UDC 347.7:004.056.5
DOI: 10.63341/naia-herald/3.2025.98

The impact of judicial precedents in data breach cases on entrepreneurial activity: Current case studies

Igor Rudenko*
Master of Science
Yaroslav Mudryi National Law University
61024, 77 Hryhorii Skovoroda Str., Kharkiv, Ukraine
https://orcid.org/0009-0008-3582-3951

Olha Khorolska
Master of Science
Yaroslav Mudryi National Law University
61024, 77 Hryhorii Skovoroda Str., Kharkiv, Ukraine
https://orcid.org/0009-0004-9853-2378

Mariia Turchina
PhD in Law
Yaroslav Mudryi National Law University
61024, 77 Hryhorii Skovoroda Str., Kharkiv, Ukraine
https://orcid.org/0000-0002-1486-1122

■ **Abstract.** This study aimed to examine the impact of judicial precedents in cases concerning the leakage of personal and corporate data on the development of legal practice and business strategies. The research involved an analysis of key court cases, which made it possible to determine how these incidents have influenced corporate liability and behaviour. The study addressed cases such as Equifax, Facebook-Cambridge Analytica, British Airways, T-Mobile, and the Ukrainian mobile operator Kyivstar. The rulings in these cases not only imposed fines but also established new principles of corporate ethics, requiring companies to adopt a systematic approach to personal data protection, ensure transparency in user interactions, and strengthen their internal legal culture. The number of incidents continues to grow: since 2024, there has been a 25% increase in recorded data breaches compared to previous years. This demonstrates that data breaches are no longer regarded merely as technical issues but have become legally significant events with substantial economic and regulatory implications. In response, businesses are compelled to reconsider their strategies, implement new data protection policies, and incorporate potential legal risks into risk management frameworks. The practical significance of the issue lies in the fact that analysing major cases enables the forecasting of possible consequences of data breaches, the assessment of legal risk levels, and the development of effective strategies for accountability and prevention

■ **Keywords:** cybersecurity; personal data; legal regulation; information security; data protection; offences; damages

■ **Suggested Citation:**
Rudenko, I., Khorolska, O., & Turchina, M. (2025). The impact of judicial precedents in data breach cases on entrepreneurial activity: Current case studies. *Scientific Journal of the National Academy of Internal Affairs,* 30(3), 98-111. doi: 10.63341/naia-herald/3.2025.98.

■ *Corresponding author

■ Received: 09.06.2025; Revised: 29.08.2025; Accepted: 29.09.2025

Copyright © The Author(s). This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/)

Introduction

Judicial precedents in the field under study establish certain standards for companies, reshaping classical approaches to risk management and corporate governance. The introduction of regulatory frameworks such as the General Data Protection Regulation[1] (GDPR) has significantly transformed the legal environment, imposing new levels of liability on companies and creating complex challenges for global commerce. Of particular importance is the examination of the influence of judicial decisions on innovative technology sectors, as traditional legal norms often fail to keep pace with rapid technological development. The analysis of recent cases helps to identify trends in the formation of new legal standards, which is critically important for strategic business planning in the context of the digital transformation of the economy. Moreover, the growing interdependence between cybersecurity issues and the financial stability of companies makes such research an integral component of contemporary corporate law and economic security.

O.O. Bernaziuk (2023), in a study, analysed current approaches to the concept of a "judicial precedent", considering, in particular, the categories of judicial precedent and judicial practice within the framework of information law and administrative procedure. The scholar emphasises that judicial precedent is intended to ensure a uniform approach to the interpretation of legal norms, the resolution of contradictions, and the filling of gaps in legislation. Judicial precedent does not create new legal norms but determines the obligatory manner in which existing norms are to be applied, which is characteristic of the continental legal system of Ukraine.

I. Sopilko & E. Zubko (2024) examine the conceptual distinctions between hacking and data breaches, analysing the risks associated with information compromise. The scholars note that judicial decisions in cases concerning unlawful access to or leakage of personal data contribute to establishing clear legal boundaries of corporate liability. They emphasise that precedents define the required scope of technical and organisational security measures and promote the standardisation of good practice in the field of cybersecurity. I. Pokhylenko (2023), having studied the specifics of legal regulation in the protection of personal data, concludes that safeguarding personal data is not only a technical or legal issue but also a key element in guaranteeing human rights and freedoms, as well as an essential component of national security. Under conditions of martial law, cyberattacks, and the temporary occupation of parts of the country's territory, the likelihood of unauthorised access to sensitive information increases, creating additional threats to citizens. For this reason, an effective system of personal data protection must be based on a combination of legislative guarantees, technical solutions, and public awareness of individual rights. Ensuring such protection is the responsibility of both the state and all entities that process personal data. In an article, K. Nekit (2020) considers the economic nature of personal data and argues for the necessity of its legal protection as a form of property. This has particular significance for businesses, as judicial precedents confirming the proprietary value of information compel companies to strengthen internal security policies and adopt a more cautious approach to the processing of customer data.

As noted in the study by O. Zadereyko *et al.* (2022), devoted to the challenges of ensuring user data protection in information systems, the consequences of data breaches for businesses can be extremely serious: loss of customers due to diminished trust, financial damage, lawsuits, regulatory sanctions, and reputational harm that may last for years and hinder corporate development. In some cases, a data breach becomes a critical turning point after which a company is unable to regain its market position. I.Y. Dumanska *et al.* (2022), in research focused on the impact of personal data protection policies on enterprise development, particularly in the IT sector, highlight the importance of a systematic approach to data management both at the level of state policy and within individual enterprises. This requires not only the implementation of effective technical solutions but also the enhancement of legal culture, the adaptation of international standards, and the advancement of sectoral research for a deeper analysis of the institutional environment's influence.

F. Schäfer *et al.* (2023), whose research addresses the challenges of data management and privacy protection in product-based businesses, observe that cases of data breaches compel enterprises to carefully review their contracts, privacy policies, and internal information-handling regulations. The risk of losing control over information presents new challenges for businesses, the most significant of which is the necessity of complying with legal requirements in the field of personal data protection. Companies are compelled to implement effective control measures, conduct regular audits, and ensure transparent reporting in order to comply with established standards. Such measures help minimise the risks of fines and reputational loss, while also maintaining the trust of clients and partners.

M. Kotenko *et al.* (2025), in a study analysing personal data protection in Ukraine through the lens of European judicial practice, emphasise the importance of adhering to the "three-part test" of lawfulness

[1] General Data Protection Regulation. (2016, May). Retrieved from https://gdpr-info.eu/.

in personal data interference: (1) in accordance with the law; (2) for the purpose of achieving a legitimate aim; and (3) by proportionate means. In their article, M. Bem & I. Horodysky (2019) draw attention to the serious challenges facing Ukrainian legislation on personal data protection, particularly regarding compliance with the requirements of the General Data Protection Regulation. The researchers note that, given the increasing prevalence of judicial decisions based on GDPR norms, Ukrainian businesses are increasingly adapting internal processes to European standards, even without direct integration with the EU.

