International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

CYBERSECURITY, DATA BREACHES, AND THE RIGHT TO PRIVACY: A CASE STUDY APPROACH IN INDIAN BANKS

[1]Shamrao Jagannath Patil, [2]Dr Namdev Jadhav
[1]Asst professor, Dayanand college of law Latur, Maharashtra, India
[2]Associate professor, Dayanand College of Law, Latur, Maharashtra, India

Introduction:

In the digital era, banks in India hold vast amounts of personal and financial information, making them prime targets for cyberattacks and data breaches. Ensuring the security of this sensitive data is not only critical for protecting consumers from fraud and identity theft, but it is also now a matter of upholding a fundamental right to privacy. The Supreme Court of India's Puttaswamy judgment (2017) affirmed privacy as a fundamental right, raising the stakes for how institutions handle personal data. Consequently, Indian banks must navigate a complex landscape of cybersecurity threats and evolving legal obligations. This paper provides an in-depth analysis of cybersecurity and data breaches in Indian banks through the lens of privacy rights. It examines the legal and regulatory framework – from the Information Technology Act and Reserve Bank of India (RBI) guidelines to recent data protection legislation – and analyzes case studies of major security incidents. The discussion highlights how these incidents impacted customer privacy and what legal or regulatory actions followed, and it evaluates the role of banks and regulators in strengthening data protection. Finally, the paper offers critical analysis of enforcement gaps and recommendations for improving privacy and cybersecurity in India's banking sector.

Right to Privacy in India: The Puttaswamy Judgment

It is impossible to divorce the idea of the right to privacy from the current conversation about data breaches in India. A nine-judge Supreme Court bench unanimously ruled in Justice K.S. Puttaswamy (Retd.) v. Union of India that the right to privacy is safeguarded under Article 21 of the Constitution as an inherent component of the fundamental rights to life and liberty. Overturning previous rules, this historic decision—often known to as the Right to Privacy judgment—established that Indians have a basic right to privacy, subject to reasonable limitations. Importantly, the ruling acknowledged that privacy has several dimensions, including informational privacy, which is closely related to safeguarding personal information. The Court acknowledged that in the age of digital data, the protection of personal information is an essential condition of privacy.

The Puttaswamy decision had a profound impact on India's legislative and policy agenda. It prompted the Union government to expedite efforts toward a comprehensive data protection law. Soon after the judgment, an expert committee chaired by Justice B.N. Srikrishna was established to propose a data protection framework. This eventually led to draft Personal Data Protection Bills (2018 and 2019) and, after several iterations and consultations, the enactment of the Digital Personal Data Protection Act, 2023. The recognition of privacy as a fundamental right thus set the constitutional backdrop against which data breaches – especially those involving institutions like banks that handle citizens' sensitive data – are now evaluated. Banks, as custodians of customers' personal and financial information, are expected to treat data protection not just as a good practice but as a legal duty flowing from the right to privacy.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

Legal and Regulatory Frameworks for Data Protection in Indian Banking

Information Technology Act, 2000 (Amended 2008): The Information Technology Act, 2000 (IT Act), as modified by the IT (Amendment) Act, 2008, is the main law managing data and cyber security in India. Significant data protection protections were included by the 2008 revisions. Notably, Section 43A was added, requiring body corporates to protect sensitive personal information by putting in place "reasonable security practices and procedures." According to Section 43A, a business, including a bank, is responsible for compensating the impacted parties for any unlawful loss or gain that arises from a careless implementation of security measures (such as a data breach that causes injury to individuals). This provision essentially makes companies accountable for data breaches, albeit through civil liability (compensation) rather than criminal penalty. Additionally, Section 72A was added to the IT Act, which criminalizes intentional personal data breaches – it punishes anyone (for example, an employee or service provider) who, in breach of a lawful contract, discloses personal information with the intent to cause harm or knowing it is likely to cause harm.

In 2011, the central government exercised the powers under Section 43A to notify the Information Technology (Reasonable Security Practices and Procedures and **Sensitive Personal Data or Information) Rules, 2011**, commonly known as the SPDI Rules. These rules define “sensitive personal data or information” (SPDI) to include financial information (like bank account or card details), authentication information (passwords), and other personal details. They mandate that organizations handling SPDI have a privacy policy, obtain consent for disclosure of information, and use reasonable security measures. The rules also provide that businesses must respond to complaints from data principals, or individuals, and show that they have put security safeguards in place in accordance with their stated policies in the event of a security breach, failing which they risk responsibility. Although these rules extended to all businesses, banks, as "body corporates," were clearly under their purview because they handled sensitive personal data.

