensation. In short, the court clearly indicated that, but for the lack of severe psychological damage, compensation would be available even in the absence of even a single penny of economic loss.[60]

[59] 'Liability for nonmaterial damage under the GDPR: Approaches of EU, UK courts' (IAPP, 13 December 2025) <https://iapp.org/news/a/liability-for-non-material-damage-under-the-gdpr-approaches-of-eu-uk-courts>.

[60] UK High Court dismisses claims following DSG data breach' (Lexology, 5 August 2021) <https://www.lexology.com/library/detail.aspx?g=f6664c7c-fa39-4320-8bfd-609b4b776f38> accessed 13 December 2025.

a far more stringent bar is adopted within the American jurisprudence. There,Cyber-breach plaintiffs are required to show that they alleged an actual or threatened "injury in fact" to plead standing, particularly within a class action suit. In the Supreme Court's opinion in TransUnion LLC v Ramirez (2021), a plaintiff's allegation that his identity might be stolen, together with a claims defendant's insistently inaccurate storage of his particular private information, lacked sufficient immediacy to state a valid claim seeking relief in compensation. Such a plaintiff's threat of identity theft, especially with thus-far unfrozen private data, is insufficient to state a valid claim when suffering no contemporaneous financial harm. This stringent approach is far more restrictive when contrasted with the current, far more permissive regime adopted within the U.K.[61]

On the other hand, the American rule is far more stringent. It has been emphasized that to develop standing, especially in a class action suit, it is necessary that there be an actual or imminent "injury in fact." The Supreme Court, in the case of TransUnion LLC v. Ramirez (2021), has ruled that a possible threat of identity theft or improper storage of data cannot constitute a grievance eligible for compensation unless there is some concrete, immediate harm involved. This is a far more restrictive regime on cyber breaches that result in no real, immediate, or pecuniary harm, as is now recognized under UK law. [62]

As for Palestinian law, it is the most flexible, as detailing material or anticipated damage (such as loss of profits or reputation) is sufficient without requiring imminent harm, as evident from Palestinian Court of Cassation decisions, like Decision 453/2022 (10/12/2023). This flexibility, derived from the Civil Wrongs Ordinance of 1944, allows affected parties to file lawsuits based on potential losses. The absence of punitive damages makes the scope narrower compared to the American system, which may reduce its effectiveness in deterring gross negligence, a topic which will be discussed in the second section.

3.2. Moral Damage in Cyber Breaches.

Moral damage is the non-material harm that affects an individual's dignity, feelings, reputation, or social standing, and is characterised by difficulty in estimation compared to material damage measurable financially, such as costs for replacing credit cards or credit monitoring. [63] It includes psychological distress, emotional pain, anxiety, social embarrassment, or harm to reputation resulting from the violation of personal rights like privacy or honour.[64] In the context of cyber breaches, moral (non-material) damage primarily stems from

---

[61] TransUnion LLC v Ramirez 594 US 413 (2021) (Supreme Court of the United States) <https://www.supremecourt.gov/opinions/20pdf/20-297_4g25.pdf> accessed 13 December 2025.

[62] MSM Alqudah, 'Civil Legal Framework for Moral Damage in Jordanian Law' (2024) 16 Pakistan Journal of Criminology 317.

[63] WH van Boom, 'European Tort Law – An Integrated or Compartmentalized Approach?' in A Vaquer (ed), *European Private Law Beyond the Common Frame of Reference* (Europa Law Publishing 2008).

[64] Abdelaziz Al-Sasmeh, *Tortious Civil Liability, The Harmful Act* (Al-Dar Al-Ilmiyah Al-Dawliyah and Dar Al-Thaqafa 2002) 90 [Arabic], D J Solove, *The Digital Person: Technology and Privacy in the Information Age* (NYU Press 2004) 45.

the unauthorised disclosure or misuse of personal data, producing tangible psychological and social consequences for the victim: persistent anxiety over potential identity theft, constant fear of blackmail following the leak of intimate photographs or medical records, or a profound sense of helplessness and personal violation when one's financial or health history becomes accessible to strangers.