This study aimed to determine how judicial decisions in cases of breaches of personal and corporate data confidentiality influence the development of legal practice and the shaping of corporate business strategies.

Materials and Methods

The study was based on the case study method, which made it possible to identify key legal precedents and their impact on business practice. Judicial rulings were examined in Case "Mr L Beresford v. British Airways Plc"[1], "People of the State of California, v. Equifax Inc."[2], "United States of America v. Facebook"[3], "Mr M Osborne v. British Airways Plc"[4] and T-Mobile case[5], as well as the Ukrainian case of the cyberattack on the country's largest mobile operator, Kyivstar (as of June 2025, no court rulings are publicly available). Each case was analysed in terms of judicial decisions, regulatory findings, financial penalties, reputational consequences, and changes in corporate policies. This approach demonstrated how specific legal proceedings shape corporate governance practices, data protection policies, and communication strategies in times of crisis.

The comparative legal method enabled the examination of judicial approaches across different legal systems, particularly those of the USA, the United Kingdom, and Ukraine. This facilitated the identification of both commonalities and divergences in the interpretation of corporate liability for data breaches, which in turn allowed for the formulation of broader conclusions regarding the influence of judicial practice on commercial activity.

Using the formal legal method, the study examined the regulatory framework, in particular: the GDPR[6], the California Consumer Privacy Act[7], the Gramm-Leach-Bliley Act[8], and the Law of Ukraine "On the Protection of Personal Data"[9]. The research also included an analysis of annual data breach statistics in the USA (Statista, 2025). In addition, a prognostic approach was applied to formulate forecasts regarding future directions in corporate responsibility for personal data protection.

In exploring the impact of judicial precedents on data breaches in entrepreneurial activity, several theoretical methods were employed, including analysis, synthesis, induction, and deduction. The analytical method facilitated the examination of specific judicial decisions related to data breaches, enabling the identification of key legal approaches to determining corporate liability, characterising offences, and outlining typical consequences for busi nesses. The method of synthesis made it possible to combine information from diverse sources to construct a comprehensive understanding of the influence of case law on business activity. By applying induction, general conclusions were formulated from the analysis of individual cases, particularly concerning the growing stringency of data protection requirements. The deductive method, grounded in general principles of law and judicial practice, assisted in predicting potential risks and legal consequences for businesses in the event of breaches of data processing and storage norms.

[1] Judgement of the Employment Tribunal of the United Kingdom in Case No. 3301827/2020 "Mr L Beresford v. British Airways Plc". (2022, August). Retrieved from https://assets.publishing.service.gov.uk/media/63172208d3bf7f79312b7f95/Mr_L_Beresford_v_British_Airways_Plc_-_3301827-2020_-_Judgment.pdf.

[2] Final Judgement and and Permanent Injuction of the Superior Court of the State of California for the County of San Francisco Unlimited Jurisdiction in Case No. CGC-19-57780 "People of the State of California, v. Equifax Inc.". (2019, July). Retrieved from https://oag.ca.gov/system/files/attachments/press-docs/Equifax%20-%20Final%20approved%20%20judgment.pdf.

[3] Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief of the United States District Court for the District of Columbia in Case No. 19-cv-2184 "United States of America v. Facebook". (2019, July). Retrieved from https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf.

[4] Judgement of the Employment Tribunal of the United Kingdom in Case No. 3301841/2020 "Mr M Osborne v. British Airways Plc". (2021, October). Retrieved from https://assets.publishing.service.gov.uk/media/62388cf6e90e07799cd3de42/Mr_M_Osborne_v_British_Airways_PLC_3301841.2020_FMH_Reserved_Judgment.pdf.

[5] Stipulation and Order of the United States District Court For The District of Columbia in Case "United States of America et al., Plaintiffs, v. Deutsche Telekom AG, T-Mobile US, INC., Softbank Group Corp., and Sprint Corporation". (2019, July). Retrieved from https://www.justice.gov/d9/press-releases/attachments/2019/07/26/stipulation_and_order_0.pdf?utm.

[6] General Data Protection Regulation. (2016, May). Retrieved from https://gdpr-info.eu/.

[7] California Consumer Privacy Act. (2020, September). Retrieved from https://oag.ca.gov/system/files/initiatives/pdfs/19-0017%20%28Consumer%20Privacy%20%29.pdf.

[8] Gramm-Leach-Bliley Act. (1999, November). Retrieved from https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf.

[9] Law of Ukraine No. 2297-VI "On the Protection of Personal Data". (2010, June). Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17#Text.

Results

In the modern business environment, where information is one of the most valuable resources, the protection of personal and corporate data has become a vital component of risk management strategies. Companies must implement effective cybersecurity measures, control access to information, train employees, and respond swiftly to potential threats. Judicial precedents in data breach cases exert a significant influence on business, shaping the legal environment and setting standards for information protection. This influence is reflected in several key areas. Companies operating internationally are obliged to take into account precedents from different jurisdictions, which complicates business operations but simultaneously raises the overall level of data protection. Changes in judicial practice began with major cyber incidents in the early 2000s, when courts first confronted the challenge of assessing the harm caused by the leakage of millions of citizens' personal data (Tapkir, 2023). The difficulty lay in the fact that traditional methods of damage assessment proved inadequate for new types of offences, where potential harm might only manifest years after the initial incident.

In the business environment of the USA, there is a clear and persistent trend towards an increase both in the number of data breach incidents and in the scale of their impact (Fig. 1). This phenomenon is driven by several factors. The digitalisation of business processes leads to the accumulation of large volumes of data in electronic form, making companies more attractive targets for cybercriminals. At the same time, cyberattack techniques are becoming increasingly complex and sophisticated, enhancing their effectiveness and making detection more difficult. Insufficient investment in modern cybersecurity systems and reliance on outdated technologies create vulnerabilities that facilitate unauthorised access to protected information. In addition, the growing use of mobile devices and remote working formats complicates the control of information flows and increases the likelihood of unauthorised access. Equally significant are the strengthened legislative requirements for incident reporting, which enhance the transparency of statistical data. Furthermore, the globalisation of business processes and the complexity of interactions with external partners lead to a greater number of potential vulnerabilities in supply chains, which in turn heightens the risks of data breaches.

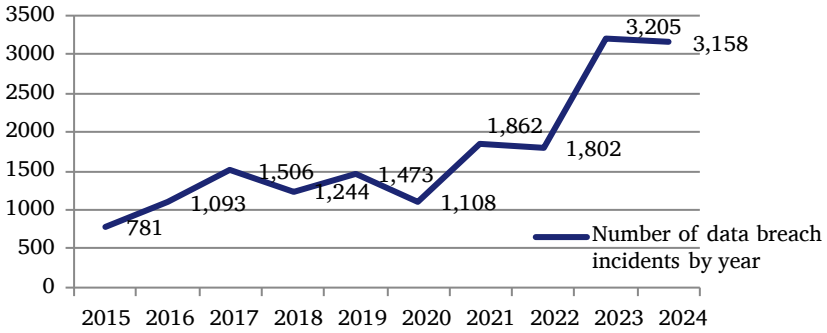

Figure 1. Annual number of data breaches and affected individuals in the USA
Source: compiled by the authors based on data from Statista (n.d.)