RBI Cybersecurity Guidelines: In parallel with the IT Act, the banking sector is governed by regulations and guidelines issued by the RBI. The RBI has over the years developed a comprehensive cybersecurity framework for banks: In June 2016, the RBI circulated the “Cyber Security Framework in Banks” to all commercial banks. This framework required banks to take a proactive stance on cyber security.

Key mandates included: banks must have a Board-approved cyber security policy, an effective cyber risk assessment process, and robust controls to protect customer data. Banks were directed to set up 24x7 surveillance mechanisms and an incident response team to handle cyber incidents. The circular stressed the need for continuous resilience, noting that cyber-attacks were increasing in frequency and sophistication, and specifically mentioned that banks should have an adaptive incident response, management, and recovery plan to deal with breaches. Banks were also instructed to report any “unusual” cyber incidents to RBI immediately. The framework built on earlier guidance (such as the G. Gopalakrishna Committee’s 2011 report on information security) and elevated cyber security to a board-level concern.

Additionally, the RBI has sector-specific mandates that intersect with privacy and security. For example, RBI’s guidelines on digital payments security, its IT outsourcing guidelines,

and the payments data storage directive (2018) (which required payment system data to be stored only in India) all contribute to the protection of customer data. Banks are also subject to Know Your Customer (KYC) regulations, which include confidentiality obligations for customer data and periodic updates to protect against identity fraud. Violation of these various regulations can invite

regulatory scrutiny or penalties under the Banking Regulation Act. Thus, by the late 2010s, a multi-layered governance structure—IT Act rules, RBI regulations, and oversight by agencies like CERT-In—was in place to address data security in banks.

Data Protection Legislation –DPDP Act, 2023: The enactment of a specific data protection legislation is the most important recent development. The Digital Personal Data Protection Act, 2023 (DPDP Act) was passed in August 2023 following years of discussion following Puttaswamy. India's first comprehensive data privacy regulation, similar in aim to the EU's GDPR, was notified but not yet completely implemented in early 2025. It applies to a variety of industries, including banking, and aims to strike a balance between people's right to privacy and businesses' need to handle data for valid reasons.

Some key features relevant to banks and data breaches are:

1) Data Security Obligation:: In accordance with and in replacement of Section 43A of the IT Act for digital data, all data fiduciaries (businesses that decide how and why to process personal data) are required to protect personal data by putting in place appropriate security measures to stop breaches. Under this Act, banks that handle substantial amounts of sensitive financial and personal data would most likely be categorized as significant data fiduciaries, which entails additional duties like frequent audits and effect assessments on data protection.

2) Breach Notification: The DPDP Act introduces a requirement to report data breaches to the Data Protection Board of India (an adjudicatory body created by the Act). While the exact notification timelines are to be prescribed, the law mandates timely intimation of breaches. The Board may direct the organization to also inform affected individuals if it deems the breach likely to result in harm. This is a new mechanism; previously, Indian law had no direct requirement to notify data principals (customers) of a breach.

3) Penalties: The Act arms the Data Protection Board with powers to levy hefty financial penalties for non-compliance, including for data breaches. The law specifies tiered penalties These penalties represent a dramatic escalation of potential consequences for banks compared to the older IT Act (which limited compensation to actual damages and had relatively small fines under Section 72A). The prospect of such penalties is expected to incentivize banks to invest more in cybersecurity infrastructure and privacy compliance.