These effects are far from mere transient embarrassment. In many cases they evolve into genuine psychiatric disorders (generalised anxiety, depression, or even post-traumatic stress disorder in severe instances) and can endure for years and significantly impair quality of life and interpersonal relationships. Consequently, moral damage in data-breach litigation must be regarded as real and compensable harm in its own right, even in the complete absence of direct financial loss. [65]

A growing body of jurisprudence (particularly in post-GDPR Europe) now recognises that the very fact of a serious cyber breach constitutes a profound assault on personal privacy. Victims frequently describe an overwhelming sense of helplessness, a lasting erosion of trust in the institutions entrusted with their data, and, in many cases, acute social embarrassment that can linger for years. [66]

The harm becomes especially intractable when the breach involves the publication of intimate photographs or deeply private records. Reputational injury of this kind is often effectively irreversible: even successful takedown efforts rarely erase every trace from the internet, leaving the individual with a permanent digital shadow. [67]

What sets moral damage in cyber cases apart from traditional torts is its inherently transnational and intangible character. Unlike a cross-border, digital phenomenon that is far harder to quantify and prove than, say, a broken limb. Courts are therefore grappling with the challenge of translating subjective, non-pecuniary suffering into compensable loss without the comfort of concrete medical bills or lost earnings statements, a task that remains one of the most difficult frontiers in contemporary privacy litigation. [68]

Legal systems differ in addressing moral damage. In British law, Article 82 of the GDPR allows compensation for non-material damage without proving financial loss.[69] In Various Claimants v WM Morrison Supermarkets Plc [2020] UKSC 12, the UK Supreme Court affirmed the company's liability for the psychological distress of 100,000 employees due to a data leak by an internal employee.[70] In American law, proof of tangible psychological harm is required. In compensation for general anxiety was rejected due to the lack of medical evidence.[71] In In re Anthem, Inc Data Breach Litigation 327 FRD 299 (ND Cal 2018) compensation was only accepted for those who provided medical reports proving psychological impact.[72]

---

[65] ibid 47.
[66] ibid 49.
[67] Rogers (n 58) 127.
[68] Regulation (EU) 2016/679 (GDPR), art 82.
[69] *Various Claimants* (n 19).
[70] *In re Yahoo! Inc Customer Data Security Breach Litigation*, 334 F Supp 3d 1010 (ND Cal 2019).
[71] *In re Anthem* (n 52).
[72] Civil Wrongs Ordinance 1944, art 2.

In Palestinian law, moral damage is defined under Article 2 of the Civil Wrongs Ordinance (1944) as an infringement on honour or reputation,[73] but it faces challenges in the cyber context due to the absence of specialised judicial precedents. [74] Palestinian Court of Appeal, Appeals Nos 819/2022 and 900/2022 (30 June 2024), the court confirmed that moral damage is limited to infringement on reputation or honour and does not include general psychological distress without strong evidence. [75] The Palestinian Court of Cassation, Decision No 632/2025 (13 February 2025).that compensation for moral damage requires an explicit legal text, and pure moral damage is difficult to estimate without primary evidence, and in this case, the plaintiff did not prove moral damage, so the failure to award moral compensation was in accordance with the law.[76]

4. Legal Integration Between Articles 60 and 55 bis in Addressing Causality.

Proving causality is an essential element in civil liability cases for cyber breaches, requiring the determination of the direct or contributory link between negligence or the wrongful act and the resulting damage. This issue gains special importance in the context of cyber breaches due to the complexity of intertwined causes, such as negligence by entities responsible for data protection, actions of hackers, or even negligence by the victims themselves (e.g., using weak passwords). This chapter discusses the legal integration between Article 60 and Article 55 bis of the effective British Civil Wrongs Ordinance in Palestine, with reference to Article 50, to analyse how causality is addressed in cyber liability cases.

4.1. Article 60 of the Palestinian Civil Wrongs Ordinance Provides a Solid Legal Framework for Linking Compensation to Causality.

Article 60 of the British Civil Wrongs Ordinance of 1944 states: "Compensation may be awarded either alone or in addition to a prohibitory or mandatory order, subject to the following conditions:

(a) If the plaintiff has suffered damage, punishment shall only be for damage which might naturally arise in the ordinary course of things and which directly results from the civil wrong committed by the defendant.

(b) If the plaintiff has suffered material damage, compensation for that damage shall only be awarded if the plaintiff has detailed that damage in his statement of claim or attached it thereto."

Article 60 of the British Civil Wrongs Ordinance links compensation to causality by requiring direct or foreseeable damage (clause a) and detailing material damage (clause b).