In 2015, 781 breaches were recorded, and by the following year, the number of incidents had risen to 1,093. This trend continued in 2017, reaching 1,506 incidents. However, in 2018, the figure declined to 1,244, which may indicate either improvements in data protection or a reduction in the reporting of such events. In 2019, the situation again intensified, with incidents increasing to 1,473, but in 2020 the number fell to 1,108. These fluctuations may be attributed both to changes in cybercriminal activity and to variations in corporate and governmental reporting policies. From 2021 onwards, the data show a sharp upward trend. In 2021, 1,862 incidents were recorded, while in 2022 the number fell slightly to 1,802. In 2023, however, the sharpest increase occurred, with 3,205 data breaches – almost twice as many as in the previous year. This surge may be linked to the widespread adoption of digital technologies, the growing popularity of remote work, and the intensification of hacker attacks. In 2024, a minor decrease was recorded, down to 3,158 incidents, although the overall level remained critically high. Thus, the data illustrate a general upward trend in data breach incidents over the past decade. This dynamic underline the increasing relevance of cybersecurity issues, the need to strengthen information protection measures, and the importance of raising awareness among organisations and users regarding the risks associated with unauthorised access to personal or corporate data.

The analysis of data breach statistics in the USA is of particular significance for understanding global trends in cybersecurity and has direct implications for businesses in Ukraine for several key reasons. The USA is a global leader in the digital economy

and serves as the home jurisdiction for many of the world's leading multinational technology corporations, including Google, Microsoft, Amazon, and Apple. This demonstrates that the American experience in cybersecurity reflects the most pressing challenges and the strategies adopted to address them in the field of data protection.

Data disclosure leads to direct financial losses, including regulatory fines, compensation payments to clients, legal costs, and reduced revenues. The average cost of a single incident can reach millions of dollars, particularly for large enterprises (Bhadouria, 2022). Often, the loss of customer trust exceeds the financial damage itself. Organisations lose existing clients, face difficulties in attracting new ones, and must allocate significant resources to restore their reputation. In addition, data breaches disrupt business processes, necessitate urgent IT system upgrades, and require the redesign of operational procedures, sometimes negatively affecting efficiency (Nejad, 2023). Companies also face investigations by regulatory authorities, class-action lawsuits from clients, and potential criminal inquiries targeting management, creating long-term legal risks. Data breaches reduce a company's competitiveness, as consumers and partners increasingly opt for more reliable alternatives in the market. Following such incidents, firms are compelled to substantially increase cybersecurity expenditures, which may lead to a reduction in investments in other areas of business development.

Case People of the State of California v. Equifax Inc."[1], which was considered from 2017, exemplifies how judicial decisions can radically transform an entire industry and establish new standards of corporate responsibility. Cybercriminals gained access to the private information of more than 147 million people, including social security numbers, driver's licence details, and financial data. The breach occurred due to a vulnerability in the Apache Struts web application, which Equifax failed to update in a timely manner despite the availability of a patch. This data breach resulted in an unprecedented fine of USD 700 million from the US Federal Trade Commission, as well as additional civil settlements exceeding USD 1.4 billion (Diniyatullah & Rindu, 2024).

The precedent-setting significance of this case lies in the creation of a new concept of corporate responsibility, which frames cybersecurity not merely as a technical procedure but as a strategic requirement of corporate management. During the proceedings, the courts determined that companies bear full responsibility for protecting personal data entrusted to them, regardless of technological complexity or external threats. Consequently, the principle of "due diligence in cyberspace" was established, requiring organisations to implement industry best practices and continually enhance their security systems. This case significantly transformed business approaches to cybersecurity due to substantial financial losses and reputational damage. The main changes included a marked increase in organisational investment in preventive cybersecurity measures, as the cost of threat prevention proved far lower than the cost of mitigating consequences.

The Facebook data scandal involved the unauthorised access to and use of users' personal data. The scandal led to numerous lawsuits against Facebook, including a class-action suit and investigations by regulatory authorities (Tiwari, 2022). In Case "United States of America v. Facebook"[2], new and significant standards of liability for the unlawful use of personal data for political purposes were established. The scandal, which arose from the use of data from 87 million Facebook users for targeted political advertising, resulted in a USD 5 billion fine and substantial changes in the company's corporate governance.

The Facebook-Cambridge Analytica scandal emerged from allegations of unauthorised collection of data from approximately 87 million Facebook users without their consent. These data were used for political micro-targeting, including during the US presidential elections and the Brexit referendum. Although technically, Facebook did not allow a data breach in the conventional sense – since users had granted permission for the third-party application to access their data – regulators viewed this as an abuse of user trust and insufficient oversight of third-party applications. Case "United States of America v. Facebook"[3] set a precedent for the personal liability of senior management for failures in data protection and established requirements for implementing the principle of "privacy by design" at all levels of corporate activity.

A particularly important aspect of this case was the establishment of the principle of transparency in the use of personal data, which obliges companies to provide users with complete information regarding the methods of collection, processing, and application of their data. During the proceedings of this case, it was established that complex and unclear

[1] Final Judgement and and Permanent Injuction of the Superior Court of the State of California for the County of San Francisco Unlimited Jurisdiction in Case No. CGC-19-57780 "People of the State of California, v. Equifax Inc.". (2019, July). Retrieved from https://oag.ca.gov/system/files/attachments/press-docs/Equifax%20-%20Final%20approved%20%20judgment.pdf.

[2] Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief of the United States District Court for the District of Columbia in Case No. 19-cv-2184 "United States of America v. Facebook". (2019, July). Retrieved from https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf.

[3] Ibidem, 2019.

privacy policies cannot serve as a legal basis for the processing of personal data. This led to a significant simplification and standardisation of user notification processes. Facebook was fined USD 5 billion by the US Federal Trade Commission, setting a new benchmark for liability in privacy violations. The ruling compelled technology companies to reassess their spending on data security and regulatory compliance. Moreover, the incident demonstrated how rapidly privacy breaches can undermine consumer trust and diminish brand value. As a result, new roles emerged within organisations, such as Chief Privacy Officers and AI Ethics Officers.