4) Rights and Consent: The DPDP Act emphasizes consumer rights – it gives bank customers (as "Data Principals") rights to access information on how their data is used, to correct or erase data, and to grievance redressal, among others. Banks must now process personal data only for specific, consented purposes or for certain legitimate uses defined in law. For example, a bank can no longer use a customer's data for cross-selling unrelated products without obtaining informed consent, or it could face regulatory sanctions for misuse of data. This focus on consent and purpose limitation ties into privacy: it curtails the potential abuse of personal data and thereby indirectly reduces privacy risks.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

Recent Cybersecurity Incidents in Indian Banks: Case Studies

Indian banks have faced numerous cyber incidents in recent years, ranging from data leaks exposing personal information to sophisticated hacks stealing millions of rupees. A 2021 disclosure in Parliament, for example, noted that 290,445 cyber security incidents related to digital banking were reported in 2020 alone – a sharp increase from previous years. These incidents include

phishing attacks, malware infections, unauthorized access to systems, and data breaches. According to one study, Indian banks reported 248 significant information breaches between June 2018 and March 2022, reflecting the growing attack surface with increased digitization (Khan, 2024). To illustrate the challenges and implications, we discuss two notable case studies from the past five years: a data leak at India's largest bank (SBI) that directly impacted customer privacy, and a major cyber-heist at a cooperative bank (Cosmos Bank) that exposed systemic vulnerabilities.

Case Study 1: State Bank of India Data Leak

In January 2019, the State Bank of India (SBI) – the country's largest public sector bank – experienced a major data breach that demonstrated how even basic security lapses can put millions of customers' privacy at risk. The incident revolved around SBI's "SBI Quick" facility, a service that allows customers to obtain their account balance or mini-statement via a simple text message or missed call. It was discovered that one of SBI's servers in its Mumbai data center, which handled the backend SMS functionality for this service, was left unprotected – no password or authentication was required to access it. This misconfiguration effectively exposed a treasure trove of personal financial data to anyone who knew where to look.

The impact on customer privacy in this case was direct. Sensitive financial information that customers reasonably expected to remain confidential between them and their bank was effectively public (for as long as the server was unsecured). While the leaked data did not include names or full account numbers, the phone number and partial account digits could identify individuals, and their private financial status was being broadcast. Such exposure violates the principles of privacy and data minimization – SBI was storing far more data (every SMS sent to every customer) than necessary on a live server, and failing to secure it.

Case Study 2: Cosmos Bank Cyber Heist

Cosmos Cooperative Bank – one of India's largest cooperative banks, headquartered in Pune – fell victim to a highly coordinated cyberattack. While this incident was primarily a theft of funds rather than a leak of personal data, it had significant implications for data security and prompted regulatory action. The Cosmos Bank attack is often referenced as a case where state-sponsored hackers targeted the backbone of a bank's IT systems. Over a fateful weekend (August 11 and 13, 2018), attackers managed to infiltrate the bank's network and compromise its ATM switch and the SWIFT payment system. They authorized a flood of fraudulent ATM withdrawals worldwide, siphoning off ₹94.42 crore (approximately USD 13.5 million) in just two days.

According to investigations (including a report by a U.N. Security Council panel), the operation was "advanced, well-planned and highly coordinated," bypassing multiple layers of security. The hackers effectively faked the bank's backend systems responses: when their accomplices around the globe used cloned debit cards at ATMs, the malware in Cosmos's network approved those transactions even though they vastly exceeded any customer's balance or card limits.

From a privacy and data perspective, the Cosmos Bank breach is illustrative of systemic risk. The attackers penetrated the bank's internal systems, which means they had access to sensitive customer data stored in those systems (card numbers, PINs or encrypted PIN blocks, account details, etc.). They manipulated data flows and probably extracted some data to create cloned cards. While the primary objective was stealing funds (which they accomplished), one can infer that customer information was compromised as a means to that end – for example, card information and associated PINs had to have been obtained, either by planting malware that captured them or by infiltrating the switch that validates PINs. So, although Cosmos did not report a "data leak" of personal details to the public, the incident intrinsically involved a breach of confidentiality of customer data and banking processes. Customers of Cosmos Bank were directly affected in that their account balances were altered by unauthorized withdrawals (which the bank had to subsequently reconcile and likely refund). They also experienced disruption – the bank briefly halted all digital channels and ATM services to contain the breach once detected.