[73] Civil Wrongs Ordinance 1944, art 64.
[74] Appeal Nos 819/2022 & 900/2022 (Palestinian Court, 30 June 2024).
[75] Court of Cassation Decision No 632/2924 (13 February 2025).
[76]CrowdStrike, 'Log Files: Definition, Types, and Importance' (20 December 2022).

Article 60 of the Civil Wrongs Ordinance (which remains in force in Palestine) is heavily weighted towards pecuniary loss. Subsection (b) of Article 60 does so explicitly by requiring "the claimant to particularise the loss in his statement of claim." Such a phrase seems to marginalise claims of non-pecuniary loss. In an age where cybercrime causes severe emotional distress, loss of privacy, and anxiety, it seems to offer victims no hope of recompense for what most directly concerns them. The Equifax settlement in the US in 2017, which involved substantial damages claims for "emotional distress" due to identity theft, represents what Article 60 currently has no possibility of awarding. [77]

The same provision (b) also sets an almost insurmountable evidentiary bar for the digital case. The demand for "precise details" of the damage forces the plaintiff to submit advanced technical evidence – system logs, forensic reports, blockchain data, AI-generated attribution studies – that is often costly, technically sophisticated, and beyond the reach of the ordinary individual. Although such evidence was clearly dispositive in the SolarWinds (2020) and The DAO (2016) cases, [78] Additionally, there are no clear Palestinian laws or judicial standards to evaluate the reliability of scientific or technical evidence (similar to the U.S. "Daubert" standards), which would enable Palestinian judges to apply a reliable framework in admitting such evidence. [79]

Clause (a), on the other hand, specifically incorporates the classic common law limitation of "foreseeability" – i.e., damage is limited to that which was "foreseeable" or resulted "naturally" from the tort. In the world of advanced persistent threats and zero-day exploits (again, Solar Winds is the paradigm case), such a standard can easily lead to the exclusion of all damage on the theory that no reasonable person would have foreseen the particular attack vector used. In contrast, the "substantial factor" test used in many US jurisdictions greatly expands the range of recoverable damage. [80]

Taken together, these features of Article 60 – material-damage centrism, stringent particularity requirements, and foreseeability constraints – place Palestinian data-breach victims at a distinct disadvantage when measured against the more generous remedial landscape now prevailing in both the post-GDPR United Kingdom and large parts of the United States. [81]

4.2. Enhancing Integration Between Article 60 and Articles 50 and 55 bis.

Article 50 of the British Civil Wrongs Ordinance effective in the West Bank stipulates that civil liability requires proving that the act or omission was the direct or contributory cause of the damage, meaning it must be proven that the damage would not have occurred but for the act or omission, whether it was the sole cause or one of the contributing causes.

Article 50 focuses on the direct link between the act and the damage, making it an effective tool in simple cases, such as a company's negligence in protecting

[77] MyCrypto, 'Understanding Event Logs on the Ethereum Blockchain' (Medium, 4 March 2020).
[78] *Daubert v Merrell Dow Pharmaceuticals, Inc*, 509 US 579 (1993).
[79] Mandiant, *'Sunburst: A Sophisticated Supply Chain Attack*' (2020).
[80] Restatement (Second) of Torts § 431 (1965).
[81] OWASP, 'Zero Day Attacks' (2023).

customer data leading to a data leak. However, in complex cyber cases with multiple intertwined causes (like company negligence and hacker actions or victim negligence), applying the article may be difficult due to the lack of a clear framework for analysing intertwined causes.

Article 50 offers a robust approach to establishing causation, but there is a failure to address how intertwined causes, such as a hacker attack and negligence on the part of the plaintiff, will be managed. In fact, this could seriously weaken Article 50's potential impact on cyber-related cases, as evidence will inevitably involve a complex process of teasing apart a complex chain of technical circumstances and interlinked causes.

Take, for example, a hypothetical case where some contributory fault on the part of the customer himself/she herself, perhaps a weak password, clicking on a phishing link, or failing to enable two-factor authentication, played some contributory part. Article 50, standing on its own, offers little guidance on any means of quantifying that contributory fault, or how a potential adjustment might be made in consequence. Article 60 then adds an additional layer of requirements with regard to foreseeability and particularisation, making things even more difficult for the claimant.