The American mobile operator T-Mobile experienced a series of data breaches, the largest of which occurred in 2021 and affected over 76 million users (McLymore & Bartz, 2020). Attackers gained access to names, addresses, dates of birth, social security numbers, and driver's licence information. Despite the company's assurances that security measures had been strengthened following previous incidents, this new breach triggered widespread criticism. The series of T-Mobile data breaches from 2018 to 2023 demonstrated the cumulative impact on the company's reputation and the financial losses resulting from repeated security incidents. The uniqueness of this case lies in its role in establishing industry standards for the US telecommunications sector, which is considered critical infrastructure. One of the key measures was the appointment of a mandatory Chief Information Security Officer, required to report regularly to the board of directors on the state of security and the effectiveness of implemented measures. The company was obliged to adopt a "Zero Trust" architecture, which demands continuous verification of every access request, regardless of the user's or system's location. In addition, the organisation was required to implement phishing-resistant multi-factor authentication and modern vulnerability management systems, including regular scanning, patching, and security monitoring. Another important requirement was the minimisation of personal data collection and compliance with policies for data deletion or anonymisation when retention was not justified. The company came under enhanced oversight by the Federal Communications Commission and was fined USD 60 million. This demonstrated the determination of American regulators to enforce strict measures for systemic cybersecurity failures. Large class-action lawsuits from over 76 million affected consumers exemplified the scale of compensation in the telecommunications sector.

In European Union countries, judicial precedents in the field of personal data breaches have become an important factor directly affecting business operations. As of 2023-2025, the number of data breach incidents in Europe remains consistently high, indicating increasing cyber risks for businesses and critical infrastructure. According to the European Union Agency for Cybersecurity (2024), between mid-2022 and mid-2023, more than 11,000 significant incidents were recorded across EU countries, of which approximately 41% resulted in personal data breaches. In 2024, the 15 leading European countries reported over 130,000 data protection violations – an average of more than 356 incidents per day. The highest numbers were recorded in the Netherlands (33,471 incidents), followed by Germany (27,829), Spain (2,989), and Italy (2,400); increases compared with 2023 were 65%, 47%, and 42% respectively.

These changes were driven by the implementation of the GDPR[1], which introduced new liability criteria and set a precedent for the extraterritorial application of national regulations. In particular, the regulation established the principle of accountability, requiring organisations not only to comply with data protection rules but also to demonstrate compliance through appropriate documentation and process verification. The GDPR emphasises transparency in the use of personal information, obliging companies to inform data subjects of the purposes, scope, and duration of processing, as well as any potential third-party access to that information. A further standard requires notification of data security breaches within 72 hours if the incident could threaten the rights and freedoms of individuals. This fundamentally changed the approach to corporate responsibility: shifting from mere formal compliance to active, documented accountability for protecting human rights in the context of personal data processing. The GDPR not only increased potential fines to up to 4% of a company's annual global turnover but also introduced the concept of "accountability", requiring organisations to demonstrate proactive measures to safeguard personal data (Tikkinen-Piri *et al.*, 2018).

Case "Mr L Beresford v. British Airways Plc"[2] and Case "Mr M Osborne v. British Airways Plc"[3] illustrated the practical application of the GDPR and established European standards of liability for data breaches. Following a 2018 cyberattack that

[1] General Data Protection Regulation. (2016, May). Retrieved from https://gdpr-info.eu/.

[2] Judgement of the Employment Tribunal of the United Kingdom in Case No. 3301827/2020 "Mr L Beresford v. British Airways Plc". (2022, August). Retrieved from https://assets.publishing.service.gov.uk/media/63172208d3bf7f79312b7f95/Mr_L_Beresford_v_British_Airways_Plc_-_3301827-2020_-_Judgment.pdf.

[3] Judgement of the Employment Tribunal of the United Kingdom in Case No. 3301841/2020 "Mr M Osborne v. British Airways Plc". (2021, October). Retrieved from https://assets.publishing.service.gov.uk/media/62388cf6e90e07799cd3de42/Mr_M_Osborne_v_British_Airways_PLC_3301841.2020_FMH_Reserved_Judgment.pdf.

compromised the personal data of 500,000 airline customers, a thorough investigation was conducted by the UK Information Commissioner's Office, which imposed a fine of GBP 20 million. The original fine of 183 million GBP was reduced in consideration of the economic impact of the COVID-19 pandemic (Voss, 2021).

The investigation concluded that the company had failed to implement appropriate technical and organisational measures as required under the GDPR. In 2020, the UK Information Commissioner's Office therefore imposed a 20 million GBP fine on British Airways. The court case drew attention to the necessity of continuous testing of digital infrastructure security, which became a key lesson for other industry players. The precedent set by this case lies in establishing clear standards for technical and organisational measures to protect personal data. The rulings in Case "Mr L Beresford v. British Airways Plc"[1] and Case "Mr M Osborne v. British Airways Plc"[2] defined detailed requirements for cybersecurity monitoring systems, incident detection and response procedures, and reporting obligations to regulators and affected individuals. Specifically, companies must have documented and tested incident response procedures that include the designation of responsible personnel, step-by-step action plans in the event of a security breach, and deadlines for each stage of the response. Particular emphasis was placed on the obligation to notify: under the GDPR[3], organisations must inform supervisory authorities of a detected breach within 72 hours of its discovery. Furthermore, if an incident poses a significant risk to the rights and freedoms of individuals, the company is also required to notify affected persons promptly, clearly, and with recommendations for mitigating risks.

Given that Ukraine belongs to a continental legal system, where precedent does not have the force of law, the role of judicial practice is gradually increasing (Slotwinska, 2015). In particular, decisions of the Supreme Court and appellate courts are increasingly used as reference points for interpreting legislation. In the field of personal data breaches, courts are increasingly required not only to apply the provisions of the Law of Ukraine No. 2297-VI[4] but also to interpret them in the context of new technological realities, taking into account European practice, including the provisions of the GDPR.

One consequence of personal data breaches for businesses in Ukraine is both public-law and private-law liability. This includes compensating individuals whose data has been exposed. In addition, the handling of cases involving state authorities imposing penalties for data breaches or inadequate protection helps to establish standards for responsible corporate behaviour. Court precedents indicate that judges consider how effectively a company has implemented security policies, conducted internal audits, and informed users about incidents. This encourages businesses to invest in cybersecurity, staff training, and legal support to ensure regulatory compliance.

Unlike in the USA and the EU, Ukraine lacks a significant number of high-profile court cases relating to personal data breaches. This is explained by several factors: relatively low fines for violations, insufficient enforcement of legislation, shortcomings in the regulatory framework, and low public awareness of individual rights. One of the most significant business-related data breaches was the cyberattack on Kyivstar in December 2023. As of June 2025, no court rulings regarding the Kyivstar attack are publicly available. The case remains under investigation by the SBU, with materials to be subsequently submitted to the International Criminal Court, as the suspects are Russian nationals outside Ukraine's jurisdiction. Considered the largest incident in the history of Ukraine's telecommunications sector, the attack highlighted the devastating impact that cyberattacks and data breaches can have on business operations. In terms of scale, the attack was unprecedented in the Ukrainian context. Mobile and internet services for Kyivstar subscribers across the country were completely disrupted, and users were unable to connect to other networks under domestic roaming agreements. The technical damage was catastrophic: numerous servers were destroyed, large volumes of data were erased, and overall, the attack compromised approximately 40% of Kyivstar's infrastructure.