The Cosmos Bank heist was a pivotal case that exposed vulnerabilities in smaller banks' cyber infrastructure. It highlighted a privacy loophole in a broader sense: attackers didn't need to publicly leak personal data when they could silently exploit it for illicit gain. This kind of incident pressured regulators to ensure banks, big or small, implement stringent security protocols. The UNSC panel report (2019) confirming North Korea's hand also brought geopolitical attention to Indian bank cybersecurity. In summary, while Cosmos Bank's case was a criminal heist, it serves as a case study in how failures in cybersecurity can devastate a financial institution and its customers, and how that in turn has ramifications for privacy and national security. It led to tangible regulatory tightening (especially for cooperative banks) and stands as a cautionary tale that protecting customer data isn't just about avoiding leaks – it's about securing every aspect of digital banking operations.

Impact on Customer Privacy and Regulatory Responses

The case studies and incidents outlined above illuminate several dimensions of how cybersecurity failures in banks impact customer privacy,

Impacts on Customer Privacy: When a bank suffers a data breach, the immediate impact is the loss of confidentiality of customers' personal information. In the SBI case, account and transaction details meant to be private between the bank and customer were exposed to potentially anyone on the internet – a clear breach of privacy. Such information can reveal a person's financial habits, income level, or personal circumstances (e.g., frequent hospital payments could hint at medical issues). This intrusion into a person's private domain, without their knowledge or consent, runs afoul of the fundamental right to privacy recognized in Puttaswamy. Even in incidents like Cosmos Bank, where data was misused rather than widely exposed, customers' privacy was compromised by unauthorized parties accessing their

account details and using them. Beyond the abstract notion of privacy, these breaches create tangible risks for individuals: identity theft, targeted phishing (using leaked info to sound convincing), or financial fraud. Customers also suffer a loss of autonomy and dignity when their personal financial information is out of their control.

Legal Recourse for Customers: Until the DPDP Act, customers had limited direct recourse. They could file a complaint to adjudication officers under the IT Act for compensation (Section 43A) or lodge an FIR if there was a clear offence (like Section 72A violation). In practice, such actions have been rare. One obstacle was the lack of awareness and the complexity of proving harm. Another was the absence of class-action mechanisms – each affected person would have to individually claim compensation. With the new law, this may change: the Data Protection Board can take suo motu cognizance of large breaches and impose penalties, which, though paid to the state, exert pressure on organizations to offer redress (like free credit monitoring for victims or improving services). We might see the Board ordering banks to inform customers of steps to protect themselves post-breach. Additionally, consumers might leverage the deficiency of service provisions of consumer protection law to seek remedies for data breaches, though this is untested in banking privacy context.

Customer Notification and Redressal: One glaring loophole in the regime until now has been the lack of a clear obligation to notify affected customers. In contrast to jurisdictions with data breach notification laws (e.g., under GDPR, individuals must be informed if a breach poses high privacy risks), Indian banks have often kept breaches under wraps or disclosed them only partially. For instance, SBI did not notify each of the millions of customers whose account data was exposed in 2019; Cosmos Bank's customers were not individually informed that their card data may have been at risk, beyond general statements. This can leave customers unable to take timely protective measures (like changing passwords or being vigilant about phishing attempts).

The DPDP Act's introduction of a formal reporting mechanism is expected to improve this. If the Data Protection Board directs a bank to notify customers, non-compliance could lead to penalties. Additionally, RBI could incorporate customer notification into its incident reporting framework – for example, requiring banks to issue public notices when a significant breach occurs. There have been improvements: some banks have started sending advisories to customers after industry-wide incidents (e.g., after the 2016 card breach, many banks proactively messaged cardholders to reset PINs or replace cards, even if their own systems weren't the source of breach).

Technical Controls: Strong encryption of sensitive data (both at rest in databases and in transit over networks) is essential. Many banks now use end-to-end encryption for transactions and mask personal data fields. Network segmentation is another practice – separating the ATM switch, core banking, and internet banking systems so a breach in one does not immediately grant access to others. Regular patching of software and updating of ATM/POS firmware are necessary to close known vulnerabilities.

Monitoring and Response: Banks must maintain Security Operations Centers (SOCs) that monitor for suspicious activities 24/7. This includes deploying Intrusion Detection/Prevention Systems, anti-malware tools, and anomaly detection (especially using AI/ML to catch unusual

transaction patterns that might indicate fraud or breach, as recommended by RBI's framework). Incident response plans should be in place and drilled. As the RBI noted, the ability to quickly respond and recover from cyber incidents is a critical part of resilience.