What is really needed, however, to make Article 50 and Article 60 work coherently with one another in a cyber-related case is some form of interpretative guidance or a minor amendment to Article 50 that explains how contributory negligence is to be assessed, especially with regard to a harm suffered in cyberspaceFor instance, in the case of Surety, blockchain logs could provide evidence of causation; the lack of standards for analyzing intermingled causes within Article 50 can create complexity that impede the application of Article 60 if a third party, such as hackers, intervenes to contribute to the damage.

Integration with Article 55 *bis* (a, b, c):

The following article gives a more specific framework on how to establish causality and liability:

(a) " It ties liability to the breach of a statutory duty, and it requires that the damage be of the type which the legislation seeks to prevent. This is another way of expressing the principle of foreseeability, in that the damage must be a foreseeable consequence of the breach, and the clause is thus assimilated to the American concept of "proximate cause."

(b) " It does not include damage caused by unforeseen natural forces-events or deliberate negligence of another party, such as plaintiff's negligence or hacker intervention. This exemption narrows the frame within which one may be found liable in a case where the damage is caused by factors external to the system, sophisticated cyber-attacks being one variety of these. Zero-day attacks mean cyber-attacks conducted using unknown security vulnerabilities in software for which patches have not been released yet, or they are just unknown, so that those attacks cannot be predicted or prevented in advance. Correspondingly, the damages caused by them are legally excluded because of uncontrollable character".

c) "It permits a reduction of compensation according to the plaintiff's negligence, consistent with Article 60(b)'s criteria for itemizing damage; nevertheless, this will be perfected if the courts can develop legal tests on the

percentage of comparative negligence in cyber cases, for instance, whether the use of a weak password by a plaintiff is sufficient negligence to reduce compensation. In the The DAO case, it was partial investor negligence - failure to independently verify contract security - that contributed to the damage; thus, for compensation decisions under Article 60, the application could be made under Article 55 bis c)".

5. Conclusion.

The British Civil Wrongs Ordinance of 1944, amended by Law No. (5) of 1947, in force in Palestine, is a traditional legal system tailored in a historical setting utterly unlike the technical and legal intricacies imposed upon current cyber breaches. This can critically weaken the usefulness of the provision in cyber-related cases, because proof in those cases would almost always depend on untangling a complex series of technical events and overlapping causes.

For example, in the paradigm case of contributory fault or negligence on the part of the customer, such as the poor password, clicking on a phishing email, or failure to enable two-factor authentication, which contributed to the breach to some degree, there is nothing in Article 50 which appears to offer any guidance on measuring the degree of contributory fault and apportioning liability accordingly. Then, of course, there is the added layer of cake with regard to foreseeability and particularisation of loss under Article 60.

What would actually help to make these provisions work in harmony with one another in the digital world would be to provide interpretive guidance or a limited amendment to Article 50 to provide clarification on how contributory negligence is to be determined in cyberspace. The clarification that would be created by such an amendment would remove the confusion now existing and enable Article 60's procedural requirements to be sensibly and proportionally applied to data breach litigation.

1. The difficulty of proving causality in an environment where multiple players are involved-the service provider, the hacker, and the user-all connected in various way.
2. The insufficiency of provisions to keep pace with the type of moral damage arising from data violation, which cannot be measured in tangible ways despite its severity.
3. There are no standards on which to base "reasonableness" with regard to security measures required in the digital world; this provides much room for interpretation.

It follows then that this law must be developed with a proactive approach to legislation where development is based on:

- Assisting the systematic reform of existing legislations through the introduction of clear definitions of terms such as "personal information," "cyber breach," "duty of care in cyberspace," "cyber moral damages," etc., similar to the definitions provided in contemporary legislations such as the UK GDPR.
- Improvement of coordination between articles: Providing detailed judicial and interpretive directives that clarify the application of the

combination of articles (50, 55 bis, 60) of the existing legislation in cyber crime cases, especially during the analysis of the causation of damage in the event of concurrent negligence of the victim or the intervention of a third party.

- Reference to security standards: For example, the proposed National Data Protection Authority can create a guide that explains the meaning of "reasonable security measures" using international security standards such as ISO 27001 or NIST. This will ensure that there is an objective criterion that the judiciary can take into account while deciding whether an organization has fulfilled its duty of care or not.
- Development of judicial and technical capacities: Training judges and lawyers to understand the analysis of digital evidence and the creation of specialized judicial circuits.