The attack aimed both to inflict psychological pressure and to obtain intelligence information. The December cyberattacks on Kyivstar caused losses amounting to UAH 3.6 billion, covering only the customer compensation programme (Khramov & Opirskyy, 2024). These figures do not include the costs of fully restoring the infrastructure, which required substantial investment in new equipment and

[1] Judgement of the Employment Tribunal of the United Kingdom in Case No. 3301827/2020 "Mr L Beresford v. British Airways Plc". (2022, August). Retrieved from https://assets.publishing.service.gov.uk/media/63172208d3bf7f79312b7f95/Mr_L_Beresford_v_British_Airways_Plc_-_3301827-2020_-_Judgment.pdf.

[2] Judgement of the Employment Tribunal of the United Kingdom in Case No. 3301841/2020 "Mr M Osborne v. British Airways Plc". (2021, October). Retrieved from https://assets.publishing.service.gov.uk/media/62388cf6e90e07799cd3de42/Mr_M_Osborne_v_British_Airways_PLC_3301841.2020_FMH_Reserved_Judgment.pdf.

[3] General Data Protection Regulation. (2016, May). Retrieved from https://gdpr-info.eu/.

[4] Law of Ukraine No. 2297-VI "On the Protection of Personal Data". (2010, June). Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17#Text.

security systems. The company was compelled not only to rebuild the damaged infrastructure but also to fundamentally revise its approach to cybersecurity. This required substantial additional investment and a restructuring of the 2024 budget, with millions of dollars allocated to cybersecurity programmes. The reputational consequences proved to be as severe as the financial losses.

For the Ukrainian business environment, the Kyivstar case served as a catalyst for reassessing the importance of investing in cybersecurity as a critical component of corporate strategy, rather than merely a technical necessity. Analysis of judicial precedents shows that court decisions arising from such incidents not only imposed significant fines but also compelled companies to implement stricter cybersecurity measures. In response, organisations have been forced to review their internal policies and processes, as well as invest in advanced technologies and employee training. The results are summarised in Table 1.

Table 1. Impact of data breach causes on judicial precedents and business outcomes in high-profile cases

Case	Causes of data breaches	Judicial precedents	Impact on business operations
Equifax[1]	Vulnerability in a web application; insufficient protection	Court ruling (2017): 700 million USD fine for negligence in protecting the personal data of 147 million users	Large fines; increased cybersecurity requirements; loss of consumer trust; strengthened regulation in the USA
Facebook-Cambridge Analytica[2]	Unauthorised third-party access to user data	Court proceedings in the USA and EU (2018-2020): fines for violations of the GDPR[3] and privacy laws	Changes to privacy policies; additional control over data access; reputational damage; stricter legislative requirements
British Airways[4]	Cyber-attack exploiting website vulnerability	UK Information Commissioner's Office ruling (2020): 20 million GBP fine for GDPR violations	Fines; investment in IT infrastructure protection; strengthening of internal security procedures; loss of customer trust
T-Mobile[5]	Data compromise via phishing and weak access controls	Legal claims (2021): fines and compensation to victims for the loss of millions of clients' data	Costs of compensation; reputational damage; strengthened security policies; employee training; investment in protective systems
Kyivstar	Large-scale hacker attack (December 2023); destruction of IT infrastructure; potential leak of personal and technical data	Investigations ongoing as of 2025; precedent-setting case on telecom companies' cybersecurity responsibilities in Ukraine	Disruption of mobile and internet services; erosion of customer trust; criticism of cybersecurity by authorities; increased requirements for telecom sector resilience

Source: compiled by the authors

Judicial precedents in the field of data breaches have had a significant impact across multiple sectors of the economy, prompting changes not only in technical methods of information protection but also in broader approaches to corporate governance. In the financial sector, the Equifax data breach, which involved the credit reports of millions of individuals, served as a catalyst for a substantial review of internal policies within banks, credit bureaus, and insurance companies. Financial institutions now view the protection of personal information not merely as part of IT infrastructure but as a critical element of systemic risk, comparable to liquidity and solvency considerations. This precedent triggered a wave of legislative changes. In the United States, the 2020 California Consumer Privacy Act[6] played a significant role, granting users new rights to control their personal data. Additionally, the Safeguards Rule

[1] Final Judgement and and Permanent Injuction of the Superior Court of the State of California for the County of San Francisco Unlimited Jurisdiction in Case No. CGC-19-57780 "People of the State of California, v. Equifax Inc.". (2019, July). Retrieved from https://oag.ca.gov/system/files/attachments/press-docs/Equifax%20-%20Final%20approved%20%20judgment.pdf.

[2] Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief of the United States District Court for the District of Columbia in Case No. 19-cv-2184 "United States of America v. Facebook". (2019, July). Retrieved from https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf.

[3] General Data Protection Regulation. (2016, May). Retrieved from https://gdpr-info.eu/.

[4] Judgement of the Employment Tribunal of the United Kingdom in Case No. 3301827/2020 "Mr L Beresford v. British Airways Plc". (2022, August). Retrieved from https://assets.publishing.service.gov.uk/media/63172208d3bf7f79312b7f95/Mr_L_Beresford_v_British_Airways_Plc_-_3301827-2020_-_Judgment.pdf.

[5] Stipulation and Order of the United States District Court For The District of Columbia in Case "United States of America et al., Plaintiffs, v. Deutsche Telekom AG, T-Mobile US, INC., Softbank Group Corp., and Sprint Corporation". (2019, July). Retrieved from https://www.justice.gov/d9/press-releases/attachments/2019/07/26/stipulation_and_order_0.pdf?utm.

[6] California Consumer Privacy Act. (2020, September). Retrieved from https://oag.ca.gov/system/files/initiatives/pdfs/19-0017%20%28Consumer%20Privacy%20%29.pdf.

under the Gramm-Leach-Bliley Act[1] was modernised, strengthening security requirements for financial institutions, particularly in areas such as multi-factor authentication and regular audits. In Europe, national banks and regulators began requiring periodic security audits as part of operational resilience standards. Banks also increasingly invested in cyber insurance, while internal departments were granted significantly broader powers (Bond *et al.*, 2022). Consequently, data breach precedents in the financial sector initiated a long-term transformation of risk management practices and technological strategies within institutions.

In the technology sector, particularly among companies handling large volumes of data, the Facebook-Cambridge Analytica scandal had a profound impact[2]. The incident demonstrated that even formally granted consent is insufficient justification for large-scale use of personal data for political or commercial purposes. Following this event, Facebook and other tech giants began implementing new product design approaches emphasising "privacy by design", which integrates data protection measures from the earliest stages of functionality development. At the same time, attention to transparency increased: companies are now required to clearly inform users about the purposes of data processing, storage methods, retention periods, and options for withdrawing consent. Court rulings in this area have strengthened the accountability of executives, particularly at the board level, where directors are now required to report on compliance with ethical and legal standards in data processing.