Third-Party Risk Management: Banks often rely on vendors for services (ATM management, cloud storage, payment processing). Ensuring these third parties also uphold strong data protection (through contracts and audits) is part of the bank's responsibility. RBI's guidelines on outsourcing and the DPDP Act's concept of data processors both emphasize that the ultimate responsibility lies with the data fiduciary (the bank).

Customer Awareness and Notification: Increasingly, banks in India are taking on the role of educating their customers about scams and safe banking practices (via emails, SMS alerts, and website notices). This is a vital component because a chunk of breaches involve social engineering. Furthermore, banks have started issuing timely alerts – for example, instant SMS/Email notifications for any transaction on an account can help a customer notice unauthorized activity and inform the bank, potentially limiting damage. In terms of privacy, some banks allow customers to control their privacy settings, e.g., opting out of certain data sharing or marketing uses, which is a good practice aligned with consent principles.

Recommendations and Conclusion

Indian banks stand at a crossroads where rapid digitalization must be matched with rigorous cyber security and privacy protection measures. Based on the analysis, several recommendations emerge:

Effective Implementation of the DPDP Act: The new data protection law's obligations should be completely implemented by banks, according to regulators. This entails designating Data Protection Officers, carrying out recurring impact analyses on data protection, and fostering a privacy-conscious culture. Once it is up and running, the RBI and the Data Protection Board of India should collaborate closely to monitor bank breach cases. If a bank notifies RBI/CERT-In of a significant data breach, a procedure can be established that notifies the Data Protection Board as well, initiating its own assessment. Cooperation and consistency among authorities will speed up remedial action and stop violations from slipping through the gaps.

Mandatory Breach Disclosure to Customers: Notifying the impacted parties of the breach formally is essential. The DPDP Act's regulations ought to outline the conditions under which people must be informed (for instance, if their identity or financial information is compromised). RBI can support this by releasing regulations requiring banks to promptly notify clients about data mishaps and provide advice on what to do (such as changing passwords or keeping an eye on accounts). Although acknowledging a breach may have a short-term negative impact on one's reputation, transparency fosters trust over time since customers value openness and preventative measures.

Strengthening Cybersecurity Infrastructure Banks ought to make investments in cutting-edge cybersecurity solutions, particularly smaller and mid-sized ones. This could entail implementing multi-factor authentication globally (not just for user login but also for internal inter-system access), implementing advanced threat detection systems (which use artificial intelligence to identify anomalies), and embracing zero-trust architecture (where every access

request is validated every time). Strong backup plans and network isolation techniques are required in light of the increase in ransomware and APT (advanced persistent threat) assaults. This will guarantee that,
even in the event that a bank's network is hacked in one area, the entire business or critical data stores are not immediately jeopardized.

Enhanced Regulatory Enforcement: When carelessness is obvious, regulators shouldn't be afraid to use fines or other supervisory measures (such preventing a bank from launching new digital products until security flaws are resolved). A deterrent impact is produced by consistent enforcement. Regulators can also provide positive reinforcement. For example, a "cyber hygiene rating" that honors banks with excellent cybersecurity measures may inspire others. Crucially, any fines incurred for data breaches may be recycled back into security enhancements by establishing a fund for customer awareness and CERT-In's capacity building.

Consumer Empowerment and Redressal: Consumers ought to have more control over their data. In accordance with the DPDP Act's rights, banks can offer their clients easily navigable dashboards that show them the information they have about them and how it is utilized. A simple way for clients to report privacy issues or suspected data misuse to the bank (and, if they're not satisfied, to the Banking Ombudsman or Data Protection Board) should be put in place for redress. When breaches are verified, banks may think about providing impacted clients with remedies like free credit monitoring or identity theft insurance. These measures are typical in other jurisdictions following breaches and aid in restoring customer trust.

Education and Awareness: To raise awareness about cybersecurity, cooperation is required. Regulators have the ability to launch secure banking campaigns across the country, some of which have begun with catchphrases like "Think Before You Click." Individual banks should keep informing their clients. For instance, they should post dos and don'ts for online banking or clarify that they will never request an OTP over the phone. By avoiding frauds that could circumvent technical protection, informed clients enhance the bank's security procedures.

