ZAMONAVIY ILM-FAN VA INNOVATSION TADQIQOTLARDA NATIJALAR MUHOKAMASI

XIX-RESPUBLIKA ILMIY-AMALIY KONFERENSIYA

YAKUNLARI BO'YICHA ILMIY ISHLAR TO'PLAMI

Issue - 7(2025) Available at www.uznauka.uz

# COMPARATIVE LEGAL FRAMEWORKS FOR THE COMPENSATION OF NON-MATERIAL HARM FROM CYBERATTACKS

**Yorkinova Sangina**

Master's student of Tashkent State University of Law

***Abstract:*** *Cyberattacks frequently inflict not only financial losses but also significant non-material harm, including psychological distress, reputational damage, and loss of control over personal data. Legal frameworks across jurisdictions vary widely in how they recognize and compensate such intangible harm. This thesis provides a comparative analysis of how the European Union, the United Kingdom, the United States, and Japan address non-material damage resulting from cyber incidents. It finds that EU law explicitly allows compensation for non-material harm (for example, under data protection regulations), and recent court decisions have affirmed that even loss of data control or emotional upset can be compensable if actual and proven. In contrast, English courts have been more cautious, generally requiring proof of distress beyond a de minimis threshold before awarding damages for data breaches, although UK privacy torts have recognized loss of privacy itself as a head of damage in egregious cases. The U.S. legal approach remains the most restrictive – victims of cyberattacks often struggle to sue for purely emotional or reputational harm absent concrete financial injury, due to stringent standing and damage requirements, though some state laws now provide statutory damages for data breaches. Japan's system, influenced by civil law principles, acknowledges mental anguish from privacy violations as*

*compensable even without economic loss, but awards are typically modest, reflecting a policy of recognition rather than punishment.*

***Keywords:*** *non-material harm, cyberattacks, civil liability, comparative law, psychological distress, reputational damage, data protection, digital rights, damage assessment, legal frameworks.*

Across all these jurisdictions, theoretical and practical challenges persist in defining, proving, and quantifying non-material harm. Intangible cyber harms are inherently subjective, making it difficult to delineate what level of anxiety or reputational hit constitutes a legal injury. Evidentiary hurdles are considerable: plaintiffs must demonstrate a causal link between the cyberattack and their psychological trauma or reputational setback, often relying on personal testimony or expert evidence. Quantification of non-material damage is perhaps the greatest challenge – unlike monetary loss, there is no objective market value for emotional suffering or diminished reputation. Courts have adopted various strategies, from nominal or symbolic damages to analogies with personal injury awards, but outcomes remain inconsistent. The comparative survey reveals a tension between the need to fully redress victims' intangible harms and the need to prevent speculative or trivial claims. In Europe and Japan, the trend is towards broader acknowledgment of cyber-induced emotional harm and loss of data autonomy, emphasizing the protection of individual rights. Anglo-American jurisprudence, however, exhibits more skepticism, often limiting recovery to cases of palpable suffering or clear wrongdoing. The result is a patchwork of legal responses: some jurisdictions offer victims of cyberattacks a pathway to recover for psychological distress and reputational harm, while others effectively shut the door unless

tangible damage is shown. This divergence raises profound questions about justice and deterrence in the digital age. Ultimately, the thesis highlights that while non-material harm from cyberattacks is increasingly recognized in theory, courts worldwide continue to grapple with its practical application. Achieving a coherent approach will require refining legal definitions of digital harm, developing better evidentiary standards for emotional and reputational injury, and perhaps embracing innovative solutions (such as statutory damages or settlement frameworks) to ensure that those harmed in cyberspace are not left without remedy. The ongoing evolution of comparative legal practice in this area underscores both the progress made and the work still needed to balance the rights of individuals against the realities of intangible cyber harms in civil litigation.

Beyond the challenges of proving and quantifying non-material harm, an important theoretical concern arises regarding the purpose of such compensation in civil law. Should the goal be to restore the victim to a pre-harm emotional state, deter future negligence, or symbolically affirm the importance of digital rights? Different legal cultures provide different answers. In jurisdictions with strong individual rights frameworks, such as Germany or Canada, the right to digital dignity and psychological security is often emphasized. This contrasts with the more utilitarian approach in U.S. law, where deterrence and economic efficiency dominate the rationale for civil liability. These foundational philosophical differences complicate efforts at harmonizing standards, especially in cross-border cyberattacks where multiple legal systems may claim jurisdiction.

One promising development in this area is the rise of interdisciplinary forensic methods for documenting digital trauma. Psychologists, digital forensic

analysts, and legal experts are beginning to collaborate in order to better measure the psychological and reputational consequences of cyberattacks. For instance, expert testimony is increasingly used in courts to contextualize anxiety, shame, or reputational loss arising from specific forms of cyber intrusion, such as doxxing, identity theft, or revenge porn. Courts that are receptive to this kind of evidence demonstrate a more modern understanding of the realities of digital harm, although such approaches remain underutilized. Moreover, as public awareness of data privacy and emotional integrity grows, courts and legislatures may be increasingly willing to adopt evidentiary presumptions that shift the burden onto defendants in egregious cases of data mismanagement or cyber negligence.

Lastly, the broader social implications of under-compensating non-material harm in cyber contexts should not be overlooked. In an environment where cyberattacks are rising in frequency and sophistication, the law's failure to provide meaningful redress may undermine public trust in both legal institutions and digital technologies. If victims feel that courts cannot acknowledge or address their suffering—especially when such harm involves humiliation, anxiety, or professional consequences—the legitimacy of the justice system may erode. Therefore, robust recognition of non-material harm is not merely a private matter but a structural necessity for preserving civil confidence in the digital rule of law. Developing comprehensive, predictable, and fair standards for compensating such harm remains a pressing objective for the global legal community.

**References:**

Citron, D. K., & Solove, D. J. (2018). Risk and anxiety: A theory of data-breach harms. Texas Law Review, 96(4), 737–786.

Lascelles, G. (2025, January 23). Liability for nonmaterial damage under the GDPR: Approaches of EU, UK courts. IAPP News.

MacLachlan, M. (2024, February 16). Class action liability following a data breach. Shoosmiths LLP.

Pardieck, A. (2023). Privacy matters: Data breach litigation in Japan. Washington International Law Journal (forthcoming). [SSRN Working Paper].

Pauly, D. (2024, July 5). Allegation of fear does not justify compensation – ECJ confirms case law on Art. 82 GDPR. Linklaters.

UK Supreme Court. (2021). Lloyd v Google LLC [2021] UKSC 50.