In the aviation sector, the British Airways case demonstrated that companies handling large volumes of customer data must not only implement protective measures but also ensure their effective operation in real time. Following the breach of its booking system, which resulted in the leakage of financial and personal information, regulators in the United Kingdom and Europe emphasised that even minor vulnerabilities in the customer interface can lead to substantial fines. Airlines were compelled to upgrade their sales systems, commission independent security audits, and establish internal incident response teams.

Data breach precedents have become a catalyst for a significant reassessment of corporate strategies and business models, particularly for firms involved in the collection and processing of large volumes of personal data. The principle of data minimisation has emerged as a key element of corporate strategy, prompting organisations to re-evaluate the necessity of collecting and storing personal information in terms of both business value and legal risk. Companies are increasingly adopting advanced pseudonymisation and anonymisation technologies, which preserve the analytical value of information while significantly reducing risks in the event of a potential data breach. Automated data lifecycle management systems ensure the deletion of personal information once it is no longer operationally necessary, thereby reducing the volume of data at risk of compromise.

In the context of Ukraine's European integration trajectory, it is essential to align national legislation with the requirements of the General Data Protection Regulation. In this regard, Ukrainian court decisions in cases related to data breaches are increasingly significant, as they establish a legal precedent for corporate responsibility in ensuring information security. This will foster a legal culture within the business environment, where digital ethics and data protection become integral components of corporate social responsibility strategies.

Discussion

The findings of this study indicate that court precedents concerning personal data breaches have a substantial impact on business, particularly regarding reputational risks, financial losses, and growing cybersecurity obligations.

A study conducted by A. Alessi *et al.* (2021) emphasise that the implementation of the General Data Protection Regulation and related court rulings have significantly transformed corporate governance practices. As a result, the principle of "privacy by design" has evolved from a recommendation to a mandatory requirement codified in both legislation and judicial practice. As noted by A. Singh *et al.* (2020), these changes have led to the creation of new positions within corporate hierarchies, such as Chief Privacy Officer and Data Protection Officer, reflecting a structural reorganisation of company business processes. The analysis of Case "United States of America v. Facebook"[3], significantly complements the conclusions of this study by illustrating the specific legal mechanisms underpinning this transformation. The court rulings in the Facebook case established a precedent for the personal liability of executives

[1] Gramm-Leach-Bliley Act. (1999, November). Retrieved from https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf.

[2] Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief of the United States District Court for the District of Columbia in Case No. 19-cv-2184 "United States of America v. Facebook". (2019, July). Retrieved from https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf.

[3] Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief of the United States District Court for the District of Columbia in Case No. 19-cv-2184 "United States of America v. Facebook". (2019, July). Retrieved from https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf.

for breaches of data protection standards, creating a strong economic incentive for companies to institutionalise data protection functions through the creation of specialised roles. The present study, within the framework of the Facebook case analysis, demonstrates that this case established modern standards of accountability for the misuse of personal information, particularly for political purposes. The rulings set a precedent for the personal responsibility of executives in data protection breaches and outlined requirements for implementing the principle of "privacy by design" at all levels of business operations.

Data breaches have substantial financial consequences for companies, resulting in direct losses that may include fines, compensation payments to affected clients, legal expenses, and decreased revenue due to lost consumer trust. Data breaches have caused significant financial damage: Equifax paid over USD 700 million, Facebook suffered losses due to the Cambridge Analytica scandal, British Airways was fined more than USD 200 million, T-Mobile experienced widespread losses, and Kyivstar became the victim of a large-scale cyberattack in 2023 with serious repercussions. Research conducted by S. Romanosky (2016) highlights considerable variations in the estimation of standard costs associated with data breaches.

The analysis of court rulings in Case "People of the State of California v. Equifax Inc."[1], and case "Mr L Beresford v. British Airways Plc"[2], and Case "Mr M Osborne v. British Airways Plc"[3], reveals certain divergences from the conclusions of J. Xu *et al.* (2024) regarding the mechanisms through which judicial practice influences corporate accountability. While J. Xu *et al.* argue that court decisions primarily establish new standards of responsibility through the creation of technical benchmarks, the findings of this study suggest a more nuanced picture. The analysis of the Equifax case indicates that court rulings primarily affect the transformation of organisational culture and managerial processes, rather than merely technical aspects of cybersecurity. This contrasts with the earlier analysis, as it demonstrates that the principle of "due diligence in cyberspace" entails the systematic integration of cybersecurity into strategic planning, extending beyond a purely technical approach. Assertions by A. Paraskevas (2022) that the British Airways case emphasised the need for technical security measures appear debatable, since this study shows that the primary issue was not a lack of technical solutions but rather insufficient corporate oversight and strategic risk management. Conversely, the conclusions of J. Ebuzor (2024) regarding inadequate oversight of digital system security are entirely appropriate, as they align with the findings of this research on systemic shortcomings in British Airways' organisational processes.

According to the findings of this study, judicial precedents have contributed to the development of entirely new approaches to cyber risk management, distinguished by the adoption of advanced technologies. In particular, companies have begun to employ continuous threat-monitoring systems based on artificial intelligence and machine learning to anticipate potential attacks. A. Tauseef (2023) emphasises that legal risks have indeed driven the implementation of automated cybersecurity systems within organisations. This has become especially relevant following the introduction of the General Data Protection Regulation in Europe and similar regulations in other countries. Fines can reach millions of euros or a percentage of annual revenue, making financial investment in preventive measures economically advantageous. Automated threat-detection systems enable companies to demonstrate "due diligence" to regulators, promptly identify and document incidents, respond to threats automatically without human intervention, and maintain detailed logs for potential legal proceedings.

The present study shows that losses in customer trust often exceed immediate financial damages. Companies not only lose existing clients but also face difficulties in attracting new ones and are compelled to allocate substantial resources to restoring their reputation. Loss of consumer confidence due to data breaches can have more severe consequences than direct financial losses, as it leads to long-term negative effects such as client attrition, reduced profitability, and the need for significant capital expenditure to rebuild corporate reputation. In a study conducted by M. Tripathi & A. Mukhopadhyay (2020), 131 cases of data breaches in the USA were analysed, revealing that announcements of such breaches negatively affect companies' market value. Average financial losses amounted to USD 229 million in 2012, USD 241 million in 2013, and USD 108 million in 2014. These figures include not only direct costs

[1] Final Judgement and and Permanent Injuction of the Superior Court of the State of California for the County of San Francisco Unlimited Jurisdiction in Case No. CGC-19-57780 "People of the State of California, v. Equifax Inc.". (2019, July). Retrieved from https://oag.ca.gov/system/files/attachments/press-docs/Equifax%20-%20Final%20approved%20%20judgment.pdf.

[2] Judgement of the Employment Tribunal of the United Kingdom in Case No. 3301827/2020 "Mr L Beresford v. British Airways Plc". (2022, August). Retrieved from https://assets.publishing.service.gov.uk/media/63172208d3bf7f79312b7f95/Mr_L_Beresford_v_British_Airways_Plc_-_3301827-2020_-_Judgment.pdf.