In conclusion, the relationship between cybersecurity, data breaches, and privacy rights in Indian banking is a crucial and quickly developing field. Banks are expected to handle personal data carefully since privacy is now recognized as a fundamental right. We are reminded that banks need to protect themselves from a variety of risks by case studies such as SBI and Cosmos Bank, which show that breaches can result from both straightforward setup errors and extremely sophisticated attacks. The legal frameworks have been catching up. A new data protection regime that promises stricter enforcement has strengthened the IT Act's previously disorganized rules and standards. However, the effectiveness of rules and regulations depends on how well they are implemented.
Therefore, it is incumbent on banks not just to comply minimally, but to genuinely prioritize cybersecurity and privacy as core values.

Investments in technology, qualified staff, and reliable procedures are necessary for this, as is a corporate culture that values customer data. In the end, safeguarding data in banks is about maintaining the confidence that forms the foundation of banking, not just about avoiding fines or legal action. Ensuring robust privacy and security measures will decide how safely and confidently individuals may use Indian banks as they continue to digitize and reach millions of new customers, particularly in the age of mobile banking and UPI.aInvestments in

technology, qualified staff, and reliable procedures are necessary for this, as is a corporate culture that values customer data. In the end, safeguarding data in banks is about maintaining the confidence that forms the foundation of banking, not just about avoiding fines or legal action. Ensuring robust privacy and security measures will decide how safely and confidently individuals may use Indian banks as they continue to digitize and reach millions of new customers, particularly in the age of mobile banking and UPI.

References:

1. Supreme Court of India. (2017). Justice K.S. Puttaswamy (Retd.) & Anr. vs Union of India & Ors., (W.P. (Civil) No. 494/2012, decided 24 Aug 2017). (Privacy Judgment affirming the fundamental right to privacy).

2. Information Technology Act, 2000 (Amended 2008), §43A & §72A. (India) – Provisions introducing liability for failure to protect data and penalizing wrongful disclosure of personal data.

3. Reserve Bank of India (RBI). (2016, June 2). Cyber Security Framework in Banks (RBI/2015-16/418). Mumbai: RBI. (RBI circular mandating banks to strengthen cyber security and board-approved policies).

4. Reserve Bank of India (RBI). (2019, August 2). Press Release: RBI imposes monetary penalty on Corporation Bank. (RBI penalized Corporation Bank ₹1 crore for non-compliance with cyber security directions)

5. Whittaker, Z. (2019, January 30). India's largest bank SBI leaked account data on millions of customers. TechCrunch. (Article revealing SBI's server left unprotected, exposing millions of customer records).

6. Das, S. (2019, February 1). SBI denies data leak charges, but customers be on alert. The Economic Times. (Report on SBI's response to the alleged data leak).

7. Iyer, S., & Shelke, G. (2019, March 28). North Korea hand in Pune's Cosmos Bank cyber heist: UNSC panel. The Times of India. (News report confirming Lazarus Group's link to the Cosmos Bank hack and describing the modus operandi).

8. Securonix Threat Research. (2018, August 29). Cosmos Bank SWIFT/ATM Cyber Attack – Technical Analysis. Securonix Blog. (Technical breakdown of the Cosmos Bank attack, attribution, and techniques).

9. Press Trust of India. (2021, Feb 4). Over 290,000 cyber security incidents related to banking reported in 2020. Business Standard. (Parliamentary data on cyber incidents in banking).

10. Khan, A. (2024). Regulatory Framework of Data Breaches in the Indian Banking Sector. Indian Journal of Integrated Research in Law, 4(2), 908–928. (Academic article reviewing laws and policies on data breaches in Indian banking).

11. Burman, A. (2023, October 3). Understanding India's New Data Protection Law. Carnegie India Working Paper. (Analysis of the DPDP Act 2023 and its implications for data protection).

12. Digital Personal Data Protection Act (DPDP Act), 2023. No. 22 of 2023, Govt. of India. (Comprehensive law on personal data protection providing consent, rights, and penalties).

13. Juris Corp (Sinha, A., Jhanjee, R., & Naik, G.) (2023, August 25). Digital Personal Data Protection Act, 2023 – Boon or Bane for Banks and Financial Institutions?. Lexology. (Legal commentary on how the DPDP Act will impact banks, noting new obligations and penalties).