[3] Judgement of the Employment Tribunal of the United Kingdom in Case No. 3301841/2020 "Mr M Osborne v. British Airways Plc". (2021, October). Retrieved from https://assets.publishing.service.gov.uk/media/62388cf6e90e07799cd3de42/Mr_M_Osborne_v_British_Airways_PLC_3301841.2020_FMH_Reserved_Judgment.pdf.

but also indirect consequences, such as reduced customer trust and reputational damage. Furthermore, according to the Ponemon Institute (2024), 65% of consumers lose confidence in a company following a data breach, while 27% cease doing business with it. This confirms that the loss of customer trust can have long-lasting effects that exceed immediate financial losses.

The study also found that data breaches compel companies to significantly increase investment in cybersecurity. This involves implementing advanced threat-detection technologies, upgrading existing infrastructure, and strengthening access controls. Consequently, these unforeseen expenses create additional financial obligations, particularly for small and medium-sized enterprises, often necessitating the reallocation of resources. Research by C.Y. Jeong *et al.* (2024) corroborates that firms substantially increase investment in information security following major data breaches.

An analysis of case law concerning data breaches highlights its significant and multifaceted impact on commercial organisations. Legal precedents establish new standards of corporate responsibility, prompting companies to review their methods of protecting personal data and to strengthen cybersecurity measures. Court rulings demonstrate the high stakes of compensation for damages, compelling businesses to set aside significant reserves to cover potential costs and to invest in preventative security. Overall, judicial precedents in the field of data breaches foster the development of business practices oriented towards greater accountability and transparency, contributing to the emergence of a new culture of corporate data governance.

■ Conclusions

An examination of case law concerning data breaches has revealed that the protection of personal information is becoming increasingly important for business organisations. Well-known cases such as Equifax, Facebook-Cambridge Analytica, British Airways, and T-Mobile not only resulted in substantial economic losses for corporations but also established new legal standards for businesses regarding the protection of personal data. These incidents created precedents that influenced judicial practice, regulatory approaches, and corporate strategies in the context of digital security.

It was found that court decisions in the Equifax, Facebook-Cambridge Analytica, British Airways, and T-Mobile cases created new legal benchmarks that transformed the understanding of corporate responsibility for personal data protection. Analysis of these precedents indicates that courts increasingly interpret technical incompetence as legal negligence, with corresponding financial and reputational consequences. The findings also show that the Facebook-Cambridge Analytica case contributed to a global discussion on digital ethics and the principle of accountability, while the Equifax and British Airways cases emphasised the critical importance of timely security system updates. The analysis revealed a clear trend towards the institutionalisation of the principles of "privacy by design" and "Zero Trust" as mandatory elements of corporate strategy. The findings indicate that judicial practice has acted as a catalyst for the creation of new managerial roles, such as Chief Privacy Officer and Data Protection Officer, reflecting a structural transformation in corporate governance.

In summary, the results suggest that court precedents not only establish standards of accountability but also shape a new paradigm of corporate governance, in which cybersecurity is integrated into strategic planning at all organisational levels. Conceptually, this indicates a shift from a reactive to a proactive approach to cyber risk management, where legal requirements serve as drivers of innovation in corporate practice. The analysis underscores that modern organisations must regard the protection of personal data not merely as a technical task, but as a strategic asset that determines competitiveness and long-term business resilience.

The study confirms that investments in cybersecurity and regulatory compliance should not be seen as expenses but rather as strategic capital allocations essential for maintaining stable business operations. Companies that embrace this perspective gain competitive advantages through increased consumer trust and reduced operational risks. A key limitation of this research is the confidentiality of many court cases, which significantly complicates the collection of comprehensive information on incident details. Future research prospects include a thorough analysis of the impact of artificial intelligence on the development of cyber threats and legal regulation, an evaluation of the effectiveness of international cooperation in combating cybercrime, and the study of the implementation of cybersecurity principles across different sectors.

■ Acknowledgements

None.

■ Funding

The study was not funded.

■ Conflict of Interest

None.

References

[1] Alessi, A., Ciccarelli, G., Cipolli, L., Guidotti, L., Marsano, A., & Hanganu, A. (2021). *Privacy by design and by default in software development in order to prevent unlawful processing of personal data. Privacy certifications impact on software development and liabilities*. Retrieved from https://surl.li/fmkrem.

[2] Bem, M., & Horodysky, I. (2019). Liability for violation of personal data protection legislation: Problems of compliance of Ukrainian legislation with the requirements of the European Union regulation on the protection of personal data (GDPR). *Law of Ukraine*, 2, 237-255.

[3] Bernaziuk, O.O. (2023). Judicial precedent in the legal system of Ukraine: Modern approaches to the definition of the concept. *Uzhhorod National University Herald. Series: Law*, 1(80), 403-410. doi: 10.24144/2307-3322.2023.80.1.60.

[4] Bhadouria, A.S. (2022). Study of: Impact of malicious attacks and data breach on the growth and performance of the company and few of the world's biggest data breaches. *International Journal of Scientific and Research Publications*, 10(10). doi: 10.29322/IJSRP.X.2022.p091095.

[5] Bond, M., Human, K., & Kwon, N. (2022). *Analysis and implications for Equifax data breach*. Retrieved from https://cs.ucf.edu/~mohaisen/doc/teaching/cap5150/fall2022/cap5150-proj2.pdf.

[6] Diniyatullah, L., & Rindu, K.B. (2024). Crisis management and recovery strategies after a data leak: Equifax case study. *Journal of Information System and Technology*, 1(2), 76-81.

[7] Dumanska, I.Y., Guseva, O.Y., Kazarova, I.O., Gorodetskyy, M., Melnichuk, L.V., & Saienko, V.H. (2022). Personal data protection policy impact on the company development. *Transactions on Environment and Development*, 18, 232-246. doi: 10.37394/232015.2022.18.25.

[8] Ebuzor, J. (2024). Understanding customer perception of cyber attacks: Impact on trust and security. In P. Thealla, V. Nadda, S. Dadwal, L. Oztosun & G. Cantafio (Eds.), *Corporate cybersecurity in the aviation, tourism, and hospitality sector* (pp. 83-111). London: IGI Global. doi: 10.4018/979-8-3693-2715-9.ch005.

[9] European Union Agency for Cybersecurity. (2024). *ENISA threat landscape*. Iraclion: ENISA. doi: 10.2824/0710888.

[10] Jeong, C.Y., Lee S.-Y., & Lim, J.-H. (2024). Information security breaches and IT security investments: Impacts on competitors. *Information & Management*, 56(5), 681-695. doi: 10.1016/j.im.2018.11.003.

[11] Khramov, S., & Opirskyy, I. (2024). Analysis of the current state of cyberattacks in Ukraine during the war. *Ukrainian Information Security Research Journal*, 26(1), 214-222. doi: 10.18372/2410-7840.26.18842.

[12] Kotenko, M., Karagioz, R., Sopilko, I., Andrusiv, V., & Yermakova, H. (2025). Personal data protection in Ukraine via the prism of European judicial institutions' practise. *Estudios en Derecho a la Información*, 10(19), 147-170. doi: 10.22201/iij.25940082e.2025.19.19032.

[13] McLymore, A., & Bartz, D. (2020). *T-Mobile-Sprint merger wins approval from U.S. judge*. Retrieved from https://www.reuters.com/article/technology/t-mobile-sprint-merger-wins-approval-from-us-judge-idUSKBN2042MG/.

[14] Nejad, L.P. (2023). Mitigating data loss and its impact on modern software engineering: A case study approach. *Journal of Applied Intelligent Systems & Information Sciences*, 4(2), 52-60. doi: 10.22034/JAISIS.2023.418932.1072.

[15] Nekit, K. (2020). Personal data and industrial data as objects of ownership: Evaluation of perspectives. *Journal of Civil Studies*, 36, 57-64. doi: 10.32837/chc.v0i36.202.

[16] Paraskevas, A. (2022). Cybersecurity in travel and tourism: A risk-based approach. In Zh. Xiang, M. Fuchs, U. Gretzel & W. Höpken (Eds.), *Handbook of e-tourism* (pp. 1605-1628). Cham: Springer. doi: 10.1007/978-3-030-48652-5 100.

[17] Pokhylenko, I. (2023). Legal regulation of personal data protection. *Legal Bulletin "Air and Space Law"*, 4(69), 94-99. doi: 10.18372/2307-9061.69.18322.

[18] Ponemon Institute. (2024). *Beyond the balance sheet: The real costs of data breaches in 2024*. Retrieved from https://f12.net/blog/beyond-the-balance-sheet-the-real-costs-of-data-breaches-in-2024/?utm.

[19] Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, 2(2), 121-135. doi: 10.1093/cybsec/tyw001.

[20] Schäfer, F., Gebauer, H., Gröger, C., Gassmann, O., & Wortmann, F. (2023). Data-driven business and data privacy: Challenges and measures for product-based companies. *Business Horizons*, 66(4), 493-504. doi: 10.1016/j.bushor.2022.10.002.

[21] Singh, A., Klarner, P., & Hess, T. (2020). How do chief digital officers pursue digital transformation activities? The role of organization design parameters. *Long Range Planning*, 53(3), article number 101890. doi: 10.1016/j.lrp.2019.07.001.

[22] Slotwinska, N. (2015). Theoretical and legal approaches to understanding judicial precedent as a component of judicial practice. *National Law Journal: Theory and Practice*, 15(5/1), 18-21.
[23] Sopilko, I., & Zubko, E. (2024). Data breach and data leak: Legal aspect. *Journal of the Kyiv University of Law*, 3, 62-68. doi: 10.36695/2219-5521.3.2024.7.
[24] Statista. (n.d.). *Annual number of data compromises and individuals impacted in the United States from 2005 to 2024*. Retrieved from https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.
[25] Tapkir, R.S. (2023). Privacy in Peril: Rise of data breaches in the entertainment and media industries. *Jus Corpus Law Journal*, 4, 443-465.
[26] Tauseef, A. (2023). *Database technologies in AI: Transforming cybersecurity with automated threat detection systems*. doi: 10.13140/RG.2.2.33122.54727.
[27] Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, 34(1), 134-153. doi: 10.1016/j.clsr.2017.05.015.
[28] Tiwari, P. (2022). Misuse of personal data by social media giants. *Jus Corpus Law Journal*, 3, 1041-1064.
[29] Tripathi, M., & Mukhopadhyay, A. (2020). Financial loss due to a data privacy breach: An empirical analysis. *Journal of Organizational Computing and Electronic Commerce*, 30(4), 381-400. doi: 10.1080/10919392.2020.1818521.
[30] Voss, W.G. (2021). Airline commercial use of EU personal data in the context of the GDPR, British Airways and Schrems II. *Colorado Technology Law Journal*, 19(2), 377-428.
[31] Xu, J., Yue, W.T., Leung, A.C., & Su, Q. (2024). Focusing on the fundamentals? An investigation of the relationship between corporate social irresponsibility and data breach risk. *Decision Support Systems*, 182, article number 114252. doi: 10.1016/j.dss.2024.114252.
[32] Zadereyko, O., Trofymenko, O., Prokop, Y., Loginova, N., Dyka, A., & Kukharenko, S. (2022). Research of potential data leaks in information and communication systems. *Radioelectronic and Computer Systems*, 104(4), 64-84. doi: 10.32620/reks.2022.4.05.

Вплив судових прецедентів у сфері витоку даних на підприємницьку діяльність: актуальні кейси

Ігор Руденко
Магістр права
Національний юридичний університет імені Ярослава Мудрого
61024, вул. Григорія Сковороди, 77, м. Харків, Україна
https://orcid.org/0009-0008-3582-3951

Ольга Хорольська
Магістр права
Національний юридичний університет імені Ярослава Мудрого
61024, вул. Григорія Сковороди, 77, м. Харків, Україна
https://orcid.org/0009-0004-9853-2378

Марія Турчіна
Кандидат юридичних наук
Національний юридичний університет імені Ярослава Мудрого
61024, вул. Григорія Сковороди, 77, м. Харків, Україна
https://orcid.org/0000-0002-1486-1122

■ **Анотація.** Метою дослідження було вивчення впливу судових прецедентів у справах про витік персональних і корпоративних даних на формування правової практики та стратегії ведення підприємницької діяльності. У межах дослідження було здійснено аналіз ключових судових справ, що дало змогу визначити, як ці випадки вплинули на юридичну відповідальність і поведінку компаній. Дослідження пов'язане з такими справами, як Equifax, Facebook-Cambridge Analytica, British Airways, T-Mobile та мобільного оператора «Київстар». Судові рішення в цих справах не лише передбачають накладення штрафів, а й встановлюють нові принципи корпоративної етики, що потребує від компаній системного підходу до захисту персональних даних, прозорості у взаємодії з користувачами та покращення внутрішньої правової культури. Кількість інцидентів продовжує зростати: з 2024 року фіксується на 25 % більше випадків витоку даних порівняно з попередніми роками. Це засвідчує, що витоки даних вже не розглядаються суто як технічні питання – вони стали юридично важливими подіями, що мають значний економічний і регуляторний вплив. У відповідь на це підприємства вимушені переосмислювати власні стратегії, упроваджувати нові політики захисту даних і враховувати можливі правові ризики в управлінні ризиками. Практична значущість питань полягає в тому, що аналіз основних випадків дозволяє прогнозувати наслідки можливих витоків даних, оцінювати рівень юридичних ризиків та розробляти дієві стратегії відповідальності й профілактики

■ **Ключові слова:** кібербезпека; персональні дані; правове регулювання; інформаційна безпека; захист інформації; правопорушення; відшкодування